Version released: January 25, 2015

What is Mathematics: Gödel's Theorem and Around

Hyper-textbook for students

by **Karlis Podnieks**, Professor

University of Latvia
Institute of Mathematics and Computer Science

Diploma, 1999

An extended translation of the 2nd edition of my book "Around Gödel's theorem" published in 1992 in Russian (online copy).

Diploma, 2000

This hyper-textbook contains many links to:
Wikipedia, the free encyclopedia;
MacTutor History of Mathematics archive
of the University of St Andrews;
MathWorld of Wolfram Research.

Are you a **platonist**? Test yourself.

Tuesday, August 26, 1930:

Chronology of a turning point in the human intellectual history...

Visiting Gödel in Vienna...

An explanation of

"The **Incomprehensible Effectiveness of Mathematics** in the Natural Sciences" (as put by Eugene Wigner).

Table of Contents

References

Barwise J. (1942-2000) [1977]

Handbook of Mathematical Logic, Elsevier Science Ltd., 1977, 1166 pp. (Russian translation available)

Brouwer L. E. J. [1912]

Intuitionism and formalism. Inaugural address at the University of Amsterdam (October, 14, 1912). Published in Bull. Amer. Math. Soc., 1913, vol. 20, pp.81-96 (online copy).

van Dantzig D. [1955]

Is 10**10**10 a finite number? "Dialectica", 1955, vol.9, N 3/4, pp. 273-278

Detlovs V., Podnieks K. [2000]

Introduction to Mathematical Logic. Hyper-textbook for students, 2000-2013. Available online.

Devlin K. J. [1977]

The axiom of constructibility. A guide for the mathematician. "Lecture notes in mathematics", vol. 617, Springer-Verlag, Berlin – Heidelberg – New York, 1977, 96 pp.

Feferman S., Friedman H. M., Maddy P., Steel J. R. [2000]

Does mathematics need new axioms? "The Bulletin of Symbolic Logic", 2000, vol.6, N 4, pp. 401-446 (see online copy at www.math.ucla.edu/~asl/bsl/0604/0604-001.ps).

Hadamard J. [1945]

An essay on the psychology of invention in the mathematical field. Princeton, 1945, 143 pp. (Russian translation available)

Heijenoort van J. [1967]

From Frege to Gödel: A Source Book in Mathematical Logic, 1879-1931. Harvard University Press, 1967, 680 pp.

Hersh R. [1979]

Some Proposals for Reviving the Philosophy of Mathematics. "Advances in Mathematics", 1979, vol. 31, pp. 31-50.

Jech T. Lectures in set theory with particular emphasis on the method of forcing. "Lecture Notes in Mathematics", vol. 217, Springer-Verlag, Berlin –

Heidelberg – New York, 1971 (Russian translation available)

Keldysh L. V. [1974]

The ideas of N.N.Luzin in descriptive set theory. *Russian Mathematical Surveys*, 1974, vol. 29, N 5, pp. 179-193 (Russian original: *Uspekhi matematicheskih nauk*, 1974, vol. 29, N 5, pp. 183-196).

Mendelson E. [1997]

Introduction to Mathematical Logic. Fourth Edition. International Thomson Publishing, 1997, 440 pp. (Russian translation available)

Parikh R. [1971]

Existence and Feasibility in Arithmetic. JSL, 1971, Vol.36, N 3, pp.494-508.

Podnieks K. M. [1975]

The double-incompleteness theorem. *Scientific Proceedings of Latvia State University*, 1975, Vol.233, pp. 191-200 (in Russian, online copy: PDF).

Podnieks K. M. [1976]

The double-incompleteness theorem. *Proceedings of Fourth All-Union Conference on Mathematical Logic*, 1976, Kishinev, p.118 (in Russian, online copy: PDF, English translation: Section 6.2).

Podnieks K. M. [1988a]

Platonism, Intuition and the Nature of Mathematics. "*Heyting'88. Summer School & Conference on Mathematical Logic. Chaika, Bulgaria, September 1988. Abstracts.*", Sofia, Bulgarian Academy of Sciences, 1988, pp.50-51 (online copy: PDF).

Podnieks K. M. [1988b]

Platonism, Intuition and the Nature of Mathematics. Riga, Latvian State University, 1988, 23 pp. (in Russian).

Podnieks K. M. [1981, 1992]

Around Gödel's theorem. Latvian State University Press, Riga, 1981, 105 pp. (in Russian). 2nd edition: "Zinatne", Riga, 1992, 191 pp. (in Russian).

Poincare H. [1908]

Science et methode. Paris, 1908, 311 pp. (Russian translation available)

Rashevsky P. K. [1973] (translated also as Rashevskii)

On the dogma of natural numbers. *Uspekhi matematicheskih nauk*, 1973, vol.28, N 4, pp.243-246 (in Russian). See also *Russian Mathematical Surveys*, 1973, vol.28, N4, 143-148 (online copy).

1. Platonism, intuition and the nature of mathematics

This chapter presents an extended the translation of the paper:

K. Podnieks. Platonism, intuition and the nature of mathematics. In: *Semiotika i informatika*, Moscow, VINITI, 1990, Vol. 31, pp. 150-180 (in Russian).

It was included also as the first chapter into my book "Around Gödel's theorem" published in 1992 in Russian. View onlinee copy of the Russian original.

History. The 1st edition of the book was published in 1981 in Russian (view online copy of Chapter 1). In English, its concepts were first presented in 1988 at the Heyting'88 Summer School & Conference on Mathematical Logic (view copy of Abstract), after that – in November 1994, on the QED mailing list, in 5 parts:

http://ftp.mcs.anl.gov/pub/qed/archive/147 #1
http://ftp.mcs.anl.gov/pub/qed/archive/148 #2
http://ftp.mcs.anl.gov/pub/qed/archive/149 #3
http://ftp.mcs.anl.gov/pub/qed/archive/151 #4
http://ftp.mcs.anl.gov/pub/qed/archive/152 #5

1.1. Platonism – the Philosophy of Working Mathematicians

Charles Hermite: "I believe that the numbers and functions of analysis are not the arbitrary product of our spirits: I believe that they exist outside us with the same character of necessity as the objects of objective reality; and we find or discover them and study them as do the physicists, chemists and zoologists." (quoted after Mathematical Quotes by F2.org)

Some time ago, in the former USSR this proposition was quoted as an evidence of "naive materialism of distinguished scientists".

Still, such propositions stated by mathematicians are evidences not of their naive materialism, but of their **naive platonism**. As will be shown below, **platonist attitude of mathematicians to objects of their investigations is determined by the very nature of the mathematical method**.

Henri Poincaré qualified Hermite's position as platonism already in 1912: "I have never known a more realistic mathematician in the Platonist sense than Hermite..." (H. Poincare. Last Thoughts, Chapter 5).

For more exact Hermite's quotes see:
Mathematical Quotes by F2.org,
Gödel, Cantor and Plato by Denis Eric Paul.

First let us consider the "platonism" of Plato (427-347 BC) himself . The

particular form of Plato's system of philosophy was inspired by Greek mathematics.

In VI-V centuries BC the evolution of Greek mathematics led to mathematical objects in the modern meaning of the word: the ideas of numbers, points, straight lines etc. stabilized, and thus they were detached from their real source – properties and relations of things in the human practice. In geometry, straight lines have zero width, and points have no size at all. Actually, such things do not exist in our everyday practice. Here, instead of straight lines we have more or less smooth stripes, instead of points – spots of various forms and sizes. Nevertheless, without this passage to an ideal (partly fantastic, yet simpler, stable, fixed, self-contained) "world" of points, lines etc., the mathematical knowledge would have stopped at the level of a craft and never would become a science. By idealization an extremely efficient instrument was created – the Euclidean geometry.

The concept of natural numbers (1, 2, 3, 4, ...) developed from human operations with collections of discrete objects. This development process was completed already in VI century BC, when somebody asked: how many prime numbers do there exist? And the **answer was found by means of reasoning –** there are infinitely many prime numbers. Clearly, it is impossible to verify such an assertion empirically. Still, by that time the concept of natural number was already stabilized and detached from its real source – the quantitative relations of discrete collections in the human practice, and it started working as a **stable self-contained model**. The system of natural numbers is an idealization of these quantitative relations. People abstracted it from their experience with small collections (1, 2, 3, 10, 100, 1000 things). They extrapolated their rules onto much greater collections (millions of things) and thus idealized the real situation (and even deformed it – see Rashevsky [1973] and van Dantzig [1955]).

Pyotr Konstantinovich Rashevsky (translated also as Petr, or Rashevskii) – on the FOM list http://www.cs.nyu.edu/pipermail/fom/1998-April/001825.html

Note. The idea of the Infinite deviates significantly from the situation in the physical Universe – this fact was clearly stated already in the famous June 4, 1925 lecture by David Hilbert "On the Infinite":

D. Hilbert. Über das Unendliche. "Math. Annalen", 1925, Vol.95, pp.161-190 (see also van Heijenoort [1967])

See also Bernays [1934]: "... From two integers k, l one passes immediately to k^l; this process leads in a few steps to numbers which are far larger than any occurring in experience, e.g. $67^{257^{729}}$. Intuitionism, like ordinary mathematics, claims that this number can be represented by an Arabic numeral. Could not one press further the criticism which intuitionism makes of existential assertions and raise the question: What does it mean to claim the existence of an Arabic numeral for the foregoing number, since in practice we are not in a

position to obtain it?"

and Parikh [1971], p.507: "Does the Bernays number $67^{257^{729}}$ actually belong to every set which contains 0 and is closed under the successor function? The conventional answer is yes yet we have seen that there is a very large element of fantasy in conventional mathematics which one may accept if one finds it pleasant, but which one could equally sensibly (perhaps more sensibly) reject."

My favorite example: let us consider "the number of atoms in this sheet of paper". From the point of view of common arithmetic this number "must" be either even or odd at any moment of time. In fact, however, the sheet of paper does not possess any precise "number of atoms" (because of, for example, spontaneous nuclear reactions). Moreover, the modern cosmology claims that the "total number" of particles in the Universe is far less than 10^{2000}. What should be then the real meaning of the statement "$10^{2000}+1$ is an odd number"? Thus, in arithmetic not only practically useful algorithms are discussed, yet also a kind of pure fantastic matter without any direct real meaning. (Rashevsky proposed to develop a new kind of arithmetic allowing a more adequate – "realistic"– treatment of large natural numbers.)

[Added November 14, 2005] The idea that "infinity does exist in the Universe" is, in fact, more complicated than represented above. The "total number" of particles in the Universe is, indeed, far less than 10^{2000}. But how about the "total number" of pairs, triples and other sets of these particles? Hence, in a sense, much bigger numbers may "exist" in the Universe – the number of sets of particles – less than $2^{10^{2000}}$, the number of sets of sets of particles – less than $2^{2^{10^{2000}}}$, etc. But, admitting this, we must admit also that, in the Universe, only some small enough natural numbers can be **represented in a uniform way**, for example – as sums 1+1+...+1 (the number of units cannot exceed the "total number" of particles). See also:

David Isles. What Evidence is There That 2^65536 is a Natural Number? *Notre Dame Journal of Formal Logic*, Vol.33, N4, Fall 1992, pp.465-480 (available online). Two remarkable quotes:

"... The former [computing of 2+2+2+2+2, or 2*2*2*2*2, K.P.] is quite feasible and can be performed in a short time whereas the latter [computing of 2^2^2^2^2, K.P.] represents a number which exceeds the total number of vibrations executed by all subatomic particles of size < 10^{-30} cm (smaller than a quark!) which would be needed to fill a universe of radius 10^{12} light years (larger than the observational diameter of the universe!) were each to vibrate 10^{50} times per second over a period of 10^{12} years (longer than the surmised age of the universe!). Neither now, no ever (as far as we can tell at present) is there likely to be a case where the computation that starts with 2^{65536} and proceeds according to the recursion rules terminates.

... Eventually, due to the increasing amount of data involved, any completely specified computing scheme must break down and require revision; and it is by no means clear that **the pattern of these revisions has any uniformity** [marked bold by me, K.P.]."

[Added May 6, 2006] Seth Lloyd about the computational capacity of the Universe:

"All physical systems register and process information. The laws of physics determine the

amount of information that a physical system can register (number of bits) and the number of elementary logic operations that a system can perform (number of ops). The Universe is a physical system. The amount of information that the Universe can register and the number of elementary operations that it can have performed over its history are calculated. The Universe can have performed 10^{120} ops on 10^{90} bits (10^{120} bits including gravitational degrees of freedom)."

S. Lloyd. Computational capacity of the universe. *Physical Review Letters*, 2002, vol. 88, issue 23 (available online, see also extended online version).

For similar ideas about the "ontological status" of natural numbers, see also:

E Brian Davies. Empiricism in Arithmetic and Analysis, *Philosophia Mathematica* (3) 11 (2003) 53-66.

Doron Zeilberger. "Real" Analysis is a Degenerate Case of Discrete Analysis, (appeared in "New Progress in Difference Equations" (Proc. ICDEA 2001), Taylor and Francis, London, 2004)

Thus, the process of idealization ended in stable, self-contained concepts of numbers, points, lines etc. These concepts stopped to change and were commonly acknowledged in the community of mathematicians. And all that was achieved already in VI-V century BC. Since that time our concepts of natural numbers, points, lines etc. have changed very little. The stabilization of concepts is an evidence of their detachment from the real objects that have led people to these concepts and that are continuing their independent life and contain an immense variety of changing details. When working in geometry, a mathematician does not investigate the relations of things of the human practice (the "real world" of materialists) directly, he investigates some stable notion of these relations – an idealized, fantastic "world" of points, lines etc. And during the investigation this notion is treated (subjectively) as the "last reality", without any "more fundamental" reality behind it. If during the process of reasoning mathematicians had to recall permanently the peculiarities of real things (their degree of smoothness etc.), then instead of a science (efficient geometrical methods) we would have a kind of craft – simple, specific algorithms obtained by means of trial and error or on behalf of some elementary intuition. Mathematics of Ancient Orient stopped at this level. Greeks went further.

(See an online paper "Babylonian and Egyptian mathematics" in the MacTutor History of Mathematics archive).

[Added November 8, 2005] Since XVII century, this "method of idealization" allowing to create simple and powerful models was applied with great success to physical modeling by introducing the notion of uniform motion (in fact, something that does not exist at the macro-level!), the notion of ideal gas, etc.

Studying mathematics Plato came to his surprising philosophy of two worlds: the world of ideas (as perfect as the "world" of geometry) and the world of things. According to Plato, each thing is only an imprecise, imperfect

implementation of its idea (existing independently of the thing itself in the world of ideas). Surprising and completely fantastic was Plato's notion of the nature of mathematical investigation: before a mathematician is born, his soul is living in the world of ideas, and afterwards, doing mathematics, he simply recalls what his soul has learned in the world of ideas.

For a materialist, this may seem an upside-down notion of the real situation. Plato treats the end product of the evolution of mathematical concepts – a stable, self-contained system of idealized objects – as an independent starting point of the evolution of the "world of things"? Still, it was the first attempt (and, for IV century BC – a brilliant one!) to explain the specific position of the mathematical knowledge among other branches of the human knowledge. Materialists tend to think of mathematics as "one of" the branches of science. It's true that the process of genesis of the first mathematical concepts (arithmetic and Euclidean geometry) was very similar to the process of genesis of the first concepts of "other" branches of science. But Plato realized that mathematical concepts have become stable, self-contained, and hence, "independent forever". Of course, for us, Plato's radical simple explanation of this independence seems completely fantastic. Today, we do not need the hypothesis of "platonic worlds" to explain the nature of mathematical concepts.

And today, any philosophical position treating ideal objects of human thought as a specific independent "world", should be called **platonism**. Particularly, the everyday philosophy of working mathematicians is a platonist one. **Platonist attitude to objects of investigation is inevitable for a mathematician**: during his everyday work he is used to treat numbers, points, lines etc. as the "last reality", as a specific independent "world". This sort of **platonism is an essential aspect of the mathematical method.** It explains also the inevitability of platonism in the philosophical positions of mathematicians (having, as a rule, very little experience in philosophy). Habits, obtained in the everyday work, have an immense power. Therefore, when a mathematician, not very strong in philosophy, tries to explain "the nature" of his mathematical results, he unintentionally brings platonism into his reasoning. The reasoning of mathematicians about the "objective nature" of their results is, as a rule, rather a kind of "objective idealism", not "materialism".

The problem, seen from another angle by Keith J. Devlin:

At heart, on a day-to-day basis, practically all mathematicians work in a highly intuitive fashion built on an out-and-out Platonistic philosophy. Abstract mathematical entities such as numbers ... and spaces ... are regarded as 'real objects' in a world that the mathematician sets out to *discover*. They are part the the mental world that the mathematician learns to live in and become familiar with. (p.65)

... it is far, far easier to reason using such entities. I happen to think that our intellectual

development does not progress very far beyond our childhood manipulations of marbles, sticks, counters, beans and what-have-you. We reach a stage of maturity when we can reason using abstract objects created by the mind, ... the use of *abstract* objects greatly facilitates this increased logical complexity. But it is still reasoning *about objects*. (p.67)

Full text:

K. J. Devlin. Logic and information. Cambridge University Press, 1991/1995, 328 pp.

Whether your own philosophy of mathematics is platonism or not, can be determined easily by using the following test.

Let us consider the twin prime number sequence (two primes are called twins, if their difference is 2):

(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71,73), (101, 103), (107,109), (137, 139), (149, 151), (179, 181), (191, 193), ...,

(1787, 1789), ..., (1871, 1873), ...,
(1931, 1933), (1949, 1951), (1997, 1999), (2027, 2029), ...

It is believed (as conjectured in 1849 by Alphonse de Polignac) that there are infinitely many twin pairs (the famous Twin Prime Conjecture), yet the problem remains unsolved up to day. Do you believe that the twin prime conjecture must be either true, or false, and that this does not depend on us, humans? Imagine, we are moving along the natural number system:

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, ...

And we meet twin pairs from time to time: (3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), ... It seems there are only two possibilities:

a) We meet the last pair and after that moving forward we do not meet any twin pairs (i.e. the twin prime conjecture is false),

b) Twin pairs appear over and again (i.e. the twin prime conjecture is true).

It seems impossible to imagine a third possibility...

If you think so, you are, in fact, a platonist. You are used to treat the natural number system as a specific independent "world", very much like the world of your everyday practice. You are used to think that any sufficiently definite assertion about things in this world must be either true or false. And, if you regard natural number system as a specific "world", you cannot imagine a third possibility: maybe, **the twin prime conjecture is neither true, nor false**. Still, such a possibility would not surprise you if you would realize (following Rashevsky [1973]) that **the natural number system contains not only some information about real things of the human practice, it also contains many elements of fantasy. Why do you think that such a fantastic "world" (a kind of Disneyland) should be completely perfect?**

Note. About Disneyland in mathematics. This metaphora was used by Alfred Tarski, at the

"Tarski Symposium", University of Berkeley, 1971:

"People have asked me 'How can you, a nominalist, do work in set theory and logic, which are theories about things you do not believe in?' . . . I believe there is value even in fairy tales and the study of fairy tales."

Quoted after p.52 of: **Alfred Tarski: Life and Logic**. *By Anita Burdman Feferman and Solomon Feferman, Cambridge University Press, Cambridge, UK, 2004.*

And by Reuben Hersh and Philip J. Davis:

"Do we really have to choose between a formalism that is falsified by our everyday experience, and a Platonism that postulates a mythical fairyland where the uncountable and the inaccessible lie waiting to be observed by the mathematician whom God blessed with a good enough intuition?"

See p.406 of: **The Mathematical Experience**. *By Reuben Hersh and Philip J. Davis, Birkhauser: Boston, USA , 1981.*

As another striking example of a platonist approach to the nature of mathematics let us consider an expression by N. N. Luzin from 1927 about the Continuum Problem (quoted after Keldysh [1974]):

"The cardinality of continuum, if it is thought to be a set of points, is some unique reality, and it must be located on the aleph scale there, where it is. It's not essential, whether the determination of the exact place is hard or even (as Hadamard might add) impossible for us, men".

For finite sets, **cardinality** of a set is simply the number of members it contains. Georg Cantor extended this notion to infinite sets, trying to compare such sets by their "size", see below.

The **Continuum Problem** was formulated by Cantor in 1878: does there exist a set of points with cardinality greater than the cardinality of natural numbers (the so called *countable cardinality*) and less than the *cardinality of the continuum* (i.e. the cardinality of the set of all points of a line)? In set theory (by using the Axiom of Choice) one can prove that the cardinality of every infinite set can be measured by means of the so-called *aleph scale*:

$$\aleph_0, \aleph_1, \aleph_2, \ldots, \aleph_n, \aleph_{n+1}, \ldots, \aleph_\omega, \aleph_{\omega+1}, \ldots \quad .$$

Here $\aleph_0$ is the countable cardinality, $\aleph_1$ – the least uncountable cardinality etc., and $\aleph_\omega$ follows after all $\aleph_n$ with natural number n.

Cantor established that $\aleph_0 < c$ (c denotes the cardinality of the continuum), and after this he conjectured that $c = \aleph_1$. This conjecture is called **Continuum Hypothesis**. Long-drawn efforts by Cantor himself and by many other outstanding people did not lead to any solution of the problem. In 1905 Julius König proved that $c \neq \aleph_\omega$, and that is almost all we have today...

Now we know that the Continuum Problem is undecidable, if we are using the commonly acknowledged axioms of set theory. Kurt Gödel in 1938 (the first half of the proof) and Paul Cohen in 1963 proved that one could assume safely (i.e. without contradiction) any of the following "axioms":

$$c = \aleph_1, c = \aleph_2, c = \aleph_3, \ldots \quad .$$

And even (a joke by N. N. Luzin, see Keldysh [1974]): $c = \aleph_{17}$. Thus, the axioms of set theory do not allow determining the exact place of c on the aleph scale, although we can prove that $\exists x(c = \aleph_x)$, i.e. that c "is located" on this scale.

A platonist, looking at the picture of the aleph scale, tries to find the exact place of c ... visually! He cannot imagine a situation when a point is situated on a line, yet it is impossible to determine the exact place. **This is a normal platonism of a working mathematician. It stimulates investigation even in the most complicated fields (usually, we do not know before whether some problem is solvable or not).** Still, if we pass to methodological problems, for example, to the problem of the "meaning" of Cohen's results, we should keep off our platonist habits. Do we think that, in spite of the undecidability of the Continuum Problem "for us, men", some "objective", "real" place for the cardinality of the continuum on the aleph scale does exist? If yes, then we assume something like Plato's world of ideas – some fantastic "true world of sets", that exists independently of the axioms used in the reasoning of mathematicians. At this moment the mathematical platonism (a pure psychological phenomenon) has converted into a kind of philosophy. Such people say that the axioms of set theory do not reflect the "true world of sets" adequately, that we must search for more adequate axioms, and even – that no particular axiom system can represent the "true world of sets" precisely. They pursue a mirage – of course, **no "true world of sets" can exist independently of the principles used in its investigation.**

The real meaning of Cohen's results is, in fact, very simple. We have established that $\exists x(c = \aleph_x)$, yet it is impossible to determine the exact value of x. It means that the traditional set theory is not perfect and, therefore, we may try to improve it. And it appears that one can choose between several possibilities.

For example, we can postulate the **Axiom of Constructibility** (see also Jech [1971], Devlin [1977]). Then we will be able to prove that $c = \aleph_1$, and to solve some other problems that are undecidable in the traditional set theory.

We can postulate also a completely different axiom – the **Axiom of Determinacy** – then we will be forced to reject the Axiom of Choice (in its most general form). As the result, we will be able to prove that every set of

points is Lebesgue-measurable, and that the cardinality of continuum c is incompatible with alephs (except of $\aleph_0$). In this set theory, Continuum Hypothesis can be proved in its initial form: every infinite set of points is either countable or has the cardinality of the continuum.

Both directions (the Axiom of Constructibility and the Axiom of Determinacy) have produced a plentiful collection of beautiful and interesting results. These two set theories are at least as "good" as the traditional set theory, yet they contradict each other, therefore we do not see a convergence to some unique "true world of sets".

Added July 22, 2012.

People working in set theory professionally will not agree with the above conclusion. Their favorite development scenario for set theory is based on the so-called **large cardinal axioms**. For details – see Section 2.4.4.

My main conclusion: **everyday work is permanently moving mathematicians to platonism (and, as a creative method, this platonism is extremely efficient), still, passing to methodology we must reject such a philosophy deliberately**.

Thus, a correct philosophical position of a true mathematician should be:

a) **Platonism – on weekdays** – when I'm doing mathematics (otherwise, my "doing" will be inefficient),

b) **Advanced Formalism** (see below) **– on weekends** – when I'm thinking "about" mathematics (otherwise, I will end up in mysticism).

(For the original version of this aphorism, see Hersh [1979]).

Note. As a regular term, "platonism in mathematics" is used since the lecture delivered June 18, 1934, University of Geneva, by Paul Bernays:

P. Bernays. Sur le platonisme dans les mathematiques. *L'enseignement mathematique*, Vol. 34 (1935), pp. 52-69. Quoted from online English translation by Charles D. Parsons at www.phil.cmu.edu/projects/bernays/Pdf/platonism.pdf).

Bernays considers mathematical platonism as a method that can be – "taking certain precautions" – applied in mathematics. Some remarkable quotes (fragments marked bold by me – K. P.):

... allow me to call it "platonism".

... The value of **platonistically inspired mathematical conceptions** is that they furnish models of abstract imagination. These stand out by their simplicity and logical strength. They form representations which extrapolate from certain regions of experience and intuition.

... This brief summary will suffice to characterize **platonism and its application to mathematics**. This application is so widespread that it is not an exaggeration to say that **platonism reigns today in mathematics**.

... Several mathematicians and philosophers interpret **the methods of platonism** in the sense of conceptual realism, postulating the existence of a world of ideal objects containing all the objects and relations of mathematics. It is this absolute platonism which has been shown untenable by the antinomies, particularly by those surrounding the Russell-Zermelo paradox.

... It is also this transcendent character which requires us to **take certain precautions in regard to each platonistic assumption.** For even when such a supposition is not at all arbitrary and presents itself naturally to the mind, it can still be that the principle from which it proceeds permits only a restricted application, outside of which one would fall into contradiction. We must be all the more careful in the face of this possibility, since the drive for simplicity leads us to make our principles as broad as possible. And the need for a restriction is often not noticed. This was the case, as we have seen, for the principle of totality, which was pressed too far by absolute platonism. Here it was only the discovery of the Russell-Zermelo paradox which showed that a restriction was necessary.

More about the history of the term "mathematical platonism" – see

Jacques Bouveresse. On the Meaning of the Word 'Platonism' in the Expression 'Mathematical platonism'. *Proceedings of the Aristotelian Society*, September 2004, Volume 105, pp. 55-79. Thanks to William J. Greenberg.

1.2. Investigation of Stable Self-contained Models – the True Nature of the Mathematical Method

"The human mind has first to construct forms, independently, before we can find them in things." Albert Einstein.

"It seems that the human mind has first to construct forms independently, before we can find them in things. Kepler's marvelous achievement is a particularly fine example of the truth that knowledge cannot spring from experience alone, but only from the comparison of the inventions of the intellect with observed fact."

English translation by Sonja Bargmann published in: **A. Einstein**. Ideas and Opinions. *Crown Publishers*, New York, 1954, pp. 262-266.

German original: "Es scheint, dass die menschliche Vernunft die Formen erst selbständig konstruieren muss, ehe wir sie in den Dingen nachweisen können. Aus Keplers wunderbarem Lebenswerk erkennen wir besonders schön, dass aus bloßer Empirie allein die Erkenntnis nicht erblühen kann, sondern nur aus dem Vergleich von Erdachtem mit dem Beobachteten."

Full text: Albert Einstein über Kepler. *Frankfurter Zeitung*, 9. November 1930, see also online copy published by Dr. Böttiger-Verlag-GmbH.)

See also Einstein's manuscript of this paper in Einstein Archives Online.

The term "model" will be used below in the sense of applied mathematics, not in the upside-down sense used in mathematical logic. We will discuss models intended to "model" natural processes or technical devices, not sets of formulas.

Following the mathematical approach of solving some (physical, technical etc.) problem, one tries "to escape reality" as fast as possible, passing to investigation of a definite (stable, self-contained) mathematical model. In the process of formulating a model one asks frequently: Can we assume that this dependency is linear? Can we disregard these deviations? Can we assume that this distribution of probabilities is a normal one? One tends (as fast as possible and by using a minimum of postulates) to formulate a mathematical problem, i.e. to model the real situation in some well known mathematical structure (or to create a new structure). By solving the mathematical problem one hopes that, in spite of the simplifications made in the model, (s)he will obtain some solution of the original (physical, technical etc.) problem.

After mathematics appeared as a science, all scientific theories can be divided into two classes:

a) Theories based on developing systems of principles.

b) Theories based on stable systems of principles.

In the process of their development theories of class (a) are enriched with new basic principles that do not follow from the principles acknowledged before. Such principles arise due to fantasy of specialists, supported by more and more perfect experimental data. The progress of such theories is first of all in this enrichment process.

On the other hand, in mathematics, physics and, sometimes, in other branches of science one can find theories, whose basic principles (postulates) do not change in the process of their development. Every change in the set of principles is regarded here as a passage to a new theory. For example, Einsteins's special relativity theory can be regarded as a refinement of the classical mechanics, as a further development of Newton's theory. Still, since both theories are defined very precisely, the passage "from Newton to Einstein" can be regarded also as a passage to a new theory. The evolution of both theories is going on: new theorems are being proved, new methods and algorithms are developed etc. Nevertheless, both sets of basic principles remain constant (such as they were at the lifetime of their creators).

For me, a stable self-contained system of basic principles is the distinctive feature of mathematical theories. A mathematical model of some natural process or a technical device is essentially a stable model that can be investigated independently of its "original" (and, thus, the similarity of the model and the "original" may be only a limited one). Only such models can be

investigated by mathematicians. Any attempt to refine the model (to change its definition in order to obtain more similarity with the "original") leads to a new model that must remain stable again, to enable a mathematical investigation of it.

Hence, mathematical theories are "**the part of science you could continue to do if you woke up tomorrow and discovered the universe was gone**" (I do not know the author of this elegant definition put on the web by Dave Rusin).

Working (in their platonist way!) with stable self-contained models mathematicians have developed their ability to draw a maximum of conclusions from a minimum of premises.

This is why mathematical modeling is so efficient, this is the real source of "The Incomprehensible Effectiveness of Mathematics in the Natural Sciences" (as put by Eugene Wigner) and in technology.

"In mathematics you don't understand things. You just get used to them." (John von Neumann, see Quotations by John von Neumann).

It is very important to note that a mathematical model (because it is stable) is not bound firmly to its "original" source. It may appear that some model is constructed badly (in the sense of the correspondence to its "original" source), yet its mathematical investigation goes on successfully. Since a mathematical model is defined very precisely, it "does not need" its "original" source any more. One can change some model (obtaining a new model) not only for the sake of the correspondence to the "original" source, but also for a mere experiment. In this way people may obtain easily various models that do not have any real "originals". In this way, even entire branches of mathematics have been developed that do not have and cannot have any applications to real problems. **The stable self-contained character of mathematical models makes such "mutants" possible and even inevitable**. No other branch of science knows such problems.

Polish writer Stanislaw Lem joked in his book "Summa Technologiae": **mathematicians are like mad tailors: they are making "all the possible clothes" hoping to make also something suitable for dressing...** (sorry – my own English translation). The initial version of this aphorism may be due to David van Dantzig, see Quotations by David van Dantzig).

The stable self-contained character of mathematical models and theories is simultaneously the force and the weakness of mathematics. **The ability of mathematicians to obtain a maximum of information from a minimum of premises has demonstrated its efficiency in science and technique many times**. Still, the other side of this force is a kind of weakness: **no particular stable self-contained model (theory) can solve all the problems arising in science (or even in mathematics itself).** An excellent confirmation of this

thesis was given in Kurt Gödel's famous incompleteness theorem.

Mathematicians have developed the ability "to live" (literally!) in the world of mathematical concepts and even (while working on some particular problem) – in a very specific "world" of a particular model. Investigation of models is mathematician's goal for goal's sake, during their work they disregard the existence of "realities" behind their models. Here we have **the main source of the creative power of mathematics: in this platonist way, "living" (sometimes, for many years) in the "world" of their concepts and models, mathematicians have developed their ability to draw a maximum of conclusions from a minimum of premises.**

After one has formulated some model, it usually appears that in mathematics some work already has been done on the problem, and some methods and algorithms have been already created. This allows drawing, in real time, of many important conclusions about the model. In this way we usually obtain – relatively quickly – a new useful knowledge about the "original". Clearly, if the model appears so specific that no ready mathematical means can be found to investigate it, the situation becomes more complicated. Either the model is not good enough to represent a really interesting fragment of the "reality" (then we must look for another model), or it is so important that we may initiate investigations to obtain the necessary new mathematical methods.

Have all useful mathematical structures been created in this way, i.e. as a response to real problems external to mathematics? Of course, not: "The human mind has first to construct forms, independently, before we can find them in things." (Albert Einstein). Riemannian geometry and complex Hilbert spaces were invented well before they were used in Einstein's general relativity theory and quantum mechanics. Thus, at least, for the fundamental physics, an **efficient source of the necessary mathematical structures is ... making of "all the possible clothes" (i.e. internal mathematical "mutations")!**

The key to all these powers is the mathematical platonism – the ability of mathematicians to "live" in the "worlds" of the models they are investigating, the ability to forget all things around them during their work. In this way some of them gain the ill fame of being "queer customers", etc. Platonism is, in fact, the **psychology** of working mathematicians, and that it may become a philosophy only from their subjective point of view.

What is Mathematics?

The above-stated picture of the nature of mathematics (I prefere to call it **Advanced Formalism**) is not yet commonly acknowledged. Where is the problem, why it is so hard to look at mathematics as the investigation of stable

self-contained models?

A personal communication by Svyatoslav Sergeevich Lavrov (1923-2004) from 1988: " ... Theorems of any theory consist, as a rule, of two parts – the premise and the conclusion. Therefore, the conclusion of a theorem is derived not only from a fixed set of axioms, but also from a premise that is specific to this particular theorem. And this premise – is it not an extension of the fixed system of principles? ... Mathematical theories are open for new notions. In Calculus, after the notion of continuity the following connected notions were introduced: break points, uniform continuity, Lipschitz's conditions, etc. ... All this does not contradict the thesis about the fixed character of principles (axioms and rules of inference), yet it does not allow "working mathematicians" to regard mathematical theories as fixed ones."

"When the working mathematician speaks of axioms, he or she usually means those for some particular part of mathematics such as groups, rings, vector spaces, topological spaces, Hilbert spaces and so on... They are simply definitions of kinds of structures which have been recognized to recur in various mathematical situations. I take it that the value of these kinds of **structural axioms** for the organization of mathematical work is now indisputable." (Feferman [2000]).

Of course, the fixed character of the **fundamental axioms** (discussed above) does not restrict the diversity and complexity of mathematical structures that can be introduced by various structural axioms.

The mathematical method is (by definition) investigation of stable self-contained models. What is, then, mathematics itself?

The first (trivial) idea: models can be more or less general. Let us compare, for example, arithmetic of natural numbers, Einstein's general relativity theory and some specific model of the Solar system. Very specific models can be investigated more successfully under the management of specialists who are creating and using them. A combination of specific experience with sufficient skills in mathematics (in one person or in a team) will be here the most efficient strategy. **Investigation of general models that can be applied to many different specific models, doesn't it draw up contents of a specific branch of science that is called mathematics?**

For example, Calculus has many applications in various fields and, therefore, it is a striking example of a theory that undoubtedly belongs to mathematics. On the other hand, any model of Solar system (used, for example, for exact prediction of eclipses) is too specific to be encountered as a part of mathematics (although it is surely a mathematical model).

The second idea could be inspired by the following concept proposed by Sergei Yu. Maslov on two kinds of modeling activities:

a) "left-hemispherical" activities – working in a fixed formal theory (on a fixed mathematical structure),

b) "right-hemispherical" activities – changing a theory/structure (or, inventing a new one).

S. Yu. Maslov. Asymmetry of cognitive mechanisms and its consequences. *Semiotics and information science*, N20, pp.3-31, Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Informatsii, Moscow, 1983 (in Russian).

S. Yu. Maslov. Theory of deductive systems and its applications. With a foreword by Nina B. Maslova. Translated from the Russian by Michael Gelfond and Vladimir Lifschitz. MIT Press Series in the Foundations of Computing. MIT Press, Cambridge, MA-London, 1987, xii+151 pp.

Thus, according to this approach, the above conclusion that stable self-contained system of basic principles is the distinctive feature of mathematical theories, can be regarded only as the first step in discovering the nature of mathematics. Without the next step, we would end up by representing mathematics as an **unordered heap** of mathematical theories!

But, in fact, mathematics is a complicated **system** of interrelated theories each representing some significant mathematical structure (for example, natural numbers, real numbers, sets, groups, fields, algebras, all kinds of spaces, graphs, categories, computability, all kinds of logic, etc.).

Thus, in a sense, **we should think of mathematics as a "two-dimensional" activity.** Sergei Yu. Maslov could have put it as follows: **most of a mathematician's working time is spent along the first dimension (working in a fixed mathematical theory, on a fixed mathematical structure), but, sometimes, (s)he needs also moving along the second dimension (changing his/her theories/structures or, inventing new ones).**

And thus, "Elements de Mathematique" by Nicolas Bourbaki can be regarded as an attempt of a systematic treatment of the second dimension of mathematics.

Do we need more than this, to understand the nature of mathematics?

1.3. Intuition and Axioms

The stable character of mathematical models and theories is not always evident – because of our platonist habits (we are used to treat mathematical objects as a specific "world"). Very few people will dispute the stable character of a fully axiomatic theory. All principles of reasoning, allowed in such

theories, are presented in axioms explicitly. The principal basis is fixed, and any changes in it will mean explicit changes in axioms.

Could we regard as fixed also those theories that are not fully axiomatic yet? How could it be possible? For example, all mathematicians are unanimous about the ways of reasoning that allow us to prove theorems about natural numbers (other ways yield only hypotheses or errors). Still, most mathematicians do not use, and even do not know the axioms of arithmetic! And even in those theories that seem to be completely axiomatic (as, for example, geometry in Euclid's "Elements") one can find aspects of reasoning that are commonly acknowledged as correct, yet are not presented in axioms. For example, imagine, a triangle ABC and a line that intersects the side AB and does not pass through C. Then this line must intersect either the side AC, or BC. In 1882 Moritz Pasch showed that this conclusion does not follow from Euclid's axioms, and introduced it as a new axiom (now called Pasch's Axiom). Still, until that time mathematicians somehow managed to treat the situation in a uniform way without this axiom...

Trying to explain this phenomenon, we are led to the concept of **intuition**. Intuition is treated usually as "creative thinking", "direct obtaining of truth", etc. I'm interested here in a much more prosaic aspect of intuition.

The human brain is a very complicated system of processes. Only a small part of these electrochemical fireworks can be controlled consciously. Therefore, similar to the thinking processes going on at the conscious level, there must be a much greater amount of thinking processes going on at the unconscious level. Experience shows that when the result of some unconscious thinking process is very important for the person, it (the result) can be sometimes recognized at the conscious level. The process itself remains hidden, for this reason, the effect seems like "direct obtaining of truth" (see Poincare [1908], Hadamard [1945]).

Since unconscious processes yield not only arbitrary dreams, but also (sometimes) reasonable solutions of real problems, there must be some "reasonable principles" governing them. When working in real mathematical theories our reasoning is governed by such unconscious "reasonable principles" − together with axioms or without any axioms. **Relatively closed sets of unconscious "ruling principles" represent the most elementary type of intuition used in mathematics.**

See also David G. Myers: Intuition: Its Powers and Perils (Yale U. Press, September 2002).

We can say, therefore, that **a theory (or model) can be stable not only due to some set of axioms, but also due to a specific intuition.** We can speak about intuition of natural numbers that determines our reasoning about these numbers, and about "Euclidean intuition" that makes the usual geometry

completely definite, though Euclid's axioms do not contain many essential principles of geometric reasoning.

How could we explain the emergence of intuitions that are governing uniformly the reasoning of so many different people? It seems that they can arise because human beings all are similar to each other, because they deal with approximately the same external world, and because in the process of education, practical and scientific work they tend to accordance with each other.

While investigations are going on, people arrive at a level of complexity where the degree of definiteness of intuitive models is already insufficient. Then various conflicts between specialists may appear about the ways of reasoning which could be accepted, and which should not. It may happen even that commonly acknowledged ways of reasoning lead to absurd conclusions...

In the history of mathematics, such situations appeared several times: the crash of the discrete geometric intuition after the discovery of incommensurable magnitudes (VI century BC), problems with negative and complex numbers (up to the end of XVIII century), the dispute between Leonhard Euler and Jean d'Alembert on the concept of function (XVIII century), groundless operation with divergent series (up to the beginning of XIX century), problems with the acceptance of Cantor's set theory, paradoxes in set theory (the end of XIX century), the controversy around the Axiom of Choice (the beginning of XX century). All that was caused by the inevitably uncontrollable nature of unconscious thinking processes. It seems that "ruling principles" of these processes are picked up and fastened by something like a "natural selection" which is not able to a far-reaching co-ordination without making errors. Therefore, the appearance of (real or imagined) paradoxes in intuitive theories is not surprising.

The defining intuition of a theory does not always remain constant. Frequent changes happen during the beginning period, when the intuition (as the theory itself), is not yet stabilized. During this, the most delicate period of evolution, the most intolerant conflicts may appear. The only reliable exit from such situations – we must convert the unconscious ruling "principles" into conscious ones and then investigate their accordance with each other. If this conversion were meant in a literal sense, it would be impossible, since we cannot know the internal structure of a specific intuition. We can speak here only about a **reconstruction** of a "black box" in some other – explicit – terms. Two different approaches are usually applied for such reconstruction: the so-called genetic method and the axiomatic method.

The **genetic method** tries to reconstruct intuition by means of some other theory (which can also be intuitive). Thus, a "suspicious" intuition is modeled, using a "more reliable" one. For example, in this way the objections against

the use of complex numbers were removed: complex numbers were presented as points of a plane (or, as pairs of real numbers). In this way even their strangest properties (as, for example, the infinite set of values of *log x* for a negative *x*) were converted into simple theorems of geometry. In a similar way problems with the basic concepts of Calculus (limit, convergence, continuity, etc.) were cleared up – through their definition in terms of epsilon-delta.

It appeared, however, that after the reconstruction in terms of epsilon-delta, some of these concepts, obtained unexpected properties the were missing in the original intuitive concepts. For example, it was believed that every continuous function of a real variable is differentiable almost everywhere, except at some relatively isolated "break-points". But after the concept of a continuous function was redefined in terms of epsilon-delta, it appeared that a continuous function could be constructed, which is *nowhere* differentiable (the famous construction by Karl Weierstrass).

The appearance of unexpected properties in reconstructed concepts means that here, indeed, we have a reconstruction – not a direct "copying" of intuitive concepts, and that we must consider the problem seriously: is our reconstruction adequate?

The genetic method clears up one intuition in terms of another one, i.e. it is working relatively. The **axiomatic method**, conversely, is working "absolutely": among the commonly acknowledged assertions about objects of a theory some subset is selected, and the assertions from this subset are called axioms, i.e. they are acknowledged as true without proofs. All the other assertions of the theory must be proved by using axioms. These proofs may contain intuitive moments that must be "more evident" than the ideas presented in axioms. The most famous applications of the axiomatic method: Euclid's axioms, Hilbert's axioms of Euclidean geometry, Peano axioms of arithmetic of natural numbers, Zermelo-Fraenkel axioms of set theory.

The axiomatic method (as well as the genetic method) yields only a reconstruction of intuitive concepts. The problem of adequacy can be reduced here to the question: are all the essential properties of the intuitive concepts under question presented in axioms? From this point of view the most complicated situation appears, when axioms are used to rescue some theory which had "lost its way" in paradoxes. Zermelo-Fraenkel's axioms were developed exactly in such a situation – after paradoxes appeared in the intuitive set theory. The problem of adequacy is here especially complicated: are all the **positive** contents of the theory saved?

What criteria can be set for the adequacy of a reconstruction? Let us recall various definitions of real numbers concept in terms of rational numbers, presented in the 1870s simultaneously by Richard Dedekind, Georg Cantor and some others. Why do we regard these reconstructions as satisfactory? And

how can the adequacy of a reconstruction be justified when the original concept remains hidden in the intuition and every attempt to “get it out” is a reconstruction itself with the same problem of adequacy? The only possible realistic answer is: **take into account only those aspects of intuitive concepts that can be recognized in the practice of mathematical reasoning**. It means, first, that all properties of real numbers, acknowledged before as "evident", must be provable on the basis of the reconstructed concept. Secondly, all intuitively proven theorems of Calculus must be provable by means of the reconstructed concept. If this is done, it means that those aspects of the intuitive concept of real number that managed to appear in the mathematical practice, all are explicitly presented in the reconstructed concept. Still, maybe, some "hidden" aspects of the intuitive real number concept have not yet appeared in practice, but they will appear in future? At first glance, it seems hard to dispute such an objection.

However, let us suppose that this is the case, and in 2150 somebody will prove a new theorem of Calculus using a property of real numbers, never before used in mathematical reasoning. And then, will all the other mathematicians agree immediately that this property was "intended" already in 2000? At least, it will be impossible to verify this proposition: none of the mathematicians of 2000 will survive 150 years.

By admitting that intuitive mathematical concepts can possess some "hidden" properties that do not appear in practice for a long time, we fall into the usual mathematical platonism (i.e. we assume that the "world" of mathematical objects exists independently of mathematical reasoning).

Still, let us consider

Freiling's Axiom of Symmetry (1986). Let A be the set of functions mapping Real Numbers into countable sets of Real Numbers. Given a function $f \in A$, and some arbitrary real numbers x and y, we see that $x \in f(y)$ with probability 0, i.e. $x \notin f(y)$ with probability 1. Similarly, $y \notin f(x)$ with probability 1. Freiling's axiom AX states: "for every f in A, there exist x and y such that $x \notin f(y)$ and $y \notin f(x)$ ". An intuitive justification: we can find such x and y by choosing them at random. In ZFC, **AX is equivalent to "not CH"**, i.e. neither AX, nor "not AX" can be derived from the axioms of ZFC. Do you think AX is a counter-example for the previous thesis? I.e. does AX reveal a "hidden" property of real numbers that did not appear in the mathematical practice until 1986, and that implies that CH is “obviously” false?

Christopher F. Freiling. Axioms of Symmetry: Throwing Darts at the Real Line", *Journal of Symbolic Logic*, Vol. 51, 1986, pp 190-200. (See also: Devlin's Angle, June 2001)

Exercise 1.0 (for smart students, return here after studying Section 2.4.1). In the (x, y)-plane, “horizontal line” is defined as any function y=f(x) from reals into reals. And “vertical line” is defined as any function x=f(y) from reals into reals. BX is the following claim: there is a *countable* set A of horizontal lines, and a *countable* set B of vertical lines such that the union $A \cup B$ covers the entire (x, y)-plane. Verify that BX is equivalent to CH. (Hint: for the

necessary ideas, see Freiling's Axiom of Symmetry in Wikipedia.)

Now, following Freiling's argument, consider throwing darts at the unit square [0, 1]x[0, 1]. Assume BX. Does your intuition say that the probability of hitting a particular line is 0? Then, the probability of hitting a line in the (countable!) set A is 0, and the probability of hitting a line in the (countable!) set B is 0 as well. But the probability of hitting a line in the union $A \cup B$ is 1! Contradiction. Hence, BX (and CH) is "obviously" false?

Not at all! The probability of hitting a line in the union $A \cup B$ is 1, indeed. But it's not true that the probability of hitting a particular line is 0! Some of the lines are non-measurable! So, that's your intuition that should be abandoned, not CH. And Freiling's argument does not reveal a "hidden" property of real numbers that did not appear in the mathematical practice until 1986. The paradoxicality of this argument returns us to a similar kind of intuition that all sets of real numbers are Lebesgue measurable. In 1905, Giuseppe Vitali proved, assuming the Axiom of Choice, that there exist non-measurable sets of real numbers.

For an in-depth treatment of the problem, see

Joseph Shipman. Cardinal conditions for strong Fubini theorems. Trans. Amer. Math. Soc. 321 (1990), 465-481 (available online).

Some of the intuitive concepts allow for several different, yet, nevertheless, equivalent explicit reconstructions. In this way an additional very important evidence of adequacy can be given. Let us recall, again, the various definitions of real numbers in terms of rational numbers. Cantor's definition was based upon convergent sequences of rational numbers. Dedekind defined real numbers as "cuts" in the set of rational numbers. One definition more can be obtained by using (infinite) decimal fractions. All these definitions are provably equivalent. We cannot prove strongly the equivalence of an intuitive concept and its reconstruction, yet we can prove – or disprove – the equivalence of two explicit reconstructions.

Another striking example is the reconstruction of the intuitive notion of computability (the concept of algorithm). Since 1930s several very different explicit reconstructions of this notion were proposed: recursive functions, Turing machines by A. M. Turing, the lambda-calculus by A. Church, canonical systems by E. Post, normal algorithms by A. A. Markov, etc. And here, too, the equivalence of all reconstructions was proved.

The equivalence of different reconstructions of the same intuitive concept means that the volume of the reconstructed explicit concept is not accidental. This is a very important additional argument for replacing of the intuitive concept by an explicit reconstruction.

The trend to replace intuitive concepts by their more or less explicit reconstructions appears in the history of mathematics very definitely. Intuitive theories cannot be developed without such reconstructions normally: the definiteness of intuitive basic principles becomes insufficient when the

complexity of concepts and methods is growing. In most situations the reconstruction can be performed by the genetic method, yet to reconstruct the most fundamental mathematical concepts the axiomatic method must be used (fundamental concepts are called fundamental just because they cannot be reduced to other concepts).

Gödel's incompleteness theorem has provoked very much talking about insufficiency of the axiomatic method for a true reconstruction of the "live, informal" mathematical thinking. Some people declare that axioms are not able to cover "all the treasures of the informal mathematics". Of course, it is once again the usual mathematical platonism converted into a methodological one (for a detailed analysis see Podnieks [1981, 1992], or Section 6.1 below).

Does the "axiomatic reasoning" differ in principle from the informal mathematical reasoning? Do there exist proofs in mathematics obtained by not following the pattern "premises – conclusion"? If not, and hence, every mathematical reasoning process can be reduced to a chain of conclusions, we may ask: are these conclusions going on by some definite rules that do not change from one situation to another? And, if these rules are definite, can they (being a function of human brains) be such that a complete explicit formulation of them is impossible? If we cannot formulate some "rules" explicitly, then how could we demonstrate that they are definite?

Therefore, **it is a nonsense to speak about the limited applicability of axiomatization: the limits of axiomatization coincide with the limits of mathematics itself! Gödel's incompleteness theorem is an argument against platonism, not against formalism! Gödel's theorem demonstrates that no advanced, stable and self-contained fantastic "world of ideas" can be perfect. Any advanced, stable and self-contained "world of ideas" leads either to contradictions or to undecidable problems.**

In the process of evolution of mathematical theories, axioms and intuition interact with each other. Axioms "clean up" the intuition when it loses its way. Still, axiomatization has also some unpleasant consequences: many steps of intuitive reasoning, represented by a specialist very compactly, appear very long and tedious in an axiomatic theory. Therefore, after replacing an intuitive theory by an axiomatic one (this replacement may be non-equivalent because of the defects discovered in the intuitive theory), specialists develop a new intuition. In this way they restore the creative powers of their theory. Let us recall the history of the axiomatization of set theory. In 1890s contradictions were discovered in Cantor's intuitive set theory, and they were removed by means of axiomatization. Of course, the axiomatic Zermelo-Fraenkel's set theory differs from Cantor's intuitive theory not only in its form, but also in some aspects of contents. But specialists have developed new, modified intuitions (for example, the intuition of sets and proper classes) that allow

them to work in the new theory efficiently. People are proving serious theorems of set theory non-formally, again.

What are the main benefits of axiomatization? First, as we have seen, axioms allow correcting of intuition: remove inaccuracies, ambiguities and paradoxes that arise sometimes due to the insufficient controllability of intuitive thinking.

Secondly, axiomatization allows a detailed analysis of relations between the basic principles of a theory (to establish their dependency or independence, etc.), and between the principles and theorems (to prove a particular theorem only a part of the axioms may be necessary). Such investigations may lead to general theories that can be applied to several more specific theories (let us recall theory of groups, rings, fields etc).

Thirdly, sometimes, after the axiomatization, we can establish that the theory under consideration is not able to solve some of the problems naturally arising in it (let us recall the Continuum Problem in set theory). In such situations we may try to improve the axioms of theory, even – by developing several alternative theories.

1.4. Formal Theories

How far can we proceed with the axiomatization of some theory? Complete elimination of intuition, i.e. full reduction to a list of axioms and rules of inference, is this possible? The work by Gottlob Frege, Charles S. Peirce, Bertrand Russell, David Hilbert and their colleagues showed how this could be achieved even with the most complicated mathematical theories. All theories can be reduced to axioms and rules of inference without any admixture of intuition. Logical techniques developed by these people allow us today complete axiomatization of any theory based on stable, self-consistent systems of principles (i.e. of any mathematical theory).

What do they look like – such 100% axiomatic theories? They are called **formal theories** (formal systems or deductive systems) – to emphasize that no step of reasoning can be done without a reference to an exactly formulated list of axioms and rules of inference. Even the most "self-evident" logical principles (like, "if *A* implies *B*, and *B* implies *C*, then *A* implies *C*") must be either formulated in the list of axioms and rules explicitly, or derived from it.

The most general exact definition of the "formal" can be given in terms of theory of algorithms: ***T* is called a formal theory, if and only if two algorithms (i.e. a mechanically applicable computation procedures) are presented:**

The first algorithm – for checking correctness of propositions according to the principles of T. This algorithm defines the **formal language**, on which T is based. Among all the possible character strings, it separates correct propositions of T.

The second algorithm – for checking correctness of reasoning according to the principles of *T*. This algorithm defines the notion of **formal proof**, which is used in T. When somebody is going to publish a "mathematical text" calling it "a proof of a theorem in *T*", then we must be able to check mechanically whether the text in question really is a proof according to the standards of reasoning accepted in *T*. Thus, in formal theories, the standards of reasoning must be defined precisely enough to enable checking of proofs by means of a computer program. (Note that we are discussing here **checking of ready proofs**, and not the much more complicated problem – is some proposition provable in T, or not.)

As an impractical example of a formal theory let us consider the game of chess, let us call this "theory" *CHESS*.

The **"language"** of *CHESS* consists of the following **"propositions"**: all the possible positions on a chessboard (plus one the flags: "whites to move" or "blacks to move")**.**

The only **"axiom"** of *CHESS*: the initial position.

Rules of "inference" of *CHESS*: the rules of the game.

The rules allow passing from one proposition of *CHESS* to some other ones. Starting with the axiom we obtain in this way **"theorems"** of *CHESS*. Thus, theorems of *CHESS* are all the possible positions that can be obtained from the initial position by moving chessmen according to the rules of the game.

Exercise 1.1. Could you provide an **unprovable** proposition of *CHESS*?

Why is *CHESS* called a formal theory? When somebody offers a "mathematical text" *P* as a proof of a theorem *A* in *CHESS*, it means that *P* is a record of some chess-game stopped in the position *A*. And, of course, checking the correctness of such a "proof" is an easy task. Rules of the game are formulated precisely enough – we could write a computer program that will execute the task.

Exercise 1.2. Try estimating the size of this program in some programming language.

Our second example of a formal theory is only a bit more serious. It was proposed by Paul Lorenzen, let us call this theory *L*. The language of L consists of the following propositions: all the possible "words" made of letters *a, b,* for example: *a, aa, aba, baab*. The only axiom of *L* is the word *a*, and *L* has two rules of inference:

$$\frac{X}{Xb}, \frac{X}{aXa} \quad .$$

It means that (in *L*) from a proposition *X* we can infer immediately the propositions *Xb* and *aXa*. For example, the proposition *aababb* is a theorem of *L*:

a |- *ab* |- *aaba* |- *aabab* |- *aababb*
rule1 rule2 rule1 rule1

This fact is expressed usually as *L* |- *aababb* ("L proves *aababb*").

Exercise 1.3. a) Describe an algorithm determining whether a proposition of *L* is a theorem or not.

b) Could you imagine such an algorithm for *CHESS*? Of course, you can, yet... Thus you see that even, having a relatively simple algorithm for checking of correctness of proofs, the problem of provability may be a very complicated one.

Very important property of formal theories is given in the following

Exercise 1.4. (for smart students) Show that the set of all theorems of a formal theory is computably enumerable (synonyms – effectively enumerable, “recursively enumerable”, listable).

Thus, for any formal theory, one can write a computer program that will print on an (endless) paper tape all theorems of this theory (and nothing else). Unfortunately, **such a program cannot solve the problem that the mathematicians are mainly interested in: is a given proposition provable or not?** When we see our proposition printed, it means that it is provable. Still, until that moment we cannot know whether the proposition will be printed some time later or it will not be printed at all.

T is called a **solvable theory** (or, computably solvable, or "recursive"), if and only if an algorithm (mechanically applicable computation procedure) is presented for checking whether some proposition is provable by using principles of *T,* or not. In Exercise 1.3a you proved that *L* is a solvable theory. Still, in Exercise 1.3b you established that it is hard to state whether *CHESS* is a "feasibly solvable" theory or not. Checking correctness of proofs is always much simpler than determining of provability. It can be proved that **most serious mathematical theories are unsolvable**, the elementary (first order) arithmetic of natural numbers and set theory included (see, for example, Mendelson [1997], or click here).

Normally, mathematical theories contain the negation symbol ***not***. In such theories solving the problem stated in a proposition *A* means to prove either *A* or ***not****A*. We can try to solve the problem by using the enumeration program of

Exercise 1.4: let us wait until *A* or ***not****A* is printed. If *A* and ***not****A* would be printed both, this would mean that *T* is an **inconsistent theory** (i.e. by using the principles of *T* one can prove some proposition and its negation). In total, we have here 4 possibilities:

a) *A* will be printed, but ***not****A* will not (then the problem *A* has a positive solution),

b) ***not****A* will be printed, but *A* will not (then the problem *A* has a negative solution),

c) *A* and ***not****A* will be printed both (then *T* is an inconsistent theory),

d) neither *A*, nor ***not****A* will be printed.

In the case d) we will be waiting forever, yet nothing interesting will happen: by using the principles of *T* one can neither prove nor disprove the proposition *A*. For this reason such a theory is called an **incomplete theory**. Gödel's incompleteness theorem says that **most serious mathematical theories are inconsistent or incomplete** (see Mendelson [1997] or click here).

Exercise 1.5. (for smart students) Show that a complete formal theory is solvable.

1.5. Hilbert's Program

At the beginning of XX century the honor of mathematics was questioned seriously – in set theory, contradictions were detected. Until that time set theory was acknowledged widely as a natural foundation and a very important tool of mathematics. In order to save the honor of mathematics David Hilbert proposed his famous program of "perestroika" in the foundations of mathematics:

a) Convert all the existing (mainly intuitive) mathematics into a formal theory (a new variant of set theory cleared of paradoxes included).

b) Prove the consistency of this formal theory (i.e. prove that no proposition can be proved and disproved in it simultaneously).

Solving the task (a) – it was meant simply to complete the axiomatization of mathematics. This process proceeded successfully in XIX century: formal definition of the notions of function, continuity, real numbers, axiomatization of arithmetic, geometry etc.

The task (b) – contrary to (a) – was a great novelty: try to obtain **an absolute consistency proof of mathematics**. Hilbert was the first to realize that a

complete solution of the task (a) enables one to set the task (b). Really, if we have not a complete solution of (a), i.e. if we are staying partly in the intuitive mathematics, then we cannot discuss absolute proofs of consistency. We may hope to establish a contradiction in an intuitive theory, i.e. to prove some proposition and its negation simultaneously. But we cannot hope to prove the consistency of such a theory: consistency is an assertion about the set of all theorems of the theory, i.e. about the set, an explicit definition of which we do not have in the case of an intuitive theory.

If a formal theory replaces the intuitive one, then the situation is changed. The set of all theorems of a formal theory is an explicitly defined object. Let us recall our examples of formal theories.

The set of all theorems of *CHESS* is (theoretically) finite, yet from a practical point of view it is rather infinite. Nevertheless, one can prove easily the following assertion about *all* theorems of *CHESS*:

In a theorem of *CHESS,* one cannot have a white pawn on line 1.

Indeed, by the rules of the game, white pawns start on line 2 and are allowed to move forward only. Thus, we have selected some specific properties of axioms and inference rules of *CHESS* that imply our general assertion about all theorems of *CHESS*.

With theory *L* we have similar opportunities. One can prove, for example, the following assertion about *all* theorems of *L*: if *X* is a theorem, then *aaX* also is a theorem.

Indeed, if *X* is axiom (*X=a*), then *L* |- *aaX* by rule2. Further, if for some *X*: *L* |- *aaX*, then we have the same for *X′=Xb* and *X″=aXa*:

aaX |- *aa(Xb)*, *aaX* |- aa*(aXa)*
rule1 rule2

Thus, by the induction principle (Attention! Henri Poincare, see below!), our assertion is proved for any theorem of *L*.

Hence, **if the set of theorems is defined precisely enough, one can prove general assertions about all theorems.** Hilbert thought that consistency will not be an exception, i.e. he regarded consistency as a kind of "combinatorial property" of axiom systems. Roughly, his hope was selecting of those specific properties of the axiom system of the entire mathematics that make the deduction of contradictions impossible.

Let us recall, however, that **the set of all theorems is here infinite, and, therefore, consistency cannot be verified empirically. We may only hope to establish it by means of some theoretical proof.** For example, we proved our assertion:

$$L \vdash X \rightarrow L \vdash aaX$$

by using the induction principle. What kind of **theory** must be used to prove the consistency of the entire mathematics? Clearly, the means of reasoning used for proving the consistency of some theory *T* must be more reliable than the means of reasoning used in *T* itself. How could one rely on a consistency proof when suspicious means were used in it? Still, if a theory *T* contains the entire mathematics, then we (mathematicians) cannot know any means of reasoning outside of *T*. Hence, proving the consistency of such a universal theory *T* we must use means from *T* itself – from the most reliable part of them.

There are two extreme levels of "reliability" in mathematics:

1) Arithmetical ("discrete") reasoning – only natural numbers (or similar discrete objects) are used.

2) Set-theoretical reasoning – Cantor's concept of arbitrary infinite sets is used.

The first level is regarded as reliable (only few people will question it), and the second one – as still suspicious (Cantor's set theory was cleared of contradictions, still...). Of course, (roughly) Hilbert's intention was to prove the consistency of mathematics by means of the first level.

As soon as Hilbert announced the initial version of his project in a series of papers and lectures given between 1900 and 1905, Henri Poincare expressed serious doubts about its feasibility (see Poincare [1908], Volume II, Chapter IV). He pointed out that by proving the consistency of arithmetical axioms by using the induction principle (the main tool of the first level) Hilbert would fall into *petitio principii* (**circular argument**): the consistency of arithmetical axioms means also consistency of the induction principle ... proved by means of the induction principle! At that time few people could realize the real significance of this criticism... (Brouwer [1912] was one of the few exceptions). Still, in 1930 Kurt Gödel proved that Poincare was right: **an absolute consistency proof of essential parts of mathematics is impossible!** (For details see Section 5.4 below)

1.6. Some Replies to Critics

1. I do not believe that the natural number system is an inborn property of human mind. I think that it was developed from human practice – from the operation with collections of discrete objects. Therefore, both – the properties of discrete collections from human practice and the structure of human mind,

influenced the particular form of our present natural number system. If so, how long was the development process of this system and when was it completed? I think that the process ended in VI century BC, when the first results were obtained about the natural number system as the whole (for example, theorem about infinity of primes). In human practice, only relatively small sets can appear (and following the modern cosmology we believe that only a finite number of particles can be found in the Universe). Hence, results about "natural number infinity" can be obtained in a **theoretical** model only. If we believe that general results about natural numbers can be obtained by means of pure reasoning, without any additional experimental practice, it means that we are convinced that our theoretical model is stable, self-contained and (sufficiently) complete.

2. (See Sections 5.4, 6.5 and Appendix 2 for details) The development process of mathematical concepts does not yield a continuous spectrum of concepts, yet a relatively small number of different concepts (models, theories). Thus, considering the history of natural number concept we see two different stages only. Both stages can be described by the corresponding formal theories:

– Stage 1 (VI century BC – 1870s) can be described by first order arithmetic,

– Stage 2 (1870s – today) can be described by arithmetic of ZFC.

I think that the natural number concept of Greeks corresponds to first order arithmetic and that this concept remained unchanged up to 1870s. I believe that Greeks would accept any proof from the so-called elementary number theory of today. Cantor's invention of "arbitrary infinite sets" (in particular, "the set of all sets of natural numbers", i.e. $P(w)$) added new features to the old ("elementary") concept. For example, the so-called Extended Ramsey's theorem became provable. Thus a new model (Stage 2) replaced the model of Stage 1, and it remains principally unchanged up to day.

Finally, let us consider the history of geometry. The invention of non-Euclidean geometries could not be treated as a "further development" of the old Euclidean geometry. Still, Euclidean geometry ifself remains unchanged up to day, and we can still prove new theorems using Euclid's axioms. Non-Euclidean geometries appeared as a new theories, different from the Euclidean one, and they also remain unchanged up to day.

Therefore, I think, I can retain my definition of mathematics as investigation of stable self-contained models that can be treated, just because they are stable and self-contained, independently of any experimental data.

3. I do not criticize platonism as the philosophy (and psychology) of working mathematicians. On the contrary, as a creative method, platonism is extremely efficient in this field. Platonist approach to "objects" of investigation is a necessary aspect of the mathematical method. Indeed, how can one investigate

effectively a **stable self-contained** model – if not thinking about it in a platonist way (as the "last reality", without any experimental "world" behin it)?

4. By which means do we judge theories? My criterion is pragmatic (in the worst sense of the word). If, in a theory, contradictions have been established, then any new theory will be good enough, in which main theorems of the old theory (yet not its contradictions) can be proved. In such a sense, for example, ZFC is "better" than Cantor's original set theory.

On the other hand, if, in a theory, undecidable problems appear (as Continuum Problem appeared in set theory), then any extension of the theory will be good enough, in which some of these problems can be solved in a positive or a negative way. Of course, simple postulation of the desired positive or negative solutions leads, as a rule, to uninteresting theories. We must search for more powerful hypotheses, such as, for example, "V=L" (Axiom of Constructibility), or AD (Axiom of Determinacy). Theories ZF+"V=L" and ZF+AD contradict each other, yet they both appear very interesting, and many people make beautiful investigations in each of them.

If some people are satisfied neither with "V=L", nor with AD, they can suggest any other powerful hypothesis having rich and interesting consequences. I do not believe that here any convergence to some unique (the "only right") system of set theory can be expected.

5. Mathematicians are not in agreement about the ways to prove theorems, yet their opinions do not form a continuous spectrum. The existing few variations of these views can be classified; each of them can be described by means of a suitable formal theory. Thus they all can be recognized as "right" ones, and we can peacefully investigate their consequences.

6. I think that the genetic and axiomatic methods are used in mathematics not as heuristics, and not to prove theorems. These methods are used to clarify intuitive concepts that appear insufficiently precise, and, for this reason, investigations cannot be continued normally.

The most striking application of the genetic method is, I think, the definition of continuous functions in terms of epsilon-delta. The old concept of continuous functions (the one of XVIII century) was purely intuitive and extremely vague, so that one could not prove theorems about it. For example, the well known theorem about zeros of a function f continuous on $[a, b]$ with $f(a)<0$ and $f(b)>0$ was believed to be "obvious". It was believed also that every continuous function is almost everywhere differentiable (except of some isolated "break points"). The latter assertion could not be even stated precisely. To enable further development of the theory a reconstruction of the intuitive concept in more explicit terms was necessary. Cauchy did this in terms of

epsilon-delta. Having such a precise definition, the "obvious" theorem about zeros of the above function *f* needs already a serious proof. And it was proved. The Weierstrass's construction of a continuous function (in the sense of the new definition) that is nowhere differentiable shows unexpectedly that the volumes of the old (intuitive) and the new (more explicit) concept are somewhat different. Nevertheless, it was decided that the new concept is "better", and it replaced the old intuitive concept of continuous functions.

In a similar way, the genetic method was used many times in the past. The so-called "arithmetization of Calculus" (definition of real numbers in the terms of natural numbers) also is an application of the genetic method.

7. Our usual metatheory used for investigation of formal theories (to prove Gödel's theorems etc.) is theory of algorithms (recursive functions). It is, of course, only a theoretical model giving us a somewhat deformed picture of how are real mathematical theories functioning. Perhaps, the "sub-recursive mathematics" will provide more adequate picture of the real processes (see, for example, Parikh [1971]).

2. Axiomatic Set Theory

For a general overview and set theory links, see Set Theory by Thomas Jech in Stanford Encyclopedia of Philosophy.

2.1. The Origin of Cantor's Set Theory

In the dates and facts of the real history I am following the excellent books by Fyodor Andreevich Medvedev (1923–1993):

F. A. Medvedev. Development of Set Theory in XIX Century. Nauka Publishers, Moscow, 1965, 350 pp. (in Russian)

F. A. Medvedev. The Early History of the Axiom of Choice. Nauka Publishers, Moscow, 1982, 304 pp. (in Russian)

See also:

Online paper "A history of set theory" in the MacTutor History of Mathematics archive.

A. Kanamori. Set Theory from Cantor to Cohen, *Bulletin of Symbolic Logic,* 1996, N2, pp.1-71 (available online).

In XIX century, development process of the most basic mathematical notions led to the intuition of arbitrary infinite sets. Principles of the past mathematical thinking were developed up to their logical limits. Georg Cantor did the last step in this process, and this step was inspired by a specific mathematical problem.

G. Cantor. Über die Ausdehnung eines Satzes aus der Theorie der trigonometrischen Reihen. "Mathematische Annalen", 1872, Vol. 5, pp. 123-132 (available online, see also online comments by Stanley N. Burris).

In this 1872 paper Cantor proved the following theorem: if two Fourier series are known converging to identical limit values at **all but a finite number of points** of the segment $[-\pi, \pi]$, then these series (i.e. their respective coefficients) are identical. How far could be this theorem extended?

Cantor started with the simplest kinds of infinite sets of exception points, for example:

$$\{\frac{1}{n} | n \geq 1\} \quad .$$

This set is infinite, it possess only one the so-called condensation point (namely, x=0). Cantor succeeded in proving that his theorem holds, if the set of exceptions possess only one condensation point. The generalization to any

finite number of condensation points is then straightforward.

The next step would be considering sets having infinitely many condensation points. The most simple kind of such sets possess exactly one "second order" condensation point, i.e. the condensation point for the usual ("first order") condensation points, for example:

$$\{\frac{1}{m}+\frac{1}{n}|m,n\geq 1\} \quad .$$

Cantor succeeded in proving his theorem for such sets of exceptions, too. The following step would involve the "third order" condensation points etc. In this way Cantor was forced to work with sets of points of rapidly growing complexity. Thus, gradually, the intuitive notion of an “arbitrary infinite set” of points began taking shape...

To bring some order into the process Cantor introduced the notion of the **derivative set**: if P is a set of points, then P' denotes the set of all condensation points of P. Further one can define P" as (P')', P"' – as (P")' etc.

Exercise 2.1 (optional). For any fixed k≥1, let us consider the set

$$Q(k)=\{\frac{1}{n_1}+\ldots+\frac{1}{n_k}|n_{1,}\ldots,n_k\geq 1\} \quad .$$

Prove that the k-th derivative set $Q^k(k) = \{0\}$.

Cantor generalized successfully his Fourier series uniqueness theorem for exception sets of any finite order (i.e. for sets P having a finite P^k for some k).

In this way, investigating Fourier series, and having built a plentiful collection of complicated infinite sets of points, Cantor came to the intuition of an “arbitrary infinite set”. And, at some moment he arrived to the question: have all infinite sets equal "number" of members?

This critical point was reached in the fall of 1873. Cantor's letter to Richard Dedekind from September 29, 1873 contains the surprising one-to-one correspondence between natural and positive rational numbers:

$$\frac{1}{1};\frac{1}{2};\frac{2}{1};\frac{1}{3};\frac{3}{1};\frac{1}{4};\frac{2}{3};\frac{3}{2};\frac{4}{1};\ldots$$

$$1;2;3;4;5;6;7;8;9;\ldots$$

The sequence starts with the only fraction $\frac{m}{n}$ such that m+n=2, after that follow: two fractions having m+n=3, two fractions having m+n=4 ($\frac{2}{2}$ is

omitted, it equals to $\frac{1}{1}$ that was already encountered) etc.

In other words, the (dense!) set of all rational numbers possess the same "number of members" as the (discrete!) set of all natural numbers! As the next step Cantor proposed to try enumerating of all real numbers, i.e. all the points of a straight line. In his reply, Dedekind pointed out that also the set of all algebraic numbers can be enumerated by using natural numbers. Still, he did not succeed in enumerating all the real numbers...

In his next letter to Dedekind (December 7, 1873) Cantor proved that this is impossible: there is no one-to-one correspondence between real numbers and natural numbers. Cantor's proof involves the method that is called now the **diagonal method** (perhaps, first used for another purpose by P. du Bois-Reymond in 1871).

Namely, assume that we have some segment [a, b] and some "enumerating" sequence of real numbers $r_1, r_2, ..., r_n, ...$. Divide [a, b] into three equal parts, and take the part that does not contain the number r_1. Denote this part by $[a_1, b_1]$, divide it again into three equal parts, and take the part that does not contain the number r_2, etc. This process produces a sequence of contracting segments:

$$a_1 \le a_2 \le a_3 \le ... \le b_3 \le b_2 \le b_1 \quad .$$

The only common point of these segments is some real number r that does not belong to the "counting" sequence $r_1, r_2, ..., r_n, ...$. Hence, you cannot enumerate all real numbers (or, even a tiny segment of them!) by using the natural numbers.

Thus **there are at least two kinds of infinite sets**: the so-called countable sets (that can be enumerated by using the natural numbers), and some "more strongly infinite" sets that cannot be enumerated. This discovery by Georg Cantor is the most significant event in the history of the mathematical investigation of infinity.

Still, at the moment of discovery, for Cantor himself the following corollary was even more significant: "most" real numbers are transcendent. (Indeed, all the algebraic numbers can be enumerated, hence, the transcendent ones cannot.) The above Cantor's proof is simple enough to be followed by children (unlike the 1844 construction of particular transcendent numbers by J. Liouville, and the 1873 proof by Ch. Hermite that the number e is transcendent). Here we have a striking example of the power of non-constructive reasoning: sometimes, it is much easier to prove that "most" objects possess some property, than to construct or identify at least one such object!

The above-mentioned first set-theoretical results Cantor published in 1874:

G. Cantor. Über eine Eigenschaft des Inbegriffes aller reelen algebraischen Zahlen, "J. reine und angew. Math.", 1874, Vol. 77, pp, 258-262 (see also comments by Stanley N. Burris)

Exercise 2.2 (optional). Construct a one-to-one correspondences between: a) two segments (of different length), b) between the segment [a, b] (i.e. the set $\{x \mid a \leq x \leq b\}$) and the interval (a, b) (i.e. the set $\{x \mid a < x < b\}$), c) between an interval and the entire set of all real numbers.

Having discovered the existence of at least two radically different types of infinite sets, Cantor went further. In a letter to Dedekind (January 5, 1874) he asks: is a two-dimensional continuum (for example, a rectangle) equivalent to a one-dimensional continuum (for example, a segment)? In other words: does a rectangle contain more points than a straight-line segment? Cantor conjectured "yes", and spent the following three years trying to prove that a rectangle contains more points than a segment. He did not succeed. Only after he decided to explore the "unrealistic" opposite hypothesis (rectangles and segments contain equal numbers of points), he succeeded almost immediately! His proof (first exposed in a letter to Dedekind from July 20, 1877) is simple enough to be followed by children:

A one-to-one correspondence between the rectangle $[0, 1)x[0, 1)$ and a subset the segment $[0, 1]$ can be produced easily from the decimal fractions of coordinates:

$(x, y) \rightarrow z$

$x = 0.abcd...$

$y = 0.ABCD...$

$z = 0.aAbBcCdD...$

Exercise 2.3 (optional). Fill in the gaps and complete this proof (published in 1878):

G. Cantor. Ein Beitrag zur Mannigfaltigkeitslehre. "J. reine und angew. Math.", 1878, Vol. 84, pp. 242-258 (see also comments by Stanley N. Burris)

Cantor thought that his simple proof has "destroyed" the notion of dimensionality. Replying to this, Dedekind pointed out that Cantor's correspondence seems to be discontinuous, and conjectured that continuous correspondences between continuums of different dimensionalities would be impossible. Still, G. Peano in 1890 and D. Hilbert in 1891 succeeded in producing continuous (yet not one-to-one!) mappings from a segment onto a rectangle. And only in 1911 L. Brouwer "saved" the notion of dimensionality by proving that Dedekind was right: a continuous one-to-one correspondence between continuums of different dimensionalities is impossible:

L. Brouwer. Beweis der Invarianz der Dimensionenzahl. "Math. Ann.", 1911, Vol. 70, pp. 161-165.

Cantor's remarkable paper of 1878 contains another famous statement – the so-called Continuum Hypothesis. Working hard with various infinite sets of points Cantor established that all infinite sets he could produce, fall into two categories:

a) the so-called **countable** sets (i.e. the sets that can be enumerated by using natural numbers),

b) the sets that are equivalent to the entire **continuum** (i.e. the set of all real numbers).

Cantor was unable to produce sets of "intermediate power", i.e. uncountable sets of points that were not equivalent to the entire continuum. This is why he conjectured that such sets do not exist. This conjecture is known as the **Continuum Hypothesis**: each infinite set of points either is countable, or it is equivalent to the entire continuum.

Cantor spent many years trying to prove the Continuum Hypothesis. For this purpose, he developed further his apparatus of derivative sets P^k. He introduced condensation points of infinite order, i.e. points that are simultaneously condensation points of any finite order, and defined the infinite derivative set P^ω ("P omega") as the intersection of all the P', P", P"' etc. After this, he introduced further derivatives:

$P^{\omega+1} = (P^\omega)'$, $P^{\omega+2} = (P^{\omega+1})'$,...

$P^{\omega*2}$ = intersection of thes sets $P^{\omega+k}$ for all finite k,

$P^{\omega*2+1}$,... , $P^{\omega*3}$, $P^{\omega*3+1}$,...

$P^{\omega*\omega}$, $P^{\omega*\omega+1}$,...

Exercise 2.4 (optional). Try to produce a set P such that $P^\omega = \{0\}$, such that $P^{\omega*2} = \{0\}$ etc.

In this way Cantor arrived at a remarkable extension of the natural number system, the so-called **transfinite ordinal numbers**. These numbers extend the usual finite counting process:

Finite (i.e. natural) numbers are called **first class ordinal numbers**.

ω (omega, the first transfinite ordinal number) follows after all finite numbers,

ω+1 follows immediately after ω,

ω+2 follows immediately after ω+1,

...

$\omega*2$ is defined as $\omega+\omega$, i.e. it follows after all $\omega+k$ where k is finite,

$\omega*3$ is defined as $\omega*2+\omega$, i.e. it follows after all $\omega*2+k$ where k is finite,

...

ω^2 is defined as $\omega*\omega$, i.e. it follows after all $\omega*k$ where k is finite, etc.

...

ω^ω follows after all ω^k where k is finite, etc.

...

ε_0 follows after all expressions built up of natural numbers and ω by using addition, multiplication and exponentiation,

...

Infinite numbers having a countable set of predecessors are called **second class ordinal numbers**.

ω_1 (omega 1) follows after all second-class ordinal numbers, i.e. it is the least **third class ordinal number**.

Etc.

Cantor proved that the set of all second-class ordinal numbers O_2 is the least uncountable set, i.e. if some infinite subset S of O_2 is not equivalent to the entire O_2, then S is countable. Thus, to prove the Continuum Hypothesis, it was sufficient to prove that O_2 is equivalent to the entire continuum, i.e. "simply" to produce a one-to-one correspondence between the second class ordinal numbers and the real numbers. Still, Cantor and all his numerous followers failed to do this...

Thus, in some sense, the Continuum Hypothesis represents one of the most beautiful problems in mathematics: it can be explained to children, yet it remains unsolved for more than 100 years!

Cantor was already tired of many years of failed attempts to prove the Continuum Hypothesis, when he received another blow. In 1895 he discovered that his set theory leads to contradictions...

Still, all these difficulties cannot change the verdict of history: Georg Cantor remains one of the most outstanding personalities in the history of mathematics. He succeeded in developing the principles of the past mathematical thinking up to their logical limits.

2.2 Formalization of Cantor's Inconsistent Set Theory

First let us formalize the set theory directly as Cantor created it. This theory is based on the intuitive concept of a “world of sets" where all sets (finite and infinite) and all their members exist simultaneously and completely. In our axioms we would like to describe the governing laws of this frozen "world of sets".

At the very beginning we must answer the following question: can our "world" consist of sets only? A set can consist of members, which are sets. If the set x_1 contains a member x_2, which is also a set, if x_2 contains x_3, x_3 contains x_4 etc. – then, following along this chain must we not encounter something more tangible than "sets of sets"? If nothing tangible exists, how can sets exist? Still, if nothing exists, then the world is ... an empty set, let us denote this set by *o*. Thus, from nothing we have obtained something! Having *o* we can build the set which contains *o* as a member – the set {o}. Having *o* and {o} we can build a two-element set {o, {o}} etc.:

$$x_0 = o;\ x_1 = \{o\};\ x_2 = \{o, \{o\}\};\ ...;\ x_{n+1} = x_n \cup \{x_n\};\ ...$$

Therefore, even postulating that "nothing exists" we can obtain infinitely many different sets (compare Devlin [1977]).

Now, as the first step, let us define the **language of the formal set theory**. We will use only one sort of variables: *x, y, z, ...* – subscripted or not. Intuitively, the range of each variable consists of "all possible sets" (since we have decided that the "world of sets" consists of sets only). We do not introduce constants (like as *o* to denote the empty set) and function symbols (like as $x \cup y$ to denote the union of sets *x, y*). Later we will see how to do without these symbols. We introduce two predicate symbols: $x \in y$ (intuitively, “x is a member of y"), and $x = y$ (intuitively, "x is the same set as y").

We can combine atomic formulas like as $x \in y$ and $x = y$ by using logical connectors (negation, conjunction, disjunction, implication, equivalence) and quantifier symbols, thus obtaining **formulas of set theory**. For example, the formula

$$\forall y \neg(y \in x)$$

says that *x* is empty set, and the formula

$$\exists y(y \in x \wedge \forall z(z \in x \rightarrow z = y))$$

says that *x* possess exactly one member.

Exercise 2.4a. Provide formulas expressing the following assertions:

"x possess exactly two members",

"z consists of two members – x and y",

"x is a subset of y (i.e. all the members of x are members of y)",

“y consists of all subsets of x”

"x and y do not intersect (i.e. x and y do not possess common members)",

"x is an infinite set" (hint: try to say something about some of the proper subsets of x).

As the second step, as any serious formal theory, set theory must adopt some kind of logic – let us use the axioms and inference rules of the classical first order logic (see Detlovs, Podnieks [2000], Section 1.3). For example, the following formulas in the language of set theory we will use as logical axioms:

$x \in y \to (y = z \to x \in y)$ – an instance of the axiom schema $L_1 : B \to (C \to B)$;

$x = x \vee \neg (x = x)$ – an instance of the axiom schema $L_{11} : B \vee \neg B$;

$x = x \to \exists x (x = x)$ – an instance of the axiom schema $L_{13} : F(t) \to \exists x F(x)$.

After this, as the third step, we must introduce the **specific axioms of set theory**.

First, let us introduce the axioms defining the **specific meaning of the identity predicate in the set theory: x=y means that the sets x and y have the same members**. It may seem obvious, yet it requires special axioms – you cannot derive this specific meaning from pure logic. If the sets x and y have different definitions, and after some effort we managed to establish that $\forall z (z \in x \leftrightarrow z \in y)$, then we can conclude that x=y only by using the specific meaning of identity adopted in set theory. Therefore, to define the specific meaning of set identity we must introduce the following axioms:

$$x = y \leftrightarrow \forall z (z \in x \leftrightarrow z \in y) \ ; \qquad \text{(Ext)}$$

$$x = y \to \forall z (x \in z \leftrightarrow y \in z) \ . \qquad \text{(Ext')}$$

The axiom *Ext* is called the **Extensionality Axiom** (it says that in our set theory the identity of sets is treated extensionally, not intensionally, i.e. two different set definitions can lead to identical sets).

Exercise 2.4b. Use *Ext* and *Ext′* to verify the following properties of set identity:

a) $x = x$ (reflexivity),
b) $x = y \to y = x$ (symmetry),
c) $x = y \wedge y = z \to x = z$ (transitivity),

d) $F(x,x)\wedge x=y\rightarrow F(x,y)$ (substitution of an equal). Here, F is any formula, the designation F(x, x) means that the occurrences of the free variable x are split into two groups. In F(x, y), the occurrences of the second group have been replaced by y (which equals to x). (Hint: use induction by the structure of F.)

Since we adopted the classical logic for our "world of sets", we can prove the formula $\exists x(x=x)$, i.e. that at least one set exists in our "world". Indeed, it follows from the logical axiom $L_{13}: F(x)\rightarrow\exists xF(x)$. Hence, $x=x\rightarrow\exists x(x=x)$. Still, pure logic does not allow to conclude something about the properties of this set x. To obtain sets having specific properties (for example, the empty set) we must introduce additional axioms.

The main principle of Cantor's set theory says that a set is a "many" of which we can think as of a single "whole":

"Unter einer Mannigfaltigkeit oder Menge verstehe ich nämlich allgemein jedes Viele, welches sich als Eines denken lässt, d.h. jeden Inbegriff bestimmter Elemente, welcher durch ein Gesetz zu einem ganzen verbunden werden kann..." (Cantor [1883]).

Or:

"Unter einer 'Menge' verstehen wir jede Zusammenfassung *M* von bestimmten wohlunterschiedenen Objecten *m* unsrer Anschauung oder unseres Denkens (welche die 'Elemente' von *M* genannt werden) zu einem Ganzen" (Cantor [1895-1897]).

"A set is a collection into a whole of definite distinct objects of our intuition or of our thought. The objects are called the elements (members) of the set." (An English translation by Fraenkel, Bar-Hillel, Levy [1973]).

How could we think of many things as of a whole? One of the ways would be to define the combination of properties which allows to separate things that belong to the whole from things that do not belong to it. The corresponding notation is now used widely in mathematics, for example, c = {x | C(x)}, where C(x) says that "x is a crocodile". Mathematicians say that *c* is the "set of all crocodiles" and may operate with *c* as with a single object.

In the modern language we formulate Cantor's principle as the **Comprehension Axiom Schema**. Let F(y) be a formula of set theory (it may contain additional free variables, then let us call them parameters). We may think of F(y) as of an assertion "the set y possess the property F". Hence, according to the Cantor's principle we can introduce the set x of all y's possessing the property F:

$$x = \{y \mid F(y)\}.$$

To legalize operations like this one we must adopt the following axiom schema:

$$\exists x \forall y (y \in x \leftrightarrow F(y)) \qquad \text{(C[F(y)])}$$

(of course, formula F does not contain x). For each formula F(y) we have a separate comprehension axiom C[F(y)].

In particular, the axiom $C[\neg(y=y)]$ allows to prove the existence of the empty set:

$$\exists x \forall y (y \in x \leftrightarrow \neg(y=y)) \quad .$$

Hence, $\exists x \forall y \neg(y \in x)$, i.e. "there is a set x that is empty".

Let us prove the existence of the set {o}, i.e. of x such that $\forall y (y \in x \leftrightarrow y = o)$. It follows from the axiom C[y=o], or, more precisely, from $C[\forall z \neg(z \in y)]$.

Exercise 2.5. By using appropriate comprehension axioms: a) prove the existence of the following sets (o is the empty set): {o, {o}}; {o, {o}, {o, {o}}}; b) prove that the complement of a set, difference of two sets, intersection and union of any collection of sets ("set of sets") is a set.

The axioms *Ext*, *Ext'* and C[F(y)] (for all formulas F(y) that do not contain x, but may contain other parameters) and the Axiom of Choice define a formal set theory C which corresponds almost 100% to Cantor's intuitive set theory (of the "pre-paradox" period of 1873-94).

Cantor and the Axiom of Choice

Of course, in 1873-94 Cantor believed in the unrestricted comprehension principle. Still, did Cantor really accept a kind of Axiom of Choice as a valid principle of set theory? Let us check his two main papers on foundations of set theory:

G.Cantor. Grundlagen einer allgemeinen Mannigfaltigkeitslehre. "Math. Annalen", 1883, Vol.21, pp.545-586

G.Cantor. Beiträge zur Begruendung der transfiniten Mengenlehre. "Math. Annalen", 1895, Vol.46, pp.481-512; 1897, Vol.49, pp.207-246 (see also photocopies at Göttinger Digitalisierungs-Zentrum).

I am using the book by F.A.Medvedev "The early history of the axiom of choice" (Medvedev [1982]) that contains extensive relevant quotes from Cantor's works and Zermelo's comments.

Two main conclusions:

1. Cantor is using *ad hoc* – as he needs, and tens of times! – the "possibility of arbitrary choices" without any attempt to formulate something like a general Axiom of Choice. For example, when proving that each infinite set contains a countable subset (a quote from the 1895-97 paper):

"If we have some rule of deleting of elements $t_1, t_2, ..., t_{n-1}$ from [an infinite set – K.P.] T, then

always there is a possibility to delete one more element t_n..."

2. Cantor believed in "validity" of some assertions that are equivalent (or almost equivalent) to the Axiom of Choice. For example, in the 1883 paper he qualifies the thesis "each well defined set can be well ordered" as a "remarkable generally valid law of thought" and promises to consider it in one of subsequent papers. Still, he never did, and in the 1895-97 paper this thesis does not appear at all. Because of the "smell" of paradoxes?

Today, we can guess, did Cantor's thesis "each well defined set can be well ordered" mean that **all** sets can be well ordered (this would be equivalent to the Axiom of Choice, see below)? Or, maybe, Cantor intended (already in 1883?) to distinguish between "well defined" and "ill defined" sets? This could mean that Cantor believed only that "each constructible set can be well ordered" (as proved – without the Axiom of Choice – by K. Gödel in 1938, see Section 2.4 below).

Extending the Exercise 2.5 by introducing the notions of subset, "the set of all subsets of the set x", relations, functions, etc., we could derive from our formal set theory *Ext*+*Ext'*+*C* (i.e. from a very simple set of axioms!) all the common mathematics. **A very remarkable fact – 100% of mathematics can be derived from an extremely simple set of axioms!**

Note. At the time of Cantor and Frege, the axioms *Ext*, *Ext'* and C were regarded as "pure logical" ones. Thus, the reduction of mathematics to these axioms could be interpreted as a **reduction of mathematics to logic** (the so-called **logicism**, for details, see Logicism by Wikipedia, and Logicism by R.B.Jones).

Surprisingly, these axioms are also sufficient... to derive a contradiction!

Russell's Paradox

A very simple way how to do this was invented by Bertrand Russell in 1901, and is now called **Russell's paradox** – first published in

B. Russell. Principles of Mathematics. Cambridge University Press, Cambridge, 1903.

How Russell described this event in his *Autobiography* (in *Interactive Mathematics Miscellany and Puzzles* by Alexander Bogomolny)

A detailed reconstruction: How Bertrand Russell discovered the "Russell Paradox" by Paul Elliott.

About the history and significance of Russell' paradox see the online article Russell's Paradox in Stanford Encyclopedia of Philosophy.

In terms of our formal set theory, Russell's paradox can be derived as follows.

Normally, sets are not members of themselves, i.e. normally, $\neg(y\in y)$, for example, $\neg(o\in o)$. Still, our axioms do not exclude the existence of "abnormal" sets, which are members of themselves. Hence, let us consider the set of all "normal" sets:

$$x=\{y|\neg(y\in y)\} \quad .$$

The existence of this x is guaranteed by the comprehension axiom $C[\neg(y \in y)]$:

$$\exists x \forall y (y \in x \leftrightarrow \neg(y \in y)) \quad .$$

Now substitute x for y, and you will have a contradiction:

$$\exists x (x \in x \leftrightarrow \neg(x \in x)) \quad .$$

Hence, unexpectedly, some of the comprehension axioms lead to contradictions. Cantor's set theory *Ext+Ext'+C* is inconsistent. **The unrestricted comprehension axiom scheme cannot serve as a foundation of set theory!**

The first paradox in Cantor's set theory was discovered already in 1895 by Cantor himself. In 1897, Cesare Burali-Forti discovered – and published – another paradox. These paradoxes were more complicated than Russell's paradox, yet much easier to discover! See

Eric W. Weisstein. "Burali-Forti Paradox." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/Burali-FortiParadox.html

Cantor did not publish about the problem, he only communicated about it with David Hilbert. Hilbert proposed his own simpler version of a paradox, and, after this, around 1900, Hilbert's Göttingen collaborator Ernst Zermelo made one more step – he simplified Hilbert's paradox, thus, in fact, inventing Russell's paradox before Russell! Still, this discovery remained "Göttingen folklore" until Russell's publication in 1903.

For details of the story, see

V. Peckhaus, R. Kahle. Hilbert's Paradox. "Historia Mathematica", 2002, vol.29, N2, pp.157-175.

Today, more than 100 years after, perhaps, the discovery of paradoxes in mathematics would not be perceived as a catastrophe. Still, for G. Cantor (1845–1918) and G. Frege (1848–1925), who started to believe in the unrestricted comprehension schema in 1870's and lived with this absolute belief for more than 20 years, the discovery of paradoxes was a kind of a personal tragedy. For Georg Cantor – his set theory, and for Gottlob Frege – his formal system of mathematics were their main contributions to mathematics.

The solution was found by mathematicians of the next generation.

2.3. Zermelo-Fraenkel Axioms

Cantor did not think that the paradoxes discovered in his set theory are real contradictions (because of his platonist background: for him, investigating set theory meant exploring of "the true world of sets"). Instead of revising the foundations of set theory, he started *ad hoc* separating "finished sets" / "non-finished sets", "transfinite sets" / "absolutely infinite sets", and finally – in 1899 – "consistent multiplicities" / "inconsistent multiplicities" (see Peckhaus, Kahle [2002]). In modern terms, this would mean that Cantor proposed to restrict the comprehension axiom schema to those instances of it that do not lead to contradictions.

Ernst Zermelo proposed a more radical and more successful idea. He proposed to restrict the comprehension axiom schema by adopting only of those instances of it, which **are really necessary for reconstruction of common mathematics**. In 1908 Zermelo published his account:

E. Zermelo. Untersuchungen über die Grundlagen der Mengenlehre. "Math. Annalen", 1908, Vol. 65, pp. 261-281 (see English translation in Heijenoort [1967], (see also comments by Stanley N. Burris)

We will consider (a modern equivalent of) Zermelo's axioms some time later (for Zermelo's original system see the above online document). Of course, you will not find the axiom $C[\neg(y\in y)]$ among them, since such a kind of reasoning is not used in common mathematics.

Sets and Classes

Still, how to handle the situation, when we have some formula F(y), we use it to collect the sets y having the property F, yet trying to treat this collection as a set, we obtain a contradiction? For example, what to do with the Russell's collection $R=\{y|\neg(y\in y)\}$. The empty set o belongs to it: $\neg(o\in o)$, hence, $o\in R$. Still, if you will consider the collection R as a set and denote it by r, then you will have the Russell's paradox: $r\in r$ will be equivalent to $\neg(r\in r)$. How to solve this problem? Let us apply the well-known method due to King Solomon: let us consider Russell's paradox as the **proof** that Russell's collection **is not a set**!

Using this approach we must legalize some collections of sets that are not sets. Let F(y, z_1, ..., z_n) be a formula in the language of set theory (z_1, ..., z_n are optional parameters). Then let us say that for any fixed values of z_1, ..., z_n the formula F defines a **class**

$$A = \{y \mid F(y, z_1, ..., z_n)\},$$

i.e. the class of all y's possessing the property F. In general, different values of z_1, ..., z_n will yield a different class. For example, the class $\{y|\neg(y=z_1)\}$ consists of all sets except the set z_1, i.e. it really depends on the parameter z_1.

On the other hand, the class

$$V=\{y|y=y\}$$

consists of all sets at all, and does not depend on parameters. The class $V-\{x\}=\{y|\neg(y=x)\}$ depends on the parameter x.

Each set is a class: the set x coincides with the class $\{y|y\in x\}$. In its most general (inconsistent!) form, the *comprehension axiom schema says that all classes are sets*:

$$\exists x\,\forall y(y\in x\leftrightarrow F(y,z_1,\ldots,z_n)) \quad .$$

Still, "in fact", some classes are not sets. For example, the Russell's class $R=\{y|\neg(y\in y)\}$ cannot be a set: if R=x, then $y\in x$ is equivalent to $\neg(y\in y)$, and by setting y=x we obtain a contradiction. Classes that are not sets we will call **proper classes**. We can say simply that each paradox of set theory "generates" some proper class.

We will denote classes by capital letters: A, B, C, ... (small letters a, b, c, ... are variables of the language of set theory, i.e. they denote sets). This notation must remind to us of the metaphoric character of the following "formulas":

$$y\in A,\ A=B,\ A\subseteq B,\ A\cap B,\ A\cup B,\ A-B \quad .$$

These "formulas" do not belong to the language of set theory, which does not contain "capital" variables. They are used merely as a convenient notation for the following formulas:

$$F(y),\forall y(F(y)\leftrightarrow G(y)),\forall y(F(y)\rightarrow G(y))\,G(y) \quad ;$$
$$F(y)\wedge G(y),\ F(y)\vee G(y),\ F(y)\wedge\neg G(y) \quad ,$$

where the formula F defines the class A, and the formula G defines B.

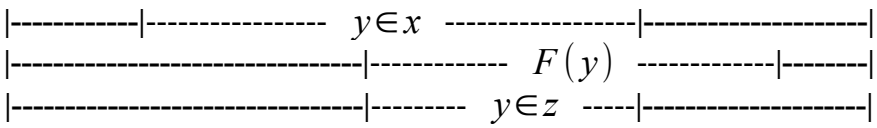
Now we can start formulating the axioms of set theory as Zermelo proposed them. We will use the same formal language of set theory introduced in the previous section, and the same axioms and inference rules of the classical first order logic.

As the first axioms we adopt the same extensionality axiom *Ext* and the axiom *Ext'*. But, following that, we will adopt only those comprehension axioms that are really used in mathematics for building of "useful" sets.

Separation Axiom Schema

Perhaps, the simplest way to obtain new sets would be **separation**: having a set x, let us separate those members of x that possess some common property F. For example, in this way the set of all prime numbers is obtained from the set of all natural numbers. In general, the situation could be represented as

follows:



The condition F(y) is any formula of set theory (it may contain parameters z_1, ..., z_n). Using this condition we separate those members of the set x that satisfy the condition F. The members separated make up a new set denoted by z.

To legalize this way of reasoning we must introduce the following the **Separation Axiom Schema**: if F(y, z_1, ..., z_n) is any formula that contains free variables y, z_1, ..., z_n, but does not contain x and z, then the following formula is declared to be an axiom:

$$\exists z \forall y (y \in z \leftrightarrow y \in x \wedge F(y, z_1, \ldots, z_n)) \quad . \qquad \text{(C1[F])}$$

Of course, this schema is a part of the general comprehension schema, namely, $C[y \in x \wedge F(y, z_1, \ldots, z_n)]$.

An alternative, extremely convenient form of the separation schema can be obtained by using the notion of classes: the formula F defines a class A, hence, the axiom C1[F] says that the intersection A∩x (of the class A and the set x) is a set: A∩x = z.

Now we can prove the **existence of the empty set**, i.e the formula $\exists x \forall y \neg(y \in x)$. Indeed, from the logical axioms we know that some sets exist, let z_0 be a set. Then, using the impossible condition $\neg(y = y)$ and the axiom $C1[\neg(y = y)]$ we obtain a set x such that

$$\forall y (y \in x \leftrightarrow y \in z_0 \wedge \neg(y = y)) \quad .$$

hence, $\forall y \neg(y \in x)$. Q.E.D.

On the other hand, the Axiom of Extensionality implies that there is only one empty set. Indeed, if the sets x_1, x_2 both are empty, i.e. $\forall y \neg(y \in x_1)$ and $\forall y \neg(y \in x_2)$, then $\forall y (y \in x_1 \leftrightarrow y \in x_2)$, and (by *Ext*) $x_1 = x_2$.

Note. Do not underestimate this simple invention – the empty set! You may think safely, that the empty set is not a set. Still, this would make the treatment of, for example, set intersections somewhat complicated – sometimes x∩y would be a set, but sometimes – empty!

It would be nice to denote the empty set, for example, by *o*, yet our language of set theory does not contain constants. If we would introduce one, this would not solve the problem completely, because after the first constant we may wish

to introduce the second one etc. Therefore, it would be better to do without any constants at all. Let us see how this can be achieved.

If we wish to use the empty set constant *o* in our reasoning legally, we must provide a method allowing to translate our "*o*-extended" formulas into the pure language of set theory that does not contain *o*. This can be done easily. Indeed, if we assert that the empty set *o* possess some property expressed by a formula F(x), i.e. we use the formula F(*o*), then this assertion can be expressed also by the formula

$$\forall x((\forall y \neg(y \in x)) \rightarrow F(x)),$$

i.e. if x is empty, then x possess the property F. This formula does not contain the constant *o*. Hence, we can use the constant *o* in our reasoning safely. If needed, we can reformulate any such reasoning by using (more complicated) formulas that do not contain *o*.

The above approach can be generalized. Let us assume that we have proved the existence and uniqueness of the set satisfying some formula T(x). I.e. we have proved the following two formulas:

$$\exists x\, T(x) \quad ,$$
$$\forall x_1 \forall x_2 (T(x_1) \wedge T(x_2) \rightarrow x_1 = x_2) \quad .$$

Then we may introduce a constant *t* denoting the above-mentioned unique set satisfying T(*t*), and use it in our reasoning safely. Any assertion like as F(*t*) (i.e. "*t* possess the property F") we can reformulate without using of *t:* $\forall x(T(x) \rightarrow F(x))$.

Still, the formula T could contain parameters, for example, T(x, z_1, z_2). If we have proved that for each pair of z_1 and z_2 there is a unique x such that T(x, z_1, z_2), then T defines some **operation**. We may wish to introduce a specific symbol # denoting this operation, and use expressions like $z_1 \# z_2$ in our reasoning. Then $x = z_1 \# z_2$ will be just another record of the formula T(x, z_1 , z_2). This can be done safely, since, for example, the assertion F($z_1 \# z_2$) can be reformulated as $\forall x(T(x, z_1, z_2) \rightarrow F(x))$.

The possibility of safe introduction of additional constants and operation symbols is widely used in semi-formal reasoning of set theory.

Note. The above explanation somewhat simplifies the problem. For full treatment see Mendelson [1997].

Exercise 2.6. a) Use appropriate separation axioms to prove that for each pair of sets x_1, x_2 the intersection $x_1 \cap x_2$ and the difference $x_1 - x_2$ also are sets. Justify the usage of both operation symbols.

b) Prove that if $A \subseteq B$, and A is a proper class, then B also is a proper class.

Hence, the **class of all sets** V = {y | y=y} **is a proper class**. Indeed, $R \subseteq V$, where R is (the proper) Russell's class.

The separation schema allows only obtaining of smaller sets from larger ones. Hence, without additional axioms, we would be able to prove only the existence of the "smallest" set – the empty set. So, we must adopt some "enlarging" axioms, too.

Pairing Axiom

As the first "positive" axiom, let us consider the **Pairing Axiom**. If we have two sets x_1 and x_2, then we can build a new set containing x_1 and x_2 as its only members. We will denote this set by $\{x_1, x_2\}$ (if $x_1=x_2$, then we will write simply $\{x_1\}$). To make this way of reasoning legal, we must adopt as an axiom the following formula:

$$\forall x_1 \forall x_2 \exists z \forall y \left(y \in z \leftrightarrow y = x_1 \vee y = x_2 \right) . \qquad \text{(C2)}$$

Of course, C2 is a comprehension axiom, namely, $C[y = x_1 \vee y = x_2]$. In terms of classes: the Pairing Axiom says that if x_1 and x_2 are sets, then the class $\{x_1, x_2\}$, defined by the formula $y = x_1 \vee y = x_2$, also is a set.

The set $\{x_1, x_2\}$ represents the so-called **unordered pair**. How to introduce in our theory the notion of **ordered pair**, which is important, for example, as a base for the notions of relation and function? We will denote the ordered pair of x_1 and x_2 by (x_1, x_2).

In his 1914 paper

N. Wiener. A simplification of the logic of relations. "Proc. of the Cambridge Philos. Soc.", 1914, vol. 17, pp.387-390

Norbert Wiener proposed to define (x_1, x_2) as a combination of unordered pairs, where the first member is marked by adding the empty set:

$$(x_1, x_2) = \{ \{\{x_1\}, o\}, \{\{ x_2\}\}\}.$$

After this, in the paper

K. Kuratowski. Sur la notion d'ordre dans la theorie des ensembles. "Fund. Math.", 1921, Vol. 2, pp.161-171

Kazimierz Kuratowski proposed an even simpler method of deriving (x_1, x_2) from $\{x_1, x_2\}$:

$$(x_1, x_2) = \{\{x_1\}, \{x_1, x_2\}\}.$$

Intuitively, x_1 and x_2 have different positions in the right hand side expression, i.e. they seem to be "ordered".

Note. Do not underestimate this simple invention – it greatly simplifies the language and the axioms of set theory! Without it, we would need an additional construct (x, y) in the language of set theory, and, correspondingly, additional axioms to define the properties of this construct.

Exercise 2.7. Justify the definition of (x_1, x_2) by Wiener and Kuratowski by proving that

$$(x_{1,} x_2)=(y_{1,} y_2) \rightarrow x_1 = y_1 \wedge x_2 = y_2 \quad .$$

And, in particular, if $x_1 \neq x_2$, then $(x_1, x_2) \neq (x_2, x_1)$.

Using the notion of ordered pairs we can introduce the notions of Cartesian product, relation and function – simply as specific kinds of classes and sets.

The **Cartesian product** of classes A, B is defined as follows:

$$A \times B = \{(u, v) | u \in A \wedge v \in B\} \quad ,$$

or, more precisely:

$$A \times B = \{z | \exists u \exists v (u \in A \wedge v \in B \wedge z = (u, v))\} \quad .$$

If A, B are sets, then the Cartesian product $A \times B$ also will be a set? Sorry, to legalize such a conclusion we must wait for additional axioms.

Relations are defined as classes that consist of ordered pairs only. I.e. the class Q={ y | F(y) } will be called a relation, if and only if

$$Ay (y \in Q \rightarrow \exists u \exists v\, y = (u, v)) \quad .$$

Each formula $F_1(u, v)$ having two free variables defines a relation:

$$Q = \{(u, v) | F_1(u, v)\} \quad .$$

And conversely, for each relation Q we can build a formula $F_1(u, v)$ such that

$$(u, v) \in Q \leftrightarrow F_1(u, v) \quad .$$

Some time later we will prove that some relations are proper classes, for example:

$$E = \{(u, v) | u = v\}; C = \{(u, v) | u \in v\} \quad .$$

Union Axiom

If we had only the axioms C1 and C2, we could not build sets that possess

more than two members. Therefore, let us consider the next operation for building "useful" sets – the **union** of sets.

The simplest case is the union $x \cup y$, yet in general we can merge arbitrary collections of sets. For any class B we can define the union of all members of B:

$$\cup B = \{ y | \exists z (y \in z \wedge z \in B) \} \quad .$$

In other words, the union ∪B consists of all "members of members" of B. By the way, ∪{x, y} represents exactly the well-known $x \cup y$.

The next axiom we adopt is the **Union Axiom**. It says that if x is a set, then ∪x also is a set:

$$\forall x \exists u \forall y (y \in u \leftrightarrow \exists z (y \in z \wedge z \in x)) \quad . \qquad \text{(C3)}$$

This axiom is a comprehension axiom, namely, $C[\exists z (y \in z \wedge z \in x)]$.

Exercise 2.8. a) Prove that if B is a proper class, and x is a set, then the difference B−x is a proper class.

b) Show that the axioms C1, C2 and C3 allow proving the existence of any set which can be defined by using a finite number of the empty set symbols *o*, commas and braces, for example, {o, {o, {o}}, {o, {o, {o}}}}.

If we had only the axioms C1, C2 and C3, we could build only sets that possess a finite number of members.

But now we can prove that, if A and B are non-empty classes, and their Cartesian product $A \times B$ is a set, then A and B also are sets. Indeed, let v_0 be a member of B, then for each $u \in A$:

$$(u, v_0) \in A \times B ; \{\{u\}, \{u, v_0\}\} \in A \times B ; u \in \cup (A \times B) ; u \in \cup \cup (A \times B) .$$

Hence, $A \subseteq \cup \cup (A \times B)$. Since $A \times B$ is a set, according to the Union Axiom, $\cup \cup (A \times B)$ also is a set, hence, by the Separation Schema, so is A. Similar argument proves that B also is a set. (For the proof that, if A and B are sets, then the product $A \times B$ also is a set, we must wait for additional axioms, see below.)

Exercise 2.8. c) Prove that the relations E and C defined above are proper classes.

Natural Numbers in Set Theory

The only kind of objects known in our set theory are sets. Hence, if we wish to have natural numbers in our theory, then we must declare that some sets are natural numbers. And indeed, now we are ready to try declaring some of the

simplest finite sets as **natural numbers** (by definition). Namely, let us declare the empty set *o* to be the number "zero", the set {o} – to be the number "one", then, {o, {o}}, or {0, 1} will be the number 2, {0, 1, 2} – the number 3, etc. In general, if the set c_n is declared to be the number *n*, then the set

$$c_{n+1}=c_n\cup\{c_n\}$$

is declared to be the number *n+1*. It seems that we have in this way also the set of all natural numbers

{0, 1, 2, 3, ..., n, n+1, ...}?

As noted above, the axioms we have adopted so far do not allow proving of the existence of such an (infinite!) set. Therefore, let us try to define at least the **class of all natural numbers**. It appears not an easy task! The easy "solutions" by using "infinite formulas" like as

$$y=c_0\vee y=c_1\vee y=c_2\vee\ldots\vee y=c_n\vee\ldots$$

cannot be taken seriously, since the language of set theory allows only finite formulas (and, the idea of an "infinite formula" is, in fact, a crazy one). To obtain a finite formula N(y) expressing $\exists n(y=c_n)$, let us follow an early (1923) idea by John von Neumann:

J. von Neumann. Zur Einführung der transfiniten Zahlen. "Acta Szeged", 1923, 1, pp. 199-208

In 1930s, R. M. Robinson, K. Gödel and P. Bernays simplified von Neumann's constructions considerably – see

A. A. Fraenkel, Y. Bar-Hillel, A. Levy. Foundations of Set Theory. *Studies in Logic*, Vol. 67, Elsevier Science, 1973, 404 pp. (Russian translation available)

First, let us try defining formally the notion of **finite sets**. Let us use the idea due to Paul Stäckel (according to Finite set in Wikipedia): let us say that some set *y* is finite, if and only if its members can be ordered in such a way that each non-empty subset of *y* contains a minimum and a maximum member.

A relation *R* (possibly, a class) is called a (partial) **ordering** of a class B if and only if

$$\forall b(b\in B\rightarrow\neg R(b,b)) \quad \text{(non-reflexivity);}$$

$$\forall b\forall c\forall d(b,c,d\in B\rightarrow(R(b,c)\wedge R(c,d)\rightarrow R(b,d))) \quad \text{(transitivity).}$$

Let us call an ordering r a **double-well-ordering** of the set *y*, if and only if r is a set, and each non-empty subset of *y* contains a minimum and a maximum member under r, i.e. if and only if

$$\forall z(z\subseteq y\wedge\exists s(s\in z)\rightarrow\exists u\,MIN(r,u,z)\wedge\exists u\,MAX(r,u,z)) \quad ,$$

where *MIN(r, u, z), MAX(r, u, z)* are the following formulas:

$$(u \in z \wedge \forall v(v \in z \rightarrow r(u,v) \vee v = u)) \quad ;$$
$$(u \in z \wedge \forall v(v \in z \rightarrow r(v,u) \vee v = u)) \quad .$$

Intuitively, only finite sets (and all of them) can be double-well-ordered (by some relation). Thus, this could serve as a good formal definition of finite sets: ***y* is a finite set, if and only if we can provide a relation-set r such that r is a double-well-ordering of *y*.**

Exercise 2.9 (optional, coursework for smart students). Prove the following:

a) For finite sets, prove the Replacement Axiom Schema (see below).

c) For finite sets, prove the Power-Set Axiom (see below): if x is a finite set, then P(x) is a set (and a finite one).

d) If *a, b* are finite sets then $a \times b$ is a set (and a finite one). Note: for a general proof that "if *a, b* are sets, then $a \times b$ is a set" additional axioms are necessary.

e) For finite sets, prove the Axiom of Choice (see below).

All sets c_n are finite sets:

$$c_0=o;\ c_1=\{o\}=\{c_0\};\ c_2=\{o,\ \{o\}\}=\{c_0, c_1\};\ c_3=\{c_0, c_1, c_2\};\ ...$$

Namely, each of them is double-well-ordered by the membership relation: $c_0 \in c_1 \in c_2 \in c_3 \in ...$!

Another remarkable property of c_n is as follows: it contains all members of its members, members of members of members etc. Hence, the definiton: the set *y* is called **transitive** if it contains all members of each of its member, i.e.

$$\forall u(u \in y \rightarrow u \subseteq y) \quad ,$$

or

$$\forall u \forall v(u \in v \wedge v \in y \rightarrow u \in y) \quad \text{(transitivity, indeed!).}$$

Thus, all sets c_n are transitive and double-well-ordered by the membership relation.

Let us use this combination of two properties to formalize the semi-formal predicate $\exists n(y=c_n)$ as a definition of the class N of natural numbers:

N = {y | (y is transitive) and
(y is double well ordered by the membership relation)}.

Now, natural numbers will be – by definition – simply members of N! (Does N contain the numbers c_n only? Good question! See below.)

Exercise 2.10 (optional). a) Show that the "standard" natural numbers c_n

defined above all are members of the class N. I.e. prove the theorem schema "for all n: $c_n \in N$ ". We do not know how to replace this schema $c_n \in N$ (i.e. an infinite sequence of theorems) by one (finite) theorem. This seems to be impossible.

b1) Show that, if $x \in N$ and y is the maximum member of x (under the membership relation), then $x - \{y\} = y$ and hence, $x = y \cup \{y\}$.

b2) Show that $y \in x \in N \rightarrow y \in N$, i.e. that N is a transitive class, or, natural numbers (a sets) consist of natural numbers.

c) Prove that if B is a non-empty subclass of N, then B contains a minimum member under the membership relation.

d) Prove the "induction principle" for N: if B is a subclass of N such that $0 \in B \wedge \forall x (x \in B \rightarrow x \cup \{x\} \in B)$, then B=N.

e) (coursework for smart students). Define addition and multiplication for members of N. (Hint: uses the result of Exercise 2.22 below). Prove that all the axioms of first order arithmetic PA (see Section 3.1) hold in N. You will need for this only the above axioms *Ext*+*Ext'*+*Separation*+*Pairing*+*Union*. Thus, in the set theory *Ext*+*Ext'*+*Separation*+*Pairing*+*Union* one can fully re-build (in the sense of Section 3.2) the first order arithmetic PA (defined in Section 3.1). On the other hand, consider in *Ext*+*Ext'*+*Separation*+*Pairing*+*Union* the class consisting of all finite sets that can be built of the empty set by using the pairing and union operations. Verify that in this class: a) all the axioms of set theory ZFC are true, except the Axiom of Infinity; b) the axiom "all sets are finite" (i.e. the negation of the Axiom of Infinity) is true. And finally, derive the following

Exercise 2.10X (optional, coursework for smart students). Answering a question by Calvin Ostrum (thanks), prove that the following theories are equiconsistent (i.e. they are all consistent, or all inconsistent, simultaneously):

PA;
Ext+*Ext'*+*Separation*+*Pairing*+*Union*;
ZF minus *Axiom of Infinity*;
ZFC minus *Axiom of Infinity* plus negation of *Axiom of Infinity.*

(Hint: to conclude the consistency of *Ext*+*Ext'*+*Separation*+*Pairing*+*Union* from the consistency of PA, use the techniques of Section 3.3 below.)

Now, in a sense, the Question of Questions: for you, are the results of the Exercise 2.10 sufficient to conclude that "N is the class of all natural numbers"?

Axiom of Infinity

The axioms of set theory we have adopted so far allow proving of the existence of finite sets only. Indeed, if you wish, you can verify easily that all these axioms hold when interpreted in the area of sets, which can be defined by using of a finite number of the empty set symbols o, commas and braces, for example, {o, {o, {o}}, {o, {o, {o}}}}. A kind of infinity we have only among classes, for example, N is an infinite class.

Hence, our next step must be adopting of some Axiom of Infinity.

The approach used below is somewhat non-traditional: I will introduce the **Axiom of Infinity as a comprehension axiom.** Namely, if we wish to think of N as of a set, then we must adopt the following **Axiom of Infinity**:

$$\exists x \forall y (y \in x \leftrightarrow y \in N) \quad . \quad \text{(C4)}.$$

Of course, this is a comprehension axiom, namely, $C[y \in N]$.

Exercise 2.11. Write down the full text of C4 and count the number of characters in it.

The set of all natural numbers is denoted traditionally by ω (omega), instead of the above class letter N.

Note. As you see, C4 is somewhat lengthy when compared to other single Zermelo axioms (not axiom schemas, of course!). Perhaps, for this reason, Zermelo and his followers used shorter forms of the Axiom of Infinity, for example:

$$\exists x (o \in x \wedge \forall y (y \in x \rightarrow y \cup \{y\} \in x)) \quad ,$$

or even shorter (why is it shorter?):

$$\exists x (\exists y (y \in x) \wedge \forall y (y \in x \rightarrow \exists z (z \in x \wedge y \subset z))).$$

Of course, C4 implies these formulas (simply take ω for x). If you wish, try proving that the converse is true as well (it is!).

A set x is called a **countable set**, if and only if x is finite, or members of x can be enumerated by using natural numbers, i.e. if there is a 1-1-mapping (possibly, a class) between ω and x.

After adopting of the Axiom of Infinity, we can prove the existence only of countable sets. To prove the existence of **uncountable sets**, the Power-Set Axiom C5 must be applied additionally (see below).

Exercise 2.12 (optional, for smart students). Prove the following:

a) If *a, b* are countable sets then $a \times b$ is a set (and a countable one). Note: for a general proof that "if *a, b* are sets, then $a \times b$ is a set" we still need additional axioms.

b) For countable sets, prove the Replacement Axiom Schema (see below).

Power-Set Axiom

The following rather complicated way of building sets was invented, perhaps, as late as in 1870s – during the attempts to derive the definition of real numbers from the properties of rational numbers. It appeared that speaking about "arbitrary" real numbers involves inevitably speaking about "arbitrary" sets of natural numbers. Let us consider, for example, the definition of real numbers by means of infinite binary expansions. Any such expansion, for example,

$$0.10101100110000101110...$$

"generates" some set of natural numbers. The above example generates the set

$$\{1, 3, 5, 6, 9, 10, 15, 17, 18, 19, ...\}.$$

In principle, in this way we can "generate" all the possible sets of natural numbers.

In general, this new operation is defined as follows. If x is a set, let us consider all the possible **subsets** of x, i.e. all y's such that $y \subseteq x$, or $\forall z(z \in y \rightarrow z \in x)$. Let us denote the class of all subsets of x by

$$P(x) = \{y | y \subseteq x\}$$

(P stands for "power-set"). We wish to postulate that if x is a set, then P(x) also is a set. Thus, we adopt the following **Power-Set Axiom**:

$$\forall x \exists z \forall y (y \in z \leftrightarrow y \subseteq x) \quad . \qquad \text{(C5)}$$

Of course, C5 is a comprehension axiom, namely, $C[y \subseteq x]$.

Now we can prove that the **Cartesian product of two sets is a set**. Indeed,

$$y \times z = \{(u, v) | u \in y \wedge v \in z\} \quad .$$

If $u \in y$ and $v \in z$, then $\{u\} \in P(y)$ and $\{u, v\} \in P(y \cup z)$. Hence,

$$\{\{u\}, \{u, v\}\} \in PP(y \cup z); (u, v) \in PP(y \cup z) \quad ,$$

i.e. the class $y \times z$ is a part of the set $PP(y \cup z)$. Q.E.D.

Note. For an alternative proof that does not depend on the Power-Set Axiom (but depends on the Replacement Schema below) see Exercise 2.15(d).

Cantor's Theorem (the classical version). For any set x, there is no one-to-one-correspondence between x and P(x) (i.e. one-to-one-correspondence between members of x and all subsets of x).

Corollary. P(w) ("the set of all sets of natural numbers") is an uncountable set. Hence, so is the set of all real numbers.

Cantor's Theorem (a refined version, implies the classical version, verify!). If f is a function mapping members of a set x into subsets of x, (i.e. f: x→P(x)), then there is a subset of x that does not belong to *range(f)*.

Proof. By the Separation Axiom $C1[\neg(y\in f(y))]$,

$$y_0=\{y|y\in x\wedge\neg(y\in f(y))\}$$

is a subset of x. If $y_0=f(y)$ for some $y\in x$, then

$$(y\in y_0)\leftrightarrow\neg(y\in f(y))\leftrightarrow\neg(y\in y_0) \quad .$$

Contradiction. Hence, y_0 is a subset of x that does not belong to *range(f)*. Q.E.D.

In this proof, only the axioms C1, C2 and C3 are used, i.e. **this proof does not depend on the Power-Set Axiom** C5 (as noted by Neil Tennant in Cantor's argument, February 2003, on the FOM List). Cantor's Theorem does not depend on the Power-Set Axiom, but the "sethood" of P(w) does!

Replacement Axiom Schema

Functions are relations that possess the "mapping" property:

$$(u,v_1)\in F\wedge(u,v_2)\in F\rightarrow v_1=v_2 \quad ,$$

or,

$$\forall u\forall v_1\forall v_2(F(u,v_1)\wedge F(u,v_2)\rightarrow v_1=v_2).$$

If F is a function, then F(u)=v can be used as a convenient record of $(u,v)\in F$. Some functions are proper classes, for example, the above-mentioned identity function E(x)=x, or, more precisely,

$$E = \{(u, v) \mid u=v\}.$$

The well-known notions of **domain** and **range** of the function F can be defined as follows:

$$\text{domain}(F) = \{ u \mid \exists v\ F(u)=v \}$$

$$\text{range}(F) = \{ v \mid \exists u\ F(u)=v \}.$$

If F is a proper class, then, in general, domain(F) and range(F) also will be proper classes. For example, domain(E) = range(E) = V.

Exercise 2.13. Prove, for any relation Q, that Q is a set, if and only if domain(Q) and range(Q) both are sets.

The "zero-constant" function, i.e. $F_0 = \{(u, v) \mid v=o\}$, has a proper class domain ($\text{domain}(F_0)=V$), yet its range is a set ($\text{range}(F_0)=\{o\}$). Still, how

about the fourth possibility – can a function have a set domain and a proper class range, i.e. **can a function map a set onto a proper class**? Of course, we do not wish such functions. To prohibit them, we must adopt additional axioms – the so-called Replacement Axiom Schema. You will not find such axioms in Zermelo's 1908 paper. Abraham Fraenkel noticed that they are necessary some time later – in 1921:

A. A. Fraenkel. Zu den Grundlagen der Cantor-Zermeloschen Mengenlehre. "Math. Annalen", 1922, Vol. 86, pp. 230-237.

If F is a function, then, for any class B, we will denote by F"B the **F-image** of B:

$$F''B=\{v|\exists u(u\in B\wedge F(u)=v)\} \quad .$$

Exercise 2.14. Prove that if some function f is a set, then, for any class B, the image f"B is a set.

Still, if the function F is a class, and b is a set, then the image F"b is ... a set? Imagine, you take members of the set b one by one, and replace each member y by F(y). The result is F"b. Of course, we wish F"b to be a set. So, let us adopt the **Replacement Axiom Schema**:

$$\text{F is function} \rightarrow \quad \forall b\exists c\, F''b=c \quad . \text{ (C6[F])}$$

Or, more precisely, let F(u, v, z_1, ..., z_n) be a formula that does not contain v_1, v_2, x, y, b, c, then we adopt as the axiom C6[F] the following formula:

$$\forall u\forall v_1\forall v_2(F(u, v_1, z_1, \dots, z_n)\wedge F(u, v_2, z_1, \dots, z_n)\rightarrow v_1=v_2)\rightarrow$$
$$\forall b\exists c\forall y(y\in c\leftrightarrow\exists x(x\in b\wedge F(x, y, z_1, \dots, z_n))) \quad .$$

Of course, this is again a comprehension axiom, namely, $C[\exists x(x\in b\wedge F(x, y))]$, yet we allow to apply it only after we have proved that for each *x* there is only one (or none) *y* such that F(x, y).

Exercise 2.15. a) Prove that if B is a proper class, and b is a set, then no one-to-one function can map B into b (or, equivalently, there is no function F with domain(F)=b and range(F)=B).

b) Derive the Separation Axiom Schema C1 from the Replacement Axiom Schema C6.

c) (Jan Mycielski) Derive the Pairing Axiom C2 from C1, C5 and C6. (Hint: apply first C1, then twice – C5, and finally – C6).

d) Above, we used the Power-Set Axiom C5 to prove that the Cartesian product of two sets is a set. By using the Replacement Axiom Schema C6, this can be proved without C5. Elaborate the following proof put on the FOM list by Harvey Friedman (see "What do you lose if you ditch Powerset?", November 2003):

LEMMA. {x} cross B exists.

Proof: For each y in B, {x} cross {y} exists. Then use Replacement to get the set of all <x,y> such that y in B (x fixed).

THEOREM. A cross B exists.

Proof: For each x in A, {<x,y>: y in B} exists. Use Replacement to get E = {{<x,y>: y in B}: x in A}. A cross B = ∪E.

The Replacement Axiom Schema completes the list of comprehension axioms, that are necessary for reconstruction of the common mathematics, i.e. for building of "useful" sets. Is our list (the axioms from C1 to C6) "complete" in the sense that no "acceptable" comprehension axioms will be discovered in the future? The answer could be "yes" (Church's Thesis for set theory?). We will discuss this problem in Section 2.4.

Exercise 2.16. Prove that, in the set ω, the semiformal ("second order") Peano axioms hold (see Section 3.1).

So, it would be nice to stop at this point and finish our list of axioms by adopting an axiom asserting that no other sets exist – except those, which can be built by using the comprehension axioms? I.e. the axiom: "All sets can be built by using the comprehension axioms". Still, how to put this restriction into one (finite!) formula of set theory?

Open problem. How to put the statement "All sets can be built by using the comprehension axioms" into one formula of set theory? Is this possible at all?

While this problem remains unsolved, let us return to the tradition, and discuss the remaining two axioms – the Axiom of Regularity and the Axiom of Choice.

Axiom of Regularity

Sometimes called also the "**Axiom of Foundation**".

It appears that the existence of some "abnormal" kinds of sets is consistent with all the axioms we have adopted so far. For example, if you wish to assert the existence of a set x such that $x \in x$, you can do this safely: no contradiction with our previously adopted axioms will arise.

An idea, allowing to avoid such "abnormal" sets, was first proposed in 1917 by Dmitry Mirimanoff (1861-1945):

D. Mirimanoff. Les antinomies de Russell et de Burali-Forti et le probleme fondamental de la theorie des ensembles. "Enseign. math", 1917, Vol. 19, pp. 37-52.

Mirimanoff introduced the notion of "ordinary sets" (or, as we would call them today, "well-founded sets", or "regular sets"), in which infinite chains "down"

the membership relation do not appear, for example:

$$...\in x_n\in...\in x_3\in x_2\in x_1\in x. \qquad (*)$$

In these terms, the above-mentioned "abnormal" sets ($x\in x$, $x\in y\wedge y\in x$, etc.) should be qualified as "non-ordinary".

In 1925, J. von Neumann proposed to avoid such "abnormal", "non-ordinary", "non-regular" sets at all by introducing the following *Axiom der Fundierung*, now called the **Axiom of Regularity**:

$$\forall x(\neg(x=o)\rightarrow\exists y(y\in x\wedge y\cap x=o)) \ ,$$

or, with abbreviations excluded,

$$\neg\exists x(\exists y(y\in x)\wedge\forall y(y\in x\rightarrow\exists z(z\in x\wedge z\in y))) \ . \qquad (Reg)$$

J. von Neumann. Eine Axiomatisierung der Mengenlehre. "Journal für reine und angewandte Mathematik", 1925, Vol.154, pp. 219-240.

Exercise 2.17. Verify that, indeed, *Reg* excludes all the above-mentioned "abnormal" sets:

a) Derive from *Reg* that $\neg(x\in x)$ for all x, i.e that V=R, where R is Russell's class.

b) Similarly, derive from *Reg* that there are no two sets x, y such that $x\in y\wedge y\in x$.

c) (for smart students) Assume Axiom of Choice. Verify, that then, *Reg* is equivalent to the proposition “sets of the kind (*) do not exist”.

The set theory adopting the Axiom of Extensionality (*Ext*), the axiom *Ext'*, the Separation Axiom Schema (C1), the Pairing Axiom (C2), the Union Axiom (C3), the Axiom of Infinity (C4), the Power-Set Axiom (C5), the Replacement Axiom Schema (C6), and the Axiom of Regularity (*Reg*), is called **Zermelo-Fraenkel set theory**, and is denoted by ZF.

Zermelo included in his axiom list also the famous Axiom of Choice.

Axiom of Choice

See also
Home Page for the Axiom Of Choice by Eric Schechter
Axiom of Choice by Wikipedia
Eric W. Weisstein. "Axiom of Choice." From *MathWorld*--A Wolfram Web Resource.
http://mathworld.wolfram.com/AxiomofChoice.html

If all members of a set x are non-empty sets, then we can try to define a **choice function** f that assigns to each $y\in x$ some $f(y)\in y$. Can we hope to define a choice function for each collection x of non-empty sets? At least, we

can postulate, that such a function always exists. In this way we obtain the **Axiom of Choice** (AC):

$$\forall x(\forall y(y\in x \rightarrow y \text{ not empty}) \rightarrow \exists f(f \text{ is function} \wedge domain(f)=x \wedge \forall y(y\in x \rightarrow f(y)\in y)))$$

In 1904, Zermelo used this "principle of arbitrary choice" explicitly to prove that each set can be well-ordered.

E. Zermelo. Beweiss, dass jede Menge wohlgeordnet werden kann. "Math. Annalen", 1904, Vol. 59, pp. 514-516 (see also comments by Stanley N. Burris).

The ordering "<" of some set x is called a **well-ordering**, if and only if each non-empty subset of x contains a minimum member under "<". For example, the set of all natural numbers ω is well ordered by the membership relation "∈" . Finite sets can be **double-well-ordered**, see above.

This provocative paper by Zermelo was by far not the first time in the history when something like the "principle of arbitrary choice" was used in mathematical proofs. (About the way, how this principle was used by the founder of set theory – Georg Cantor, see above.) Still, Zermelo dared to state this principle explicitly and in its most unrestricted form.

Exercise 2.18. a) Prove the converse statement: if the union ∪x is well-ordered (by some relation "<"), then there is a choice function for x.

b) Derive from AC that each infinite set contains an infinite countable subset. Which definition of infinite sets would you prefer to use here?

Note that **AC is not a comprehension axiom**. The choice function f is **not** defined by some formula F(x, y, z) expressing that f(y)=z. The existence of f is merely postulated. The term "principle of arbitrary choice" emphasizes the extremely non-constructive nature of AC. I.e. we assume that we are able to make an infinite number of choices without having any guiding rule. (For the long history of hot discussions "around the Axiom of Choice" – non-measurable sets, the Banach-Tarski Paradox etc. – see Medvedev [1982]).

We can "judge" AC as we please, yet as an axiom of set theory it is absolutely safe: in 1938 Kurt Gödel proved that

"If ZF+AC would be an inconsistent theory, then so would be ZF".

K. Gödel. The consistency of the axiom of choice and of the generalized continuum hypothesis. "Acad. U. S. A.". 1938, Vol. 24, pp.556-557 (see also Section 2.4.1 below).

The set theory ZF+AC is denoted traditionally by **ZFC**. By using the axioms of ZFC all theorems of Cantor's intuitive set theory can be proved.

Mathematicians may be interested to verify this themselves – just follow an excellent concise book Jech [1971]. You will be inspired to do yourselves 90% of the technical work.

Since the end of XIX century we know that all the other theories of common mathematics can be reformulated in set theory. **This completes the first stage**

of Hilbert's program: convert all the existing mathematics into a formal theory (namely, ZFC).

2.4. Around the Continuum Problem

2.4.1. Counting Infinite Sets

Trying to prove the Continuum Hypothesis, Cantor developed his **theory of transfinite ordinal numbers**. The origin of this concept was described in Section 2.1. The idea behind is simple enough (to explain, but much harder to invent).

Counting a set means bringing of some very strong order among its members. After the counting of a finite set x is completed, its members are allocated in a linear order: x_1, x_2, ..., x_n, where x_1 is the first member, and x_n is the last member of x (under this particular ordering). If we select any non-empty subset y of x, then y also contains both the first and the last members (under the same ordering of x).

But infinite sets cannot be ordered in this way. How strong can be the orderings that can be introduced on infinite sets? For example, consider the "natural" ordering of the set w of all natural numbers. If you separate a non-empty subset y of ω, then you can definitely find the first (i.e. the least) member of y, but for an infinite y you will not find the last element. Can each infinite set be ordered at least in this way?

The precise framework is as follows. The relation R is called a **well-ordering** of the set x, if and only if:

a) R is irreflexive on x: uRu is impossible for $u \in x$.

b) R is transitive on x: $uRv \wedge vRz \rightarrow uRz$ for all $u, v, z \in x$.

c) each non-empty subset of x contains (under R) a minimum member:

$$\forall y(\neg(y=o) \wedge y \subseteq x \rightarrow \exists u(u \in y \wedge \forall v(v \in y \rightarrow u=v \vee uRv))) \quad .$$

Let us take any two different members u, v of x. Apply c) to y={u, v}. If u is the minimum of y, then uRv, and if v is the minimum, then vRu, i.e. each well-ordering is a **linear ordering** (but the converse is not true – verify!).

Can all infinite sets be well-ordered, or some cannot? We know already that Zermelo proved in 1904 that a positive answer to this question is equivalent to the Axiom of Choice.

For counting of finite sets people have invented natural numbers: 0, 1, 2, 3, 4, ... In set theory, traditionally, these numbers are represented by the following sets:

0 = o (the empty set), 1 = {0}, 2 = {0, 1}, 3 = {0, 1, 2}, ...

I.e. the number n+1 is represented by the set $n \cup \{n\}$. In Section 2.3 we introduced a single formula expressing "x is a natural number" and adopted the Axiom of Infinity stating that ω = {x | x is a natural number} is a set.

For counting of infinite sets Cantor invented his transfinite ordinal numbers:

ω (omega, the first transfinite number – it follows after all natural numbers),

ω+1 – follows immediately after ω,

ω+2 – follows immediately after ω+1,

...

ω*2=ω+ω – follows after all ω+n (n – natural number),

ω*2+1 – follows immediately after ω*2,

...

ω*3=ω*2+w – follows after all ω*2+n (n – natural number),

...

ω^2=ω*ω – follows after all ω*n (n – natural number),

...

ω^{ω} – follows after all ω^n (n – natural number),

...

ε_0 – follows after all expressions built of ω and natural numbers by addition, multiplication and exponentiation,

...

etc.

How to define these numbers by a single formula? Let us follow the idea proposed by von Neumann (simplified by Raphael Robinson, Gödel and Bernays), and let us call a set x an **ordinal number**, if and only if:

a) x is a transitive set, i.e. $\forall u \forall v (u \in v \in x \rightarrow u \in x)$,

b) x is well-ordered by the membership relation $a \in b$.

This definition differs from our above definition of natural numbers in just one point: the double-well-ordering is replaced by "simple" well-ordering.

Exercise 2.19 (optional). a) Verify (by using the Axiom of Regularity) that the second part of the ordinal number definition can be replaced by "x is **linearly** ordered the membership relation $a \in b$ ". Do you like a definition of ordinal numbers depending on the Axiom of Regularity?

b) Write a formula expressing "x is ordinal number". How many characters does it contain?

This formula defines the class of all ordinal numbers (or simply, ordinals), that is denoted traditionally by On. The relation b<c for ordinals b, c is defined simply as $b \in c$.

Let us prove that

$$b \in c \wedge c \in On \rightarrow b \in On \ ,$$

i.e. that an ordinal (as a set) consists only of ordinals. We must verify that b is a transitive set, well-ordered by $a \in b$.

Transitivity. Suppose, $u \in v \in b$. Since $v \in b \in c \rightarrow v \in c$ (c is transitive), we have: $u \in v \in c$. Hence, $u \in c$. Now, since u, v, b are all members of c, and $x \in y$ is an ordering of c, then $u \in v \in b \rightarrow u \in b$. Q. E. D.

Well-ordering. Since c is transitive, $b \subseteq c$, hence, $x \in y$ is an ordering on b. Each non-empty subset of b is also a subset of c, i.e. it contains a minimum member under $x \in y$. Q. E. D.

Thus, for each ordinal c: c = {b | b<c} – a generalization of n = {0, 1, 2, ..., n−1}.

Exercise 2.20. Verify that:

a) If b is an ordinal, then $b \cup \{b\}$ also is an ordinal (moreover, it is the least ordinal greater than b). Traditionally, $b \cup \{b\}$ is denoted by b+1.

b) Each non-empty class of ordinals contains a minimum member (the intersection of all ordinals of the class). Thus, On is well-ordered by "<".

c) If x is a set of ordinals, then ∪x also is ordinal (moreover, it is the least upper bound of x).

Hence, On is proper class. Indeed, if On=x, then ∪x is the least upper bound of On, but ∪x+1 is an ordinal greater than ∪x. This was the first published paradox of set theory (Cesare Burali-Forti published it in 1897).

An ordinal b is called **successor ordinal**, if and only if b=c+1 for some c. All the other ordinals are called **limit ordinals**. The least limit ordinal is 0 (zero, or empty set). The second limit ordinal is ω (the set of all natural numbers).

Exercise 2.21. Verify that:

a) The second limit ordinal is ω. I.e. verify that ω is ordinal, and if n<ω, then n

is a natural number.

b) If b is limit ordinal, then b=∪b.

Now we can prove easily the

Principle of Transfinite Induction. Let A be a class of ordinals such that: a) $0\in A$, b) if $b\in A$, then $b+1\in A$, c) if $x\subseteq A$, then $Ux\in A$. Then A=On.

This is a generalization of the well-known induction principle for natural numbers.

Proof. If A is not On, then let b be the least ordinal not in A. Of course, b≠0. If b=c+1, then $c\in A$, and $b\in A$. If b is a limit ordinal, then all c<b are in A, i.e. $b\subseteq A$, and $Ub\in A$. But $Ub=b$. Q.E.D.

Now, we can define new functions "by induction", or, more, precisely, by recursion. In the formulation below, the function G(x) serves as the *recursion step* (and as the recursion basis as well): if we know already the values F(c) for all c<b (i.e. the values of the function F|b), then G "calculates" F(b).

By F|b we denote here the restriction of the function F to the domain b, i.e.

$$F|b=\{(u,v)|u\in b\wedge(u,v)\in F\} \quad .$$

In the formulation below, G may depend on additional parameters. Then, of course, F will depend on these parameters as well.

Exercise 2.22 (optional). Prove the **Theorem of Transfinite Recursion**: for any function G(x) with $domain(G)=V$, there is a unique function F(x) such that $domain(F)=On$, and for all $b\in On$: $F(b)=G(F|b)$.

Hint. First, define the class B of functions f(x), having the property

$$domain(f)\in On\wedge\forall a(a\in domain(f)\rightarrow f(a)=G(f|a)) \quad .$$

Verify, that $F=U\,B$ is a function, and that it possess both the properties required. End of **Hint**.

Like as natural numbers allow counting of finite sets, it appears, ordinal numbers allow "counting" of arbitrary well-ordered sets:

Exercise 2.23. Let x be a set well-ordered by some relation r. Prove that there exists a unique ordinal b such that the structure (x, r) is isomorphic to the structure (b, <). (Hint: use transfinite recursion to build a "counting" function from On onto x).

For finite sets, ordering and counting are identical operations (in the sense that all well-orderings of a finite set are isomorphic to a unique natural number). For infinite sets, the situation is more complicated. For example, ω, ω+2 and ω*2 are different ordinals, but they can be used only for ordering of countable

sets:

0, 1, 2, 3, ..., n, ... (the set of all natural numbers ordered as ω),

2, 3, ..., n, ..., 0, 1 (the same set ordered as ω+2),

0, 2, 4, ..., 2n, ..., 1, 3, 5, ..., 2n+1, ... (the same set ordered as ω*2).

Even ω^{ω} and ε_0 (see above) allow ordering only of countable sets. Which of these ordinals should we use as "number of members" of countable sets? Of course, we will the first and the least one – ω.

This example justifies the following definition. Let us say that an ordinal b is a **cardinal number** (or, simply, a cardinal), if and only if there is no one-to-one correspondence between b and an ordinal less than b. It would be natural to use cardinal numbers for "counting" of members of infinite sets. You could verify easily that all natural numbers are cardinals, and that w is the least infinite cardinal. But beyond ω – are there more cardinals?

Let us verify that for any cardinal k, there is a cardinal grater than k. Indeed, if you have a cardinal k, then build the power-set P(k), build a well-ordering of it (this is possible, if we assume the Axiom of Choice), and take the least ordinal k_1 isomorphic to this ordering of P(k). According to Cantor's Theorem, k_1 will be a cardinal greater than k.

But this result can be proved **without using the Axiom of Choice**, i.e. in the theory ZF. The idea comes from a 1915 paper by Friedrich Hartogs (1874-1943): let us prove that for each cardinal k the class of all ordinals having one-to-one correspondence with k is a set. Hence, since On is a proper class, there exist cardinals greater than k. The following proof is adapted from Mendelson [1997]:

First let us consider all relations on k. Such relations are subsets of $k \times k$, i.e. they are members of $P(k \times k)$. You can write easily a formula expressing "r is a well-ordering of k". Hence, by an appropriate separation axiom C1 the class of all well-orderings of k is a set $z \subseteq P(k \times k)$. From our Exercise 2.23 we know that for each $r \in z$ there exists a unique ordinal b such that (k, r) is isomorphic to (b, <). This correspondence can be expressed as a formula F(r, b). Now we can apply an appropriate replacement axiom C6, and conclude that the image F"z is a set. But F"z is exactly the class of all ordinals having one-to-one correspondence with k. Q.E.D.

Alephs

Thus we have proved in ZF (i.e. without the Axiom of Choice) that for each cardinal *k* there are cardinals greater than *k*. The first infinite cardinal ω (the

set of all natural numbers) is denoted traditionally also by $\aleph_0$. This cardinal "measures" the cardinality (“number” of members) of countable sets. The first uncountable cardinal is denoted by $\aleph_1$, the second uncountable cardinal – by $\aleph_2$, etc. After all $\aleph_n$ (with n – a natural number) follows the cardinal $\aleph_\omega$, etc.

Exercise 2.24. a) Verify that $\aleph_\omega = U\{\aleph_n | n \in \omega\}$.

b) Prove that, generally, if x is a set of cardinals, then $\cup x$ is a cardinal.

Having these results we can define $\aleph_b$ for each ordinal b:

$\aleph_0 = \omega$,

$\aleph_{b+1}$ = the least cardinal greater than $\aleph_b$,

$\aleph_b = U\{\aleph_c | c < b\}$ for a limit ordinal b.

Exercise 2.26. Verify (in ZF!) that "all cardinals are alephs", i.e. if k is a cardinal, then $k = \aleph_b$ for some ordinal b.

Thus we have a somewhat modernized version of Cantor's apparatus for counting of infinite sets, which he developed trying to prove the Continuum Hypothesis. Each well-ordered infinite set is in one-to-one correspondence with some aleph. If we adopt the Axiom of Choice, then each set can be well-ordered, and we can extend the above assertion: each infinite set is in one-to-one correspondence with some aleph.

Having Cantor's "aleph scale", what could we say about the Continuum Hypothesis? If we adopt the Axiom of Choice, then the set of all real numbers can be well-ordered, i.e. it is in one-to-one correspondence with some cardinal c. But this cardinal must be somewhere on the aleph scale:

$$\exists b (c = \aleph_b) \quad .$$

We know already that b>0. The Continuum Hypothesis asserts that each infinite set of real numbers is either countable, or its cardinality is equal to c. Hence, on the aleph-scale there are no cardinals between $\aleph_0$ and c, i.e. $c = \aleph_1$. Thus, to prove the Continuum Hypothesis, we must establish a one-to-one correspondence between two fixed sets – the set of all real numbers, and $\aleph_1$. Of course, this conclusion strengthened Cantor's trust in a forthcoming solution of the Continuum Problem...

But the only (small!) success came as late as in 1905 when J. König proved his remarkable theorem (for details see Jech [1971]), and concluded from it that c is not $\aleph_\omega$ (etc.: c is not $\aleph_{\omega \cdot 2}$, not $\aleph_{\omega \cdot 3}$, ..., not $\aleph_{\omega \cdot \omega}$, etc., not $\aleph_b$ for a countable limit ordinal b).

J. König. Zum Kontinuum-Problem. "Math. Annalen", 1905, Vol.60, pp.177-180.

That is almost all we know today. Nobody has succeeded in proving that c is not $\aleph_2$, not $\aleph_3$ etc.

But today we know the cause of these difficulties...

The first step of the solution is due to Kurt Gödel who proved in 1938 that one can assume in ZF the Axiom of Choice (AC) and the Continuum Hypothesis (CH) safely: if the theory ZF is consistent, then so is ZF+AC+CH (i.e. ZFC+CH).

K. Gödel. The consistency of the axiom of choice and of the generalized continuum hypothesis. "Acad. U. S. A.", 1938, Vol 24, pp.556-557.

I.e., if we could derive a contradiction from AC and/or CH, then we could derive a contradiction already from the axioms of ZF. The consistency conjecture of a theory T is denoted traditionally by Con(T). In these terms, Gödel's result is put as follows:

$$\mathrm{Con(ZF)} \rightarrow \mathrm{Con(ZF+AC+CH)}.$$

It should be noted that Gödel proved not only the "safety" of CH. He proved simultaneously – and by the same method – the "safety" of the "black magic" – the Axiom of Choice! You can criticize AC as impossible or false, but as a means of mathematical reasoning it is as safe as are the axioms of ZF!

Note. In fact, Gödel proved more than Con(ZF) → Con(ZF+AC+CH). The so-called **Generalized Continuum Hypothesis** (GCH) is formulated as follows: for any ordinal α,

$$|P(\aleph_\alpha)| = \aleph_{\alpha+1} \quad .$$

If α=0, then we obtain simply CH. Gödel proved that

$$\mathrm{Con(ZF)} \rightarrow \mathrm{Con(ZF+AC+GCH)}.$$

Gödel's method is derived from an idea by D. Hilbert, published in 1925:

D. Hilbert. Über das Unendliche. "Math. Annalen", 1925, Vol. 95, pp. 161-190.

Namely, if you are continuously failing in **building** of sets with cardinalities between $\aleph_0$ and c, then you may try to prove that there are no "constructible" sets having this property. I.e. maybe, such sets do exist, but they cannot be **constructed**? Maybe, this kind of proof will be easier than a 100% proof of the Continuum Hypothesis?

Gödel's operations (a version from Jech [1971])

$G_1(u, v) = \{u, v\}$ (pairing),

$G_2(u, v) = u - v$ (difference of sets),

$G_3(u, v) = u \times v$ (product of sets),

$G_4(u) = \mathrm{domain}\ (u)$,

$G_5(u) = \{(t_1, t_2) \mid t_1, t_2 \in u \wedge t_1 \in t_2\}$ (membership as projected on u),

$G_6(u) = \{(t_1, t_2, t_3) \mid (t_2, t_3, t_1) \in u\}$,

$G_7(u) = \{(t_1, t_2, t_3) \mid (t_3, t_2, t_1) \in u\}$,

$G_8(u) = \{(t_1, t_2, t_3) \mid (t_1, t_3, t_2) \in u\}$ (enable permutations).

Here, (t_1, t_2, t_3) is defined, of course, as $((t_1, t_2), t_3)$. How could we define the class of all sets that can be built "from nothing" by means of Gödel's operations?

closure(u) = {t | $t \in u$, or t can be built from members of u by means of a finite superposition of Gödel's operations}.

Let us define (by transfinite recursion) the following sequence of sets $\{L_b | b \in On\}$:

$L_0 = o$;

$L_b = U\{L_c | c < b\}$ for a limit ordinal b,

$L_{b+1} = \{u | u \subseteq L_b \wedge u \in closure(L_b \cup \{L_b\})\}$.

The second rule of this definition does not create new sets, it only collects all sets that have been created so far. The only creative rule is the third one: members of L_{b+1} are built from members of L_b and of L_b itself by means of finite superpositions of Gödel's operations. The addition of "L_b itself" is necessary, since L_b is closed under Gödel's operations.

The class $L = U\{L_b | b \in On\}$ is called the **constructible universe**, and its members are called **constructible sets** (i.e. sets that can be built "from nothing" by means of Gödel's operations). It appears that L contains all ordinals, i.e. it is a proper class.

Gödel proved two theorems that are equivalent to the following (proofs can be found, for example, in Jech [1971]):

1) ZF proves: if all sets were constructible, then AC and CH (and even, GCH) were true.

2) In L, all axioms of ZF are true, i.e. if ZF is consistent, then so is ZF+ "all sets are constructible".

Hence, we can add the Axiom of Choice and Continuum Hypothesis to ZF as axioms safely. And we **cannot hope to disprove the Continuum Hypothesis** in ZFC.

Traditionally, V=L is used as a shortcut for the statement "all sets are

constructible". By using this shortcut, the above theorems can be put as follows:

1) ZF + V=L proves AC and CH (and even GCH).

2) Con(ZF) → Con(ZF + V=L).

Hence, Con(ZF) → Con(ZF+AC+CH), or, if you like it better: Con(ZF) → Con(ZFC+CH), or Con(ZF) → Con(ZFC + $c=\aleph_1$).

At first glance, Gödel's collection of set operations introduced above seems "accidental". But the following result shows that this is not the case:

If some class M is a model of ZF (i.e. all axioms of ZF are true in M), and M contains all ordinals, then $M \supseteq L$ (i.e. M contains all the constructible sets).

For details, see Jech [1971]. Hence, in a sense, the sets that can be built "from nothing" by using Gödel's technical operations, form the minimum universe of sets for which all axioms of ZF are true. And hence, Gödel's collection of operations is not an accidental one at all. In some other books on set theory you can find different collections of operations that generate the same constructible universe L.

Open problem? Let us consider any finite collection s of absolute (see Jech [1971]) operations, and let us define the class L(s) as above. We know already that if L(s) were a model of ZF containing all ordinals, then $L(s) \supseteq L$. But, maybe, under these conditions, L(s)=L?

Gödel's result of 1938 did not contradict Cantor's opinion (Cantor died in 1918) that the Continuum Hypothesis "must be" provable. But some 25 years later – in 1963 Paul Cohen (1934-2007) invented a new method (the famous method of forcing), which allowed to prove that

Con(ZF) → Con(ZFC + $c=\aleph_2$),

Con(ZF) → Con(ZFC + $c=\aleph_3$),

...

Con(ZF) → Con(ZFC + $c=\aleph_{b+1}$),

for any finite or countable ordinal b. Hence, you can adopt safely as an axiom any of the following assertions:

$$c=\aleph_1, c=\aleph_2, c=\aleph_3, \ldots ,$$

and even (a joke by N.N. Luzin, see Keldysh [1974]) that $c=\aleph_{17}$.

Some facts about this event from Infinite Ink: The Continuum Hypothesis by Nancy McGough:

April 2, 1934	Cohen, Paul born
April, 1963	Cohen circulated notes about independence of CH
May 3, 1963	Cohen lectured on independence of CH
July 4, 1963	Cohen's lecture "Independence Results in Set Theory" at the International Symposium on the Theory of Models, University of California, Berkeley, June 25--July 11, 1963.

P. J. Cohen. The Independence of the Continuum Hypothesis. "Proc. Nat. Acad. Sci. U. S. A.", 1963, vol. 50, pp.1143-1148.

P. J. Cohen. The Independence of the Continuum Hypothesis. II."Proc. Nat. Acad. Sci. U. S. A." 1964, vol. 51, pp. 105-110.

Cohen's method of forcing allows proving also that the Axiom of Choice (of course!) cannot be derived from the (normal!) axioms of ZF. Cohen proved this in a very strong form:

$$\mathrm{Con(ZF)} \rightarrow \mathrm{Con(ZF + Q)},$$

where Q asserts the following: there is a countable set x consisting of unordered pairs (members of these pairs being sets of real numbers) such that there is no selection function for x. Hence, the axioms of ZF alone cannot prove the existence of a selection function even for a countable set of unordered pairs!

For a platonist interpretation of Cohen's results: click here.

My formalist interpretation: We have proved (in ZFC) that there is an ordinal b such that $c=\aleph_b$, but (using only axioms of ZFC) we are not able to "calculate" the exact unique value of b. Does it mean that our axioms do not conform to the "true world of sets"? To avoid a dead-end, I would propose better to think that **our axioms are not perfect**, so let us simply try to improve them – and ignore the mystical "true world of sets". And it appears that we can have here different (even contradictory!), yet very exciting development scenarios.

2.4.2. Axiom of Constructibility

The first scenario – let us adopt Gödel's technical statement V=L as an axiom of set theory and call it the **Axiom of Constructibility**. I.e. let us assume that

there are only constructible sets in the "world of sets", and let us work in the theory ZF+V=L. As an axiom, V=L is very powerful: it implies the Axiom of Choice and allows proving of the Continuum Hypothesis. It allows solving also of some other problems that were proved as undecidable for ZFC (for a detailed account – see Devlin [1977]). Let us consider one of them – the problem formulated by Mikhail Yakovlevich Suslin (1894–1919, the paper was published in 1920).

Suslin's Problem. Let (p, <) be a linearly ordered set such that:

a) p does not contain neither minimum, nor maximum members.

b) p is dense (i.e. if $x, y \in p$ and x<y, then there is $z \in p$ such that x<z<y).

c) p is complete (i.e. each bounded non-empty subset of p has (in p) the least upper bound and the greatest lower bound.

d) Every set of non-intersecting intervals of p is finite or countable.

The set of all real numbers possesses these properties. Suslin conjectured that every ordered set (p, <) having the properties (a, b, c, d) must be isomorphic to the set of all real numbers (Suslin's Hypothesis – SH).

Exercise 2.27 (optional). Show (in ZFC) that SH is equivalent with the following assertion: every linearly ordered set (p, <) possessing the properties (a, b, c, d) contains a countable dense subset.

Suslins's problem possesses the "taste" of the Continuum Problem: it seems involved in "the very nature" of the real number system, and hence, if our axioms are perfect, it "must be" proved from the axioms.

But this is not the case – Suslin's problem is undecidable for ZFC:

$$Con(ZF) \rightarrow Con(ZFC + SH) \quad ,$$

$$Con(ZF) \rightarrow Con(ZFC + \neg SH) \quad .$$

The first result was proved in 1971:

R. Solovay, S. Tennenbaum. Iterated Cohen extensions and Suslin's problem. "Annals of Math.", 1971, vol.94, pp.201-245,

and the second one – in 1968:

R. Jensen. Suslin's hypothesis is incompatible with V=L. "Notices Amer. Math. Soc.", 1968, vol.15, p.935.

Jensen proved that the Axiom of Constructibility allows disproving of SH, i.e. we can derive from V=L the existence of a linearly ordered set (p, <) that possess the properties (a, b, c, d), but is not isomorphic to the set of all real numbers (see a version of this proof in Jech [1971]).

Thus, another very natural problem that "must be" solved by a perfect axiom

system of set theory, is undecidable for ZFC, but it can be solved in ZF+V=L. Hence, ZF+V=L is a "better" set theory than ZFC?

Gödel never believed in V=L as a possible axiom of set theory. So do most people today. Maybe, they do not like V=L as a very long formula? If you wish, verify that the full form of V=L in the language of set theory contains thousands of characters (I did this work in 1975 by using a mainframe computer having 256K memory).

Open problem? As we know from the exercise 2.11, the full (i.e. comprehension) form of the infinity axiom is longer than "it should be". But it can be replaced by a much shorter (non-comprehension) axiom. How short could be made a replacement of V=L?

The second argument against V=L as an axiom: it is not an "obvious" assertion about sets – "why" should all sets be constructible? Ask in ZF or in ZFC: how many constructible sets of natural numbers exist? Or (it is the same): how many constructible real numbers exist? In ZF+V=L, there are only constructible real numbers, i.e. there are uncountably many constructible real numbers. On the other hand, according to an unpublished result of Azriel Levy from 1963:

$$\mathrm{Con}(\mathrm{ZF}) \rightarrow \mathrm{Con}(\mathrm{ZFC}+\mathrm{CH}+\text{"the set of all constructible real numbers is countable"})$$

I.e. you may think safely also that there are only countably many constructible real numbers. For details, see

A. Mostowski. Constructible sets with applications. North-Holland, 1969 (Russian translation available).

But why couldn't we investigate the consequences of all sets being constructible? Is ZF+V=L a perfect set theory? Maybe, it also contains its own "anomalies"?

For example, in ZF+V=L we can prove not only (as in ZFC) that each set can be well-ordered, but even more – that **there is a definable well-ordering of the class of all sets.** I.e. there is a (proper class) function F: On→V such that $\forall x \exists b (b \in On \wedge F(b) = x)$. Thus, F enumerates all sets by using ordinals as "numbers".

Hence, in ZF+V=L, the set of all real numbers can be well-ordered as well. But some people think that well-ordering contradicts "the very nature" of real numbers – because of the extreme density and completeness of the natural ordering of these numbers. The assertion "real numbers cannot be well-ordered" would be a poor axiom, but it could serve as a constraint that some people would use for selecting "better" axioms of set theory. These people would reject not only V=L, but also the Axiom of Choice and Continuum Hypothesis (any of these three implies that all real numbers can be well-ordered). Perhaps, they would prefer another exciting alternative – the

2.4.3. Axiom of Determinacy

(An earlier term – *Axiom of Determinateness*.)

This is an alternative scenario of developing set theory proposed in 1962 by Jan Mycielski and Hugo Steinhaus. The Axiom of Determinacy (AD) contradicts the Axiom of Choice.

J. Mycielski, H. Steinhaus. A mathematical axiom contradicting the axiom of choice. "Bull. Acad. Polon. Sci. Ser. Sci. Math. Astronom. Phys.", 1962, vol. 10, pp. 1-3.

So, let us explain AD. Its terminology is based on infinite games proposed in 1953 by David Gale and Frank M. Stewart (1917-2011):

D. Gale, F. M. Stewart. Infinite games with perfect information. "Ann. Math. Studies", Princeton, 1953, vol.28, pp.254-266.

Let x is any set of real numbers. Let us associate with x the following (infinite) **game** G_x. The first move: player 1 specifies a binary digit (0 or 1) d_1, after this, player 2 specifies a digit d_2. The second move: player 1 specifies d_3, and player 2 specifies d_4. Etc. Playing in this way *ad infinitum* some real number r ($0 \le r \le 1$) is specified:

$$r = 0.d_1d_2d_3d_4...$$

If $r \in x$, then let us say that the player 1 **wins** the game G_x. Otherwise (i.e., if $\neg(r \in x)$), let us say that the player 2 wins G_x.

What could be called a **strategy** in this kind of games? Of course, it is a function that associates with each finite sequence of binary digits (the previous replies of the opposite player) a single binary digit (the next move). If the player 1 is using some strategy s, then the game will evolve in the following way:

$d_1 = s(o)$ (o – the empty sequence),

d_2 – reply of the player 2,

$d_3 = s(d_2)$,

d_4 – reply of the player 2,

$d_5 = s(d_2, d_4)$,

...

Let us call the strategy s a **winning strategy for the player 1** in the game G_x,

if and only if for any sequence d_2, d_4, d_6, d_8, ... (i.e. for **any** sequence of replies of the player 2) the number

$0.s(o)d_2s(d_2)d_4s(d_2,d_4)d_6...$

belongs to the set x. The definition of winning strategies for the player 2 is similar.

The set x is called a **determined set**, if and only if for the game G_x there exists either a winning strategy for the player 1, or a winning strategy for the player 2.

Exercise 2.28. a) Show in ZF that if x is a finite or countable set of real numbers, then the player 2 has a winning strategy. Hence, all **countable sets are determined**. In ZF, one can prove the determinateness also of many uncountable sets of real numbers (see Kanovei [1984] or Kleinberg [1977]).

b) By using the **Axiom of Choice**, show that there exist **undetermined sets** of real numbers.

Since the existence of undetermined sets was never been proved without the Axiom of Choice, some people started to think that the assertion

"every set of real numbers is determined"

(the **Axiom of Determinacy**, or AD) is consistent with the axioms of ZF, and that the set theory ZF+AD is worth of exploring.

However, as an axiom of *set theory*, AD may seem somewhat unusual: it is dealing with sets of reals only, while AC is dealing with all kinds of sets.

One more argument in favor of AD is its representation by using an infinite sequence of quantifiers (see Kanovei [1984]):

$$\exists a_0 \forall a_1 \exists a_2 ... (a_0, a_1, a_2, ...) \in x \vee \forall a_0 \exists a_1 \forall a_2 ... \neg((a_0, a_1, a_2, ...) \in x) \quad .$$

The first part of this "formula" asserts the existence of a winning strategy for the player 1, the second part – the existence of a winning strategy for the player 2. Rewrite the second part in the following way:

$$\exists a_0 \forall a_1 \exists a_2 ... (a0, a1, a2, ...) \in x \vee \neg \exists a_0 \forall a_1 \exists a_2 ... (a0, a1, a2, ...) \in x \quad ,$$

and you will have ... the Law of the Excluded Middle. If you do not wish to reject the Law of the Excluded Middle, you must simply accept AD as "obvious".

J. Mycielski. On the axiom of determinateness. "Fund. Math.", 1964, vol.53, pp.205-224.

As we know from the Exercise 2.28(b), ZFC proves $\neg AD$, and, equivalently, ZF+AD proves $\neg AC$.

Exercise 2.29 (optional). In the traditional formulation of AD, sequences of

natural numbers are used instead of real numbers. Instead of specifying binary digits the players specify natural numbers. And the determinateness is postulated for every set of sequences of natural numbers. In the above paper, Mycielski denotes this traditional form of AD by AD_ω. The above "binary" form of AD he denotes by AD_2. Prove in ZF that AD_2 and AD_ω are equivalent (or see the paper).

Since AD contradicts the Axiom of Choice (AC), in ZF+AD, “most” sets **cannot be well-ordered**. The “cardinality” of such sets cannot be measured by alephs. In ZF+AD, well-ordered sets (with alephs among them) represent only a restricted part of the entire “world of sets”

AD contradicts the Axiom of Choice (AC) in its full form, but it retains the most useful parts of AC necessary to build a “normal” system of real numbers:

Exercise 2.29a (optional). a) Prove in ZF+AD the so-called countable Axiom of Choice (AC_ω), i.e. prove the existence of choice functions for countable collections of non-empty sets of real numbers.

b) By using AC_ω prove that every infinite set of real numbers contains a countable subset.

c) By using AC_ω prove that the union of a countable collection of countable sets of real numbers is countable.

But the main argument in favor of AD is its extreme power, and the "regularity" of the set theory ZF+AD.

Jan Mycielski and Stanislaw Swierczkowski proved in 1964 that in ZF+AD every set of real numbers is Lebesgue-measurable. (In ZFC, using the Axiom of Choice we can "construct" a non-measurable set of real numbers – the well-known example of G. Vitali.)

J. Mycielski, S. Swierczkowski. On the Lebesgue measurability and the axiom of determinateness. "Fund. Math.", 1964, vol. 54, pp.67-71.

In ZF+AD the **Continuum Hypothesis can be proved** in its initial Cantorian formulation of 1878: every infinite set of real numbers is either countable, or it is equivalent to the entire continuum (i.e. the set of all real numbers). This result follows easily from a theorem about infinite games proved in 1964 by Morton D. Davis:

M. Davis. Infinite games of perfect information. "Ann. Math. Studies", 1964, vol. 52, Princeton, pp.85-101.

In ZD+AD, the continuum cannot be well-ordered (one can prove that any well-ordered set of real numbers is finite or countable). Hence, the cardinality of the continuum (if there is such thing in ZF+AD) is larger than $\aleph_0$, but it

is **incompatible** with $\aleph_1$ and all the other alephs.

Open problem? How short can be made a replacement of AD?

How Strong is AD?

Since ZFC proves $\neg AD$, one can prove easily (in PA) that

$$\text{Con(ZF)} \rightarrow \text{Con(ZF+} \neg AD \text{)}.$$

But, as Mycielski and Swierczkowski established in their above-mentioned 1964 paper, if ZF is consistent, then

Con(ZF) → Con(ZF+AD) **cannot** be proved in ZF.

Thus, unlike AC and V=L, AD is a "strong" hypothesis. How "strong" is it? W. Hugh Woodin established that:

ZF+AD
is equiconsistent with
ZFC + “there are infinitely many Woodin cardinals”.

For (some) details see Section 2.4.4. In particular,

ZF+AD proves Con(ZFC).

Thus, in a sense, ZF+AD is “much much stronger” than ZFC.

Further reading about AD:

Chapter 6 "Determinacy" of Kanamori [2003].

Introduction for people reading in Russian:

V. Kanovei. Axiom of choice and axiom of determinacy. "Nauka Publishers", Moscow, 1984, 64 pp. (in Russian).

2.4.4. Large Cardinal Axioms

Among the people working in set theory professionally, perhaps, currently, the so-called large cardinal axioms represent the most popular scenario for extending of set theory, starting with ZFC. In a sense, people are inventing stronger and stronger versions of the Axiom of Infinity. This scenario is considered as the mainstream of the modern set theory.

For a comprehensive introduction, see Large Cardinal in Wikipedia.

For a complete treatment, see:

A. Kanamori. The Higher Infinite. Large Cardinals in Set Theory from Their Beginnings.

Second Edition. Springer-Verlag, Berlin-Heidelberg, 2003, 536 pp.

T. Jech. Set Theory. 3rd Millenium Edition, Springer-Verlag, 2003, 786 pp.

In general, the approach works as follows. First, some "large cardinal property" is invented, let us denote it by K, and after that, the consequences of the "large cardinal axiom"

Axiom[K] = "there is a cardinal number which possess the property K"

are explored. Thus, one is trying to explore set theories ZFC+Axiom[K] for various large cardinal properties K, in particular, trying to compare them "by strength".

For example, let us say that a cardinal number k is **regular**, if sets of cardinality k cannot be expressed as unions of cardinality less than k, namely, as the unions $\cup x$, such that $|x|<k$ and $(\forall y\in x)|y|<k$. One can verify that $\aleph_0$ and $\aleph_{\alpha+1}$ (for any ordinal α) are regular cardinals. But how about *uncountable limit cardinals*? The first of them – $\aleph_\omega$ is not regular. Indeed, $\aleph_\omega=U\{\aleph_n|n<\omega\}$. Are there *uncountable regular limit cardinals* at all? It appears that the existence of such cardinals cannot be proved in ZFC.

This represents the weakest of the large cardinal properties, it was invented by Felix Hausdorff in 1908: let us say that k is a weakly inaccessible cardinal, if and only if k is an uncountable regular limit cardinal.

The existence of weakly inaccessible cardinals cannot be proved in ZFC. Namely, one can prove (in PA) that:

Con(ZFC)→Con(ZFC + "weakly inaccessible cardinals do not exist").

Thus, to ensure the existence of such cardinals, additional axioms are necessary. For example, let us consider an extended set theory

ZFC+WI = ZFC + "there is a weakly inaccessible cardinal".

It appears, that **if this set theory would be consistent**, then it would be essentially stronger than ZFC. Namely, in ZFC+WI one can build a model of ZFC, hence, ZFC+WI proves Con(ZFC). By Gödel's Second Incompleteness Theorem, this means that in ZFC one cannot prove that Con(ZFC)→Con(ZFC+WI), else ZFC itself would be inconsistent.

The next (by "strength") to the weakest of large cardinal properties was invented in 1930: let us say that k is a strongly inaccessible cardinal, if and only if k is weakly inaccessible, and for all sets x, if $|x|<k$, then $|P(x)|<k$. (In most texts, strongly inaccessible cardinals are called simply inaccessible cardinals.)

Thus, a strongly inaccessible cardinal k is "large", indeed: neither the union operation, nor the power-set operation is able to produce sets of cardinality k

from sets of smaller cardinalities.

Let us consider the corresponding set theory

ZFC+SI = ZFC + “there is a strongly inaccessible cardinal”.

Of course, ZFC+SI (if consistent) is somewhat stronger than ZFC+WI. But, it appears – not very much stronger:

Exercise 2.30 (optional). Verify, that in ZFC+GCH, every weakly inaccessible cardinal is also strongly inaccessible.

Thus, ZFC+WI+GCH and ZFC+SI+GCH are identical set theories, and one cannot hope to “build” a weakly inaccessible cardinal that is not strongly inaccessible – except when GCH is false. One can derive (in PA) from this fact that Con(ZFC+WI)→Con(ZFC+SI). Hence,

$$\mathrm{Con}(\mathrm{ZFC+WI}) \leftrightarrow \mathrm{Con}(\mathrm{ZFC+SI}),$$

i.e. both theories are **equiconsistent**, in a sense, “equally strong”.

How to measure the “power” of large cardinal axioms?

The natural ordering would be by implications of the kind:

ZFC+Axiom[K1] proves: “The class of cardinals with property K1
is a proper subclass of cardinals with the property K2.”.

I.e. every K1 cardinal is K2, but there are K2 cardinals that are not K1. One could say then that the Axiom[K1] is “more powerful in the sense #1” than the Axiom[K2].

A similar as natural approach: let us say that the Axiom[K1] is “more powerful in the sense #2” than the Axiom[K2], if an only if the least cardinal with property K2 is smaller than than the least cardinal with property K1.

However, as the examples below are showing, surprisingly, these two “senses” do not correlate, and in neither of these “senses” the known large cardinal axioms are linearly ordered.

This is because another criterion of the “power” is considered as a more appropriate – the so-called “consistency strength” of large cardinal axioms. The known large cardinal axioms seem to be linearly ordered by their consistency strength!

Case 1. Let us say that the axioms K1 and K2 are **equiconsistent**, if and only if one can prove (in PA?) that

$$\mathrm{Con}(\mathrm{ZFC+K1}) \leftrightarrow \mathrm{Con}(\mathrm{ZFC+K2}).$$

Equiconsistency does not imply the equivalence of the properties (as in the

case of strongly and weakly inaccessible cardinals).

Case 2. Let us say that the **consistency strength** of the axiom K1 is **greater** than the one of K2, if and only if

ZFC+K1 proves Con(ZFC+K2)

(usually, by building in ZFC+K1 a model of the weaker theory ZFC+K2). It follows then from Gödel's Second Incompleteness Theorem that ZFC+K2 (if consistent) cannot prove that

Con(ZFC+K2)→Con(ZFC+K1).

The known large cardinal axioms seem to be linearly ordered by their consistency strength (see below). However, sometimes, the existence of cardinals with the "stronger" property K1 does not imply the existence of cardinals with the "weaker" property K2 (see example below). Nor does a greater consistency strength of K1 guarantee that every cardinal with property K1 possess also the property K2 (see examples below).

Lemma. The **consistency strength relationship is transitive:** if ZFC+K1 proves Con(ZFC+K2), and ZFC+K2 proves Con(ZFC+K3), then ZFC+K1 proves Con(ZFC+K3)

Proof. Assume, there is a proof of a contradiction from the axioms of ZFC+K3. Verify in PA, how the axioms of ZFC+K2 are used in this proof, and you will obtain a PA-proof of $\neg Con(ZFC+K3)$. Convert this PA-proof into a proof of $\neg Con(ZFC+K3)$ from the axioms of ZFC+K2.

ZFC+K2 proves Con(ZFC+K3), hence, there is a proof of Con(ZFC+K3) from the axioms of ZFC+K2.

Thus, we know, how to convert a proof of a contradiction from the axioms of ZFC+K3 into a proof of a contradiction from the axioms of ZFC+K2. Let us formalize this argument in PA. Thus,

$$\neg Con(ZFC+K3) \rightarrow \neg Con(ZFC+K2)$$

and

$$Con(ZFC+K2) \rightarrow Con(ZFC+K3)$$

are theorems of PA. Hence, they are theorems of ZFC+K1 as well.

And hence, since ZFC+K1 proves Con(ZFC+K2), it proves Con(ZFC+K3) as well. Q.E.D.

The Tower

For large lists of large cardinal properties considered today, see List of large

cardinal properties in Wikipedia and Kanamori [2003]. A subset of these lists is represented below. The axioms are given in ascending order of their consistency strengh.

ZFC+"*weakly inaccessible exists*" proves Con(ZFC).

Every (strongly) inaccessible cardinal is weakly inaccessible.

Con(ZFC+"*inaccessible exists*")↔Con(ZFC+"*weakly inaccessible exists*").

Every Mahlo cardinal (invented in 1911 by Paul Mahlo) is strongly inaccessible.

ZFC+"*Mahlo exists"* proves Con(ZFC+"*inaccessible exists*").

Every weakly compact cardinal is Mahlo.

ZFC+"*weakly compact exists*" proves Con(ZFC+"*Mahlo exists"*).

Every Ramsey cardinal is weakly compact.

ZFC+"*Ramsey exists"* proves Con(ZFC+"*weakly compact exists"*).

Every measurable cardinal is Ramsey.

ZFC+"*measurable exists"* proves Con(ZFC+"*Ramsey exists"*).

Howeve, the seeming harmony breaks down at higher levels:

ZFC+"*Woodin exists"* proves Con(ZFC+"*measurable exists"*),

ZFC+"*Woodin exists"* proves "*measurable exists",*

but:

Every Woodin cardinal is Mahlo, but **not necessarily weakly compact**! The least Woodin cardinal is **not** weakly-compact (Jech [2003], Lemma 34.2). But, under each Woodin cardinal there are "many many" (a stationary set of) measurable cardinals (Jech [2003], p. 648). **This represents the first striking anomaly of the large cardinal tower!**

But let us continue:

Every supercompact cardinal is Woodin.

ZFC+"*supercompact exists"* proves Con(ZFC+"*Woodin exists"*).

ZFC+"*huge exists"* proves Con(ZFC+"*supercompact exists"*),

but:

Every huge cardinal is measurable, but **not necessarily supercompact! And the existence of huge cardinals does not imply the existence of supercompacts!** If both exist, the least huge cardinal is smaller than the least supercompact! **This represents the second striking anomaly of the large**

cardinal tower!

Every I3 cardinal is huge.

ZFC+"*I3 exists*" proves Con(ZFC+"*huge exists*").

Every I2 cardinal is I3.

ZFC+"*I2 exists*" proves Con(ZFC+"*I3 exists*").

Every I1 cardinal is I2.

ZFC+"*I1 exists*" proves Con(ZFC+"*I2 exists*").

Every I0 cardinal is I1.

ZFC+"*I0 exists*" proves Con(ZFC+"*I1 exists*").

The consistency problem mentioned above many times, is essential here. Because, the strongest ("next to *I0*") of the large cardinal axioms invented so far contradicts ZFC, i.e. the corresponding set theory

ZFC + "there is a Reinhardt cardinal"

is inconsistent. In other words, in ZFC, one can *prove* that Reinhardt cardinals do not exist.

But all the other large cardinal axioms are still believed to be consistent with ZFC.

Fascinating...

Professionals working on large cardinals seem to be fascinated by the following phenomenon: when compared by their consistency strength, **large cardinal axioms seem to be linearly ordered (in fact, even well-ordered)**. This is proved already for the most of cases. Thus, it seems, we have a tower ("The Tower"?) of stronger and stronger axioms of set theory.

Because of this fact, some people believe that large cardinal axioms represent the only "right" way of developing the set theory, the way to discover the "true world of sets", thus overriding the barriers set by the incompleteness phenomenon.

Large Cardinals Axioms and Determinacy

For details, exposed compactly, see:

P. Koellner. The Continuum Hypothesis. In: ZALTA, E. N. (ed.) *The Stanford Encyclopedia of Philosophy. Summer 2013 Edition.* [Online] Available from http://plato.stanford.edu/archives/sum2013/entries/continuum-hypothesis/.

P. Koellner. Large Cardinals and Determinacy. In: ZALTA, E. N. (ed.) *The Stanford Encyclopedia of Philosophy. Spring 2014 Edition.* [Online] Available from http://plato.stanford.edu/archives/spr2014/entries/large-cardinals-determinacy/.

As already mentioned above, by using large cardinals, one can determine the consistency strength of the Axiom of Determinacy, i.e. of the set theory ZF+AD. Building on the work by Donald A. Martin, John R. Steel and himself, W. Hugh Woodin established in 1985 that

ZF+AD is equiconsistent with
ZFC + "there are infinitely many Woodin cardinals".

Thus, if one is ready to accept a pretty powerful large cardinal axiom as a "safe" axiom, then one could accept AD "safely" as well. And conversely, of course, ...

For (some) details of the proof see Theorem 32.16 in Kanamori [2003] and Theorem 33.27 in Jech [2003].

However, the connection between determinacy and large cardinals appears to be even deeper. While AD is asserting that "every set of real numbers is determined" (and hence, it contradicts ZFC), the somewhat weaker axiom $AD^{L[R]}$ ("in L[R], every set of real numbers is determined"), it seems, can be assumed in ZFC without contradictions.

More precisely, the argument is as follows. Let us introduce an extended version of Gödel's constructible universe L (see Section 2.4.1) by starting, instead of the empty set o, with the set of all real numbers R. Namely, let us define the following sequence of sets $\{L_\alpha[R] | \alpha \in On\}$:

$L_0[R]=R$ (the definition of Gödel's universe L started with $L_0=o$);

$L_\alpha[R]=U\{L_\beta[R] | \beta<\alpha\}$ for a limit ordinal α ,

$L_{\alpha+1}[R]=\{u | u \subseteq L_\alpha[R] \wedge u \in closure(L_\alpha[R] \cup \{L_\alpha[R]\})\}$.

As we know, one can prove in ZF, that Gödel's constructible universe L satisfies the Axiom of Choice (AC). By assuming a powerful enough large cardinal axiom one can prove in ZFC, that the extended constructible universe $L[R]=U\{L_\alpha[R] | \alpha \in On\}$ satisfies the Axiom of Determinacy.

Namely, let us denote by $AD^{L[R]}$ the formula asserting "in L[R], every set of real numbers is determined" ("every set x, $x \subseteq R, x \in L[R]$ is determined"). It appears that the theory

ZFC +"there is an infinite set of Woodin cardinals
with a measurable cardinal above it"

proves $AD^{L[R]}$.

Thus, if one is believing in most large cardinal axioms, then $AD^{L[R]}$ is one of

the consequences. This was established by Donald A. Martin, John R. Steel and W. Hugh Woodin in 1985.

As the consequence of $AD^{L[R]}$, one obtains that in L(R), all sets of real numbers are Lebesgue-measurable.

On the other hand, by assuming $AD^{L[R]}$ in ZFC, one can obtain models containing large cardinals – Woodin cardinals (one of Woodin's unpublished results?). Thus, if one is believing that $AD^{L[R]}$ "holds", then the existence at least of some large cardinals is one of the consequences.

In this way, the possible controversy between ZFC and ZF+AD was solved in favour of ZFC, and exploring of the consequences of large cardinal axioms in ZFC remains the mainstream of set theory.

However, did $AD^{L[R]}$ already "hold" in 1873, or was that decision made much later?

The Future of Set Theory

The axiom of *Projective Determinacy* asserts that AD holds for the so-called projective sets, and is thus somewhat weaker than $AD^{L[R]}$. W. Hugh Woodin commented on it as follows:

"Should the axiom of *Projective Determinacy* be accepted as true? ... Accepting *Projective Determinacy* as true does not deny the study of models in which it is false. ... I believe the axiom of *Projective Determinacy* is as true as the axioms of Number Theory. So I suppose I advocate a position that might best be described as *Conditional Platonism*." (p. 32)

W. H. Woodin. Set Theory after Russell; The journey back to Eden. September 30, 2003. In: LINK, G. (ed.) *One Hundred Years of Russell's Paradox.* De Gruyter Series in Logic and Its Applications, Volume 6. Berlin: De Gruyter, 2004.

If Conditional Platonism is defined *in terms of axioms* that are believed as true, then even some of the formalists might prefer "to work with Woodin", i.e., within a specific fascinating axiomatic framework.

Agreeing "to work with Woodin" could result in involvement with the development of a surprising solution to the Continuum Problem. The expected solution is formulated in terms of "good axioms", although the definition of "goodness" is here technically complicated. Peter Koellner notes:

"To summarize: Assuming the Strong Ω Conjecture, there is a "good" theory of $H(\omega_2)$ and all such theories imply that CH [Continuum Hypothesis] fails. Moreover, (again, assuming the Strong Ω Conjecture) there is a maximal such theory and in that theory $2^{\aleph_0}=\aleph_2$ "

Thus, even the most advanced results of modern set theory (such as Woodin's argument in favour of $2^{\aleph_0}=\aleph_2$) are formulated *in terms of axioms*. Mathematicians might not agree about "what should be believed as true", but

they are in agreement about “what follows from what axioms”.

See also:

Saharon Shellah. The Future of Set Theory. November 2002, available at http://arxiv.org/abs/math/0211397.

W. Hugh Woodin. The search for mathematical truth. November 2010, available at http://logic.harvard.edu/Woodin_talk.pdf.

Exploring the Frontiers of Incompleteness. *Logic at Harvard*, 2011-2012.

The Future of Set Theory?

See the abstract of a conference paper:

N. V. Belyakin. One $omega$-inconsistent formalization of set theory. *The 9th Asian Logic Conference*, 16-19 August, 2005, Novosibirsk, Russia (online abstract),

where the following result is announced:

"From this fact follows, in particular, that the **existence of strongly inaccessible cardinals is refutable in ZF** (marked bold by me – K.P.)."

Thus, contradictions appear already at the **second level** of the large cardinal tower?

Note. The English translation of the Abstract contains a typo: one should remove [in] from the statement “It is not hard to check that *T* is [in]consistent wrt *ZF*+(*existence of strongly inaccessible cardinals*)”.

A detailed proof of the result is still not available. The announced proof method seems plausible. It seems to “follow Poincaré”: it is based on a very strong embedding of the meta-theoretical induction into formal set theory.

In a meta-theory of ZF, one can build, by recursion, a sequence of formulas $\{F_n(\bar{x})|n=0,1,2,...\}$ such that:

$F_0(\bar{x}) \leftrightarrow \psi(\bar{x})$;

$F_{b+1}(\bar{x}) \leftrightarrow \Delta[F_b(\bar{x})]$,

where $\bar{x}$ is a list of variables, $\psi(\bar{x})$ – a formula, $\Delta[X]$ – an algorithm allowing to transform a formula X into another formula. Our naive intuition says that we have here a “class” $C=\{(\bar{x},a)|a\in\omega\wedge F_a(\bar{x})\}$.

However, in general, one cannot hope to convert the sequence $\{F_n(\bar{x})|n=0,1,2,...\}$ into a single formula $F(\bar{x}, a)$, where *a* is variable for natural numbers. Thus, all we have here (in the meta-theory), is a sequence of class definitions $C_n=\{\bar{x}|F_n(\bar{x})\}$.

Let us extend the language of ZF by adding a single predicate variable Q. The quantification over Q will not be allowed, but one will be allowed, in a

formula G, to substitute for Q(y) any formula H($\bar{x}$, y), if the variables of $\bar{x}$ are free in G.

Then any formula Δ(Q, $\bar{x}$, a) containing the variable Q could serve as the above-mentioned algorithm:

$F_0(\bar{x}) \leftrightarrow \psi(\bar{x})$;

$F_1(\bar{x}) \leftrightarrow \Delta(\psi(\bar{x}), \bar{x}, \mathbf{0})$;

$F_2(\bar{x}) \leftrightarrow \Delta(\Delta(\psi(\bar{x}), \bar{x}, \mathbf{0}), \bar{x}, \mathbf{1})$;

$F_{b+1}(\bar{x}) \leftrightarrow \Delta(F_b(\bar{x}), \bar{x}, \boldsymbol{b})$ (where **b** is the numeral for the meta-theoretical natural number b).

Thus, our naive intuition says that for any natural number n,

$F_n(\bar{x}) \leftrightarrow \Delta(\Delta(...\Delta(\psi(\bar{x}), ...)...)...)$.

Let us try to imagine here a single formula F($\bar{x}$, a). Can we hope, for any two given formulas $\psi(\bar{x}), \Delta(Q, \bar{x}, b)$, to build a formula F($\bar{x}$, a) such that:

$F(\bar{x}, 0) \leftrightarrow \psi(\bar{x})$;

$F(\bar{x}, b+1) \leftrightarrow \Delta(F(\bar{x}, b), \bar{x}, b)$?

It should be built somehow from ψ and Δ!

So (a revolutionary idea!), let us introduce a new principle of building formulas: having two formulas $\psi(\bar{x}), \Delta(Q, \bar{x}, a)$, let us build the construct $[\psi(\bar{x}), \Delta(Q, \bar{x}, a), a]$ intended to be a "formula" defining the class

$$C = \{(\bar{x}, a) | a \in \omega \wedge [\psi(\bar{x}), \Delta(Q, \bar{x}, a), a]\} \quad .$$

recursively. I.e. the following two equivalences should be declared as axioms:

$[\psi(\bar{x}), \Delta(Q, \bar{x}, 0), 0] \leftrightarrow \psi(\bar{x})$;

$b \in \omega \rightarrow ([\psi(\bar{x}), \Delta(Q, \bar{x}, b+1), b+1] \leftrightarrow \Delta([\psi(\bar{x}), \Delta(Q, \bar{x}, b), b], \bar{x}, b))$.

For other details, see the Abstract.

Exercise 2.31 (optional, for smart students?). Use ZF + "*there is a strongly inaccessible cardinal*" to build a model of the extended set theory just described. "It is not hard" – as put in the Abstract.

2.4.5. Ackermann's Set Theory

Wilhelm Ackermann's approach to set theory differs from Zermelo's approach. Zermelo adopted those kinds of comprehension axioms that correspond to set construction principles used in real mathematics. Some 50 years later, Ackermann proposed a single elegant principle instead (see axiom A4 below):

W. Ackermann. Zur Axiomatik der Mengenlehre. "Math. Annalen", 1956, Vol. 131, pp. 336-345.

The language of Ackermann's set theory differs from the standard set theory language of set theory in two points:

a) Classes are allowed as values of variables (in the standard set theory language only sets are allowed).

b) A constant V denoting the class of all sets is introduced. The assertion "x is a set" is expressed as $x \in V$.

Ackermann adopts the following axioms:

A1. **Axiom of Extensionality**

$$x = y \leftrightarrow \forall z (z \in x \leftrightarrow z \in y) \quad ,$$
$$x = y \rightarrow \forall z (x \in z \leftrightarrow y \in z) \quad .$$

A2. **Class Construction Axiom Schema**

$$\exists x \forall y (y \in x \leftrightarrow y \in V \wedge F(y, z_{1,} \ldots, z_n)) \quad ,$$

where F is any formula that does not contain x as a free variable. This seems to be the full comprehension schema, but note that x is here a class, not a set! The second feature to be noted: members of x are sets, i.e. you cannot build classes containing proper classes as members.

A3. **Completeness Axiom** for V

$$y \in x \wedge x \in V \rightarrow y \in V \quad ;$$
$$y \subseteq x \wedge x \in V \rightarrow y \in V \quad .$$

I.e. members of sets are sets, and subclasses of sets are sets also.

A4. **Ackermann's Axiom Schema**

$$z_1, \ldots, z_n \in V \wedge \forall y (F(y, z_1, \ldots, z_n) \rightarrow y \in V) \rightarrow$$
$$\exists x (x \in V \wedge \forall y (y \in x \leftrightarrow F(y, z_1, \ldots, z_n))) \quad ,$$

where the formula F does not contain the constant V, and does not contain x as a free variable.

For n=0 we have simply:

$$\forall y (F(y) \rightarrow y \in V) \rightarrow \exists x (x \in V \wedge \forall y (y \in x \leftrightarrow F(y))) \quad .$$

This axiom is dealing with the problem: when does a comprehension axiom define a set? It always defines a class, but when does it define a set? Ackermann's axiom gives an elegant answer to this question: a formula F(y) defines a set, when F does not the constant contain V (of course!), and when you can **prove** that F is satisfied only by sets!

A5. **Axiom of Regularity** (for sets only)

$$x \in V \wedge \exists y (y \in x) \rightarrow \exists y (y \in x \wedge \forall z (z \in x \rightarrow \neg (z \in y))) \quad .$$

Let us denote this set theory by A. If needed, the Axiom of Choice can be added to A.

How to compare such a different set theories as A and ZF? The language of A allows to express many things that the language of ZF does not – mainly because that variables of A range over sets and classes, but variables of ZF – only over sets. Only if you take a formula F of A that does not contain the constant V, and restrict all quantifiers in F to the domain V (i.e. replace any sub-formula $\exists u G(u)$ by a formula $\exists u (u \in V \wedge G(u))$, and any sub-formula $\forall u G(u)$ by a formula $\forall u (u \in V \rightarrow G(u))$, then you obtain a statement within competencies of ZF. Let us denote this restriction of the formula F by F^V.

Azriel Levy, William Nelson Reinhardt (1939-1998)

Levy-Reinhardt's theorem. For all closed formulas F from the language of ZF: A proves F^V, if and only if ZF proves F.

A. Levy. On Ackermann's set theory. *J. Symb. Logic*, 1959, Vol. 24, pp. 154-166 (if A proves F^V, then ZF proves F).

W. N. Reinhardt. Ackermann's set theory equals ZF. *Ann. of Math. Logic*, 1970, Vol. 2, pp. 189-249 (if ZF proves F, then A proves F^V).

Exercise 2.32 (optional). Prove the simpler part of Reinhardt's result, i.e. prove in A the following comprehension axioms of ZF: Separation, Pairing, Union, Power-Set, and Infinity. Do not try to proving of the Replacement Axiom Schema – this is possible, but might appear too complicated.

One of the popular arguments against ZF (or ZFC) as the "right" set theory says that the axioms of ZF have been chosen "*ad hoc*". But Levy-Reinhardt's theorem shows that the real contents of these "*ad hoc*" axioms are not accidental – they equal the contents of a radically different set theory – Ackermann's theory A.

If axioms of ZF are considered as chosen accidentally, then so should be considered the "engineering" principles used in Turing machines. But the equivalence proofs of all the numerous radically different formal concepts of algorithm show that the real contents of Turing's principles are not accidental. This fact is expressed in the famous Church's Thesis: the informal concept of algorithm (or computability) is equivalent to the numerous (mutually equivalent) formal concepts of algorithm.

Perhaps, now a similar "Church's Thesis for set theories" could be formulated: comprehension axioms of ZF are maximal in the sense that no more powerful

consistent set of comprehension axioms is possible? Is this an open problem? Is this true at all?

3. First Order Arithmetic

3.1. From Peano Axioms to First Order Arithmetic

Is the notion of natural numbers something independent, or it depends on other, more complicated mathematical notions – the notion of real numbers, and Cantor's notion of arbitrary infinite sets? I.e., could we define natural numbers separately from the rest of mathematics? At first glance, it seems that the answer should be positive. If natural numbers are the most fundamental mathematical concept (more fundamental than real numbers and Cantor's infinite sets), then an independent definition of them should be possible?

One more reason to search for an independent formalization of natural numbers are paradoxes of set theory. Zermelo-Fraenkel's set theory does not allow you to derive Russell's paradox, Cantor's paradox and Burali-Forti paradox. Still, who could guarantee that there this theory does not contain other inconsistencies? But, have you ever thought about paradoxes in arithmetic of natural numbers? The natural number system seems to be the most reliable branch of mathematics.

So, let us try. Our work will result in the so-called Peano axioms. This terminology is one of the numerous strange naming traditions in mathematics, since: "It is rather well-known, through Peano's own acknowledgment, that Peano borrowed his axioms from Dedekind and made extensive use of Grassmann's work in his development of the axioms." – see p.145 in

Hao Wang. The Axiomatization of Arithmetic. *J. Symb. Logic*, 1957, Vol. 22, N2, pp.145-158.

Indeed, Hermann Grassmann did already about 90% of the entire work already in his book published in 1861:

H. Grassmann. Lehrbuch der Arithmetik, Berlin, 1861.

The traditional recursive definitions of addition and multiplication are due to Grassmann (see Hao Wang [1957]):

x+0=x;

x+(y+1)=(x+y)+1;

x*0=0;

x*(y+1)=(x*y)+x.

In this way addition and multiplication of natural numbers are derived from

one single argument operation x+1. By using these definitions Grassmann proved all the other principal properties of arithmetical operations (associativity, commutativity etc.). Grassmann's axioms included also the **induction principle** (see P3 below). Of course, the hard part of the work was not the invention of the above simple formulas, but the idea that they are necessary.

Richard Dedekind made another attempt in his essay published in 1888:

R. Dedekind. Was sind und was sollen die Zahlen. Braunschweig, 1888 (see also online comments by Stanley Burris).

Dedekind's intention was not an axiomatization of arithmetic, but – giving an "algebraic" characterization of natural numbers as a mathematical structure. However, as he writes in a letter to Dr. H. Keferstein (dated 27 February 1890, the English translation from Hao Wang [1957]):

"For a brief period last summer (1889) Frege's "Begriffschrift" and "Grundlagen der Arithmetik" came, for the first time, into my possession. I noted with pleasure that his method of defining a relation between an element and another which it follows, not necessarily immediately, in a sequence, agrees in essence with my concept of chains [...]. Only, one must not be put off by his somewhat inconvenient terminology."

Dedekind refers here to the following essay by Gottlob Frege, where a similar (to Dedekind's) analysis of the natural number system is given:

G. Frege. Die Grundlagen der Arithmetik. Eine logisch-mathematische Untersuchung über den Begriff der Zahl. Breslau, 1884, 119 pp. (see also online comments by Stanley Burris).

In section 10 of his essay Dedekind proves that his characterization of the natural number system is complete in the sense that any two systems N_1 and N_2 satisfying his conditions (1)-(6) are isomorphic (for details see Appendix 1).

Giuseppe Peano made the next step in 1889 – he converted Dedekind's conditions (1)-(6) into axioms:

G. Peano. Arithmetices pricipia, nova methodo exposita. Torino, 1889, 40 pp. (see English translation in Heijenoort [1967], see also online comments by Stanley Burris).

The modern version of Peano axioms can be put as follows. Let the variables x, y, … range over natural numbers, and let 0 denote the number "zero", Sx – denote the operation x+1, and let the variable F range over arbitrary **sets** of natural numbers. Then the following statements should be called Peano axioms:

P1) $\forall x \neg(0 = Sx)$ (part of Dedekind's condition (5)),

P2) $\forall x \forall y (\neg(x = y) \rightarrow \neg(Sx = Sy))$ (Dedekind's condition (3)),

P3) $0 \in F \wedge \forall x (x \in F \rightarrow Sx \in F) \rightarrow \forall x (x \in F)$ (Dedekind's condition (6), or

the principle of complete induction).

We do not need the remaining Dedekind's conditions (1), (2) and (4) in our list, since they can be derived from the general logical axioms and identity axioms.

One can prove easily (in fact, a theorem of ZF) that any two "systems" N_1 and N_2 satisfying the axioms (P1)-(P3) are isomorphic (see Appendix 1).

One of such "systems" can be constructed in ZF. Let us define 0 as the empty set, Sx – as $x \cup \{x\}$, let the variables x, y, ... range over members of the set ω, and let F range over subsets of ω (i.e. members of the set P(ω)). Then the axioms P1-P3 can be proved as theorems of ZF (see Exercise 2.16).

Still, this is not the kind of formalization we are searching for. Using of arbitrary sets of natural numbers seems to be less dangerous than using of Cantor's general notion of arbitrary infinite sets. Still, there is one-to-one correspondence between sets of natural numbers and real numbers. Can the notion of natural numbers depend on the notion of real numbers? If we believe that it cannot depend, we must try to formalize natural numbers without the reference to arbitrary sets of these numbers.

One of the ways to do this would be replacing the axiom P3 (induction principle) by an axiom schema where the set variable F is "instantiated" by formulas in some formal language L. I.e. we could try restricting the induction principle P3 to some kind of "definable" sets F. It appears that the power of the theory we obtain in this way depends essentially on our choice of the language L.

Successor arithmetic

The minimum version of the language L (let us denote it by L_0) would contain: the constant letter 0, the function letter S, and the predicate letter "=". In this language the notion of term is defined as follows:

a) 0 and any variable is a term;

b) If t is a term, then St also is a term.

Hence, we have here only two types of terms: SS...S0 (i.e. representations of particular natural numbers) and SS...Sx (i.e. representations of functions x+n). Atomic formulas in the language L_0 are built by the following rule:

c) If t_1 and t_2 are terms, then $(t_1=t_2)$ is an atomic formula.

Formulas of the language L_0 are built from atomic formulas by using logical connectors and quantifiers. And we adopt for L_0 the axioms and inference rules of the classical first order logic.

Let us denote by PA_0 the theory in the language L_0 having the following specific axioms:

P00$_0$) $x=x$,

P01$_0$) $x=y \rightarrow y=x$,

P02$_0$) $x=y \rightarrow (y=z \rightarrow x=z)$,

P03$_0$) $x=y \rightarrow Sx=Sy$,

P1$_0$) $\neg(0=Sx)$ (the same as P1),

P2$_0$) $\neg(x=y) \rightarrow \neg(Sx=Sy)$ (the same as P2),

P3$_0$) $B(0) \wedge \forall x(B(x) \rightarrow B(Sx)) \rightarrow \forall x\, B(x)$,

where B is an arbitrary formula of the language L_0 containing x as a free variable, and (maybe) some other free variables (parameters). I.e. $P3_0$ is an axiom *schema* replacing the axiom P3.

The positive features of PA_0:

a) There is an algorithm that allows deciding whether an arbitrary closed formula in the language L_0 is "true" or not. This decision task is PSPACE-complete.

b) PA_0 is a “complete” theory: by using the axioms of PA_0 we can prove each "true" formula of L_0.

On the other hand, PA_0 is a very poor theory.

Exercise 3.1 (for smart students). Prove that PA_0 cannot "express" the relationship x<y. Hints: a) We would say that a formula $LESS(x, y)$ in the language L_0 "expresses" the assertion "x<y", if and only if:

PA_0 proves: $\neg LESS(x, x)$,

PA_0 proves: $LESS(x, Sx)$,

PA_0 proves: $LESS(x, y) \wedge LESS(y, z) \rightarrow LESS(x, z)$.

b) As the first step, prove that no formula $LESS(x, y)$ in the language L_0 can possess the property: $LESS(m, n)$ is "true" if and only if the number m is less than the number n.

Since x<y can be "expressed" as $\exists z(x+ Sz=y)$, the addition of natural

numbers also cannot be discussed in PA_0.

We can try to extend PA_0 by adding to the language L_0 the "missing" predicate letter "<", and by adding to PA_0 three new axioms:

$\neg(x < x), x < Sx, x < y \wedge y < z \rightarrow x < z$.

Unfortunately, in this way we obtain a theory PA_{00} in which the addition of natural numbers still cannot be expressed (see Hilbert, Bernays [1934], section 7.4). I.e. none of the formulas $PLUS(x, y, z)$ in the language of PA_{00} can possess the properties:

a) PA_{00} proves: $PLUS(x, 0, x)$ (i.e. x+0=x),

b) PA_{00} proves: $PLUS(x, y, u) \rightarrow PLUS(x, Sy, Su)$ (i.e. x+Sy=S(x+y)).

Presburger arithmetic

Hence, as the next step, let us try to extend PA_0 by adding to the language L_0 the "missing" function letter "+" and the constant letter 1. Then we will no more need the function letter S (the function Sx can be represented as x+1) and the predicate letter "<" (it can be "expressed" as $\exists z(x + z + 1 = y)$. Let us denote this new language by L_1. Terms of L_1 are defined as follows:

a) The constants 0 and 1, and all variables are terms.

b) If t_1 and t_2 are terms, then (t_1+t_2) also is a term.

Atomic formulas of L_1 are built as $(t_1=t_2)$, where t_1 and t_2 are terms. Since we can use, for example, the expression 2*x−3*y+1=0 as a shortcut for x+x+1=y+y+y, we can say simply that the atomic formulas of L_1 are *linear Diophantine equations*.

Formulas of the language L_1 are built from atomic formulas by using logical connectors and quantifiers. And we adopt for L_1 the axioms and inference rules of the classical first order logic.

After this, we must modify and extend the axioms of PA_0:

P00$_1$) $x = x$,

P01$_1$) $x = y \rightarrow y = x$,

P02$_1$) $x = y \rightarrow (y = z \rightarrow x = z)$,

P03$_1$) $x = y \rightarrow x + 1 = y + 1$,

P1$_1$) $\neg(0=x+1)$,

P2$_1$) $\neg(x=y)\rightarrow\neg(x+1=y+1)$,

P3$_1$) $x+0=x$,

P4$_1$) $x+(y+1)=(x+y)+1$,

P5$_1$) $B(0)\wedge\forall x(B(x)\rightarrow B(x+1))\rightarrow\forall x\,B(x)$.

The axioms $P3_1$ and $P4_1$ represent Grassmann's recursive definition of the addition. The induction schema $P5_1$ and our previous induction schema $P3_0$ look identical, yet actually $P5_1$ is much more powerful – in $P5_1$ we can take as B(x) formulas that contain the addition letter.

Let us denote our new theory by PA_1. It is called sometimes **Presburger's arihmetic**. In 1929 Mojzesz Presburger (1904-1943?) established that:

a) There is an algorithm that allows deciding whether an arbitrary closed formula in the language L_1 is "true" or not.

b) PA_1 is “complete” theory: by using the axioms of PA_1 we can prove each "true" formula of L_1.

c) PA_1 is consistent theory (in this last part of his proof Presburger used only "finitistic" means of reasoning allowed in Hilbert's program).

M. Presburger. Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. *C.R. du I Congr. des Math. des pays Slaves*, Warszawa, 1929, pp.92-101.

Presburger's proof is a non-trivial piece of mathematics (see Hilbert, Bernays [1934], section 7.4). Of course, these results strengthened (in 1929!) Hilbert's trust in a forthcoming solution of the entire problem... Just one more (maybe – technically very complicated) step, and we will have a "finitistic" proof that mathematics as a whole is both consistent and complete. Still, in 1930 a completely unexpected settlement followed... (see Section 5).

In 1974 Michael J. Fischer and Michael O. Rabin proved that any algorithm for deciding, whether an arbitrary closed formula in the language L_1 is "true" or not, requires at least $2^{2^{Cn}}$ units of time for a formula consisting of *n* characters. **Could Hilbert have been discouraged by this result in 1929?**

M. J. Fischer, M. O. Rabin. Super-Exponential Complexity of Presburger Arithmetic. "Proceedings of the SIAM-AMS Symposium in Applied Mathematics", 1974, vol. 7, pp.27-41 (see also Barwise [1977] – Russian translation available)

But unfortunately, again, PA_1 can't serve as a theory we are searching for: in PA_1, the multiplication of natural numbers cannot be expressed. I.e. none of the formulas $MULT(x,y,z)$ in the language of PA_1 can possess the properties:

a) PA_1 proves: $MULT(x,0,0)$ (i.e. x*0=0),

b) PA_1 proves: $MULT(x,y,u) \wedge MULT(x,y+1,v) \rightarrow u+x=v$ (i.e. x*(y+1)=x*y+x)).

This result follows from Gödel's incompleteness theorem, see Section 5.3. Hence, you cannot discuss in PA_1, for example, the notion and the properties of prime numbers.

First order arithmetic

Therefore, as the next step, let us try again – let us extend PA_1 by adding to the language L_1 the "missing" function letter "*". Let us denote this new language by L_2. Terms of L_2 are defined as follows:

a) The constants 0 and 1, and all variables are terms.

b) If t_1 and t_2 are terms, then (t_1+t_2) and (t_1*t_2) also are terms.

Atomic formulas of L_2 are built as $(t_1=t_2)$, where t_1 and t_2 are terms.

Since we can use, for example, the expression $2x^2-3y^2-1=0$ as a shortcut for (1+1)*x*x=(1+1+1)*y*y+1, we can say simply that atomic formulas of L_2 are arbitrary Diophantine equations.

Formulas of the language L_2 are built from atomic formulas by using logical connectors and quantifiers. And we adopt for L_2 the axioms and inference rules of the classical first order logic.

After this, we must modify and extend the axioms of PA_1 accordingly:

$P00_2$) $x=x$,

$P01_2$) $x=y \rightarrow y=x$,

$P02_2$) $x=y \rightarrow (y=z \rightarrow x=z)$,

$P03_2$) $x=y \rightarrow x+1=y+1$,

$P1_2$) $\neg(0=x+1)$,

P2$_2$) $\neg(x=y)\rightarrow\neg(x+1=y+1)$,

P3$_2$) $x+0=x$,

P4$_2$) $x+(y+1)=(x+y)+1$,

P5$_2$) $x*0=0$,

P6$_2$) $x*(y+1)=(x*y)+x$,

P7$_2$) $B(0)\wedge\forall x(B(x)\rightarrow B(x+1))\rightarrow\forall x\,B(x)$.

The axioms $P5_2$ and $P6_2$ represent Grassmann's recursive definition of the multiplication. The induction schema $P7_2$ and our previous induction schema $P5_1$ look identical again, yet actually $P7_2$ is much more powerful – in $P7_2$ we can take as B(x) formulas that contain both the addition and multiplication letters. Let us denote our new theory by PA_2.

The language of PA_2 is powerful enough to represent (at least) many simple assertions about natural numbers. For example:

$\exists z(x=y*z)$ says that “x is divisible by y”,

$1<x\wedge\neg\exists y\exists z(y<x\wedge z<x\wedge x=y*z)$ says that "x is prime number", let us denote this formula by $prime(x)$,

$\forall x\exists y(x<y\wedge prime(y))$ says that "there are infinitely many prime numbers" (one of the first mathematical theorems, VI century BC).

Exercise 3.2. Put in the language of PA_2 the following assertions:

"x and y have no common divisors >1",
"there are infinitely many twin prime numbers" (the famous conjecture),
"any non-prime x>1, is divisible by some prime number $\leq \sqrt{(x)}$ ",
" $\sqrt{2}$ is not a rational number",
"x is a power of 2",
do not try representing of "$x=2^y$", it is possible, but very hard to do (see Section 3.3).

Unsolvability of PA_2

If PA_2 is much more powerful than PA_1, then what kind of Fischer-Rabin's result can be proved for it? If all algorithms for deciding of PA_1 formulas (i.e. for deciding whether an arbitrary closed formula in the language of PA_1 is "true" or not) are extra hard, then how about such algorithms for PA_2 formulas? In Section 6.3 we will prove that there are no algorithms at all for

deciding of PA_2 formulas.

But how about another "next step" – trying to add to the language of PA_2 the **exponentiation** letter and the axioms: $x^0=1$; $x^{y+1}=x^y*x$? It appears that **this step is not necessary**. In Section 3.3 we will prove the so-called **Representation Theorem**: any computable function can be represented in PA_2. In particular, there is a PA_2 formula $EXPO(x, y, z)$ such that:

PA_2 proves: $EXPO(x, 0, 1)$ ($x^0=1$),

PA_2 proves: $EXPO(x, y, u) \wedge EXPO(x, y+1, v) \rightarrow u*x=v$ ($x^{y+1}=x^y*x$).

Thus, adding of new functional letters does not increase the power of PA_2. **By using addition and multiplication alone one can reproduce any Turing machine "in action" (and, hence, any digital computer program)! PA_2 is "computationally universal".**

See Turing machine by Wikipedia.

Another estimate of the power of PA_2 you may know from the Exercise 2.10: **PA_2 is equivalent to set theory where all sets are finite** (i.e. to ZF minus the Axiom of Infinity). (If you skipped Exercise 2.10, see Section 3.3 for a method of coding finite sets of natural numbers by using the Chinese Remainder Theorem.)

Thus, **the volume of means of reasoning included in PA_2, is not an accidental one**. In a sense, you may think of **PA_2 as a formalization of the entire so-called discrete mathematics**.

See Discrete mathematics by Wikipedia.

Usually, PA_2 is called simply **first order arithmetic**. The term "first order" means that in PA_2 the notion of natural numbers is defined "in itself" – without using a more complicated notion – the "second order" notion of arbitrary sets of natural numbers (which is equivalent to the notion of of real numbers).

Almost as frequently, PA_2 is called **Peano arithmetic**, and is denoted simply by PA (instead of the above PA_2). Read more in:

P. Hajek, P. Pudlak. Metamathematics of First-order Arithmetic. *Springer Verlag Perspectives in Mathematical Logic*, 1993, 460 pp.

The original Dedekind's system of three axioms P1, P2, P3 (see above) is called **second order arithmetic** (because it is using not only variables for natural numbers, yet also *variables for sets of these numbers*). However, to

obtain a really usable axiom system of second order arithmetic, we must add to P1, P2, P3 the axioms describing the notion of sets of natural numbers (for details, see Reverse Mathematics by Wikipedia). This can be done also by embedding P1, P2 and P3 into some full-fledged set theory, for example, ZFC (see Exercise 2.16).

A platonist step-aside

Our customary intuitive understanding of the language of PA (first order arithmetic) leads to an old platonist illusion which says that any closed formula of PA "must be" either "true" or "false". Let us clarify this. Of course, we must follow our intuition while selecting the axioms of PA. We must follow our intuition when trying to establish formal versions of statements from the usual (intuitive) number theory developed by working mathematicians (as we did it in the Exercise 3.2). Still, any attempt to go further than this, and attempt to grant our intuition of natural number sequence mysterious informal powers ends up in platonism. Many people are going this way by taking seriously the following "definition" of "true" formulas in PA:

a) Atomic formulas of PA are assertions about equality of polynomial values. For any particular values of variables the polynomial values can be calculated, and in this way the truth or falsity of atomic formulas can be established.

b) When a formula F is built up from two formulas A, B by using the connectors $\neg, \wedge, \vee, \rightarrow$, and the truth or falsity of A and B is known, then the truth of F is established easily by using the classical truth tables.

c) In PA we have two quantifier symbols $\exists, \forall$. The formula $\exists x C(x)$ is true, if and only if C(x) is true for at least one natural number x. And the formula $\forall x C(x)$ is true, if and only if C(x) is true for all natural numbers x.

Hence, it seems that any closed formula of PA (i.e. a formula containing no free variables) "must be" either "true" or "false". This corresponds well to our customary intuition: a closed formula of PA asserts some completely definite property of the natural number system (like as the assertion that there exist infinitely many prime numbers), and this system either possess this property or not.

Let us note, however, that in the above "definition", the sentence "C(x) is true for all x's" is used. According to our intuition of natural numbers, there exists an infinite amount of such x-s. Hence, it is impossible to establish the truth of the assertion $\forall x C(x)$ simply by checking the truth of C(x) for particular x-s. And hence, the truth of $\forall x C(x)$ could be established (if ever) only **theoretically**, by proving this assertion from some axioms, i.e. in some theory (for example, in PA, or ZFC). May we assert that any closed formula of PA

must be either "theoretically provable", or "theoretically refutable"? We would like to assert this..., still, **which particular theory** are we intending to use – PA, ZFC, or some other? Is this all the same? We must choose some particular theory, else our "definition" of “true” formulas will hang by a thread...

This problem was put elegantly by Paul Lévy (in 1926! – see Levy [1926]): "Ce qu'il faut admirer, c'est la puissance de l'analyse mathematique qui arrive ainsi, dans tant de cas, a reduire une infinite de verifications a un raisonnement unique. Qui peut s'etonner qu'elle n'y soit pas parvenue dans tous les cas? Non seulement cela n'a rien d'etonnant, mais il est a priory assez probable qu'il existe certains enonces, qui resument ainsi en une formule unique une infinite de cas particuliers, et pour lesquels il est impossible de jamais reduire toutes les verifications necessaires a un nombre fini d'operations..."

Maybe, the firm belief in the above-mentioned "definition" is due to the Law of the Excluded Middle, which is a *postulate* of the classical logic? Of course, in PA the formula $A \vee \neg A$ is provable for any A. Does it follow from this that for a any closed A either PA proves A, or PA proves $\neg A$? It follows from Gödel's incompleteness theorem (see Section 5.3) that neither PA, nor ZFC, nor any other fundamental mathematical theory can possess this perfect property – a mere *postulation* of the “Law” of the Excluded Middle cannot solve all problems!

End of the platonist step-aside.

Let us return to PA (former PA_2) as a formal theory. First of all, let us note that the inference rule Gen: F(x) |- $\forall x F(x)$, together with the logical axiom L_{12}: $\forall x F(x) \rightarrow F(t)$ (where t is any term) allow us to generalize our axioms $P00_2$) – $P6_2$) by replacing variables by arbitrary terms s, t, u:

s=s,
s=t → t=s,
s=t → (t=u → s=u),
s=t → s+1=t+1,
¬(0=s+1),
¬(s=t) → ¬(s+1=t+1),
s+0=s,
s+(t+1)=(s+t)+1,
s*0=0,
s*(t+1)=(s*t)+s.

For example, from x+0=x we obtain by Gen: $\forall x(x+0=x)$, and by L_{12}: s+0=s. This allows speaking about "instances" of the axioms $P00_2$) – $P6_2$), for

example, 0+0=0 is an instance of $P3_2$.

The principal means of proving theorems in PA is, of course, the induction principle $P7_2$. Let us prove, for example, the formula 0+x=x (until we have not proved that x+y=y+x, this formula differs from the axiom x+0=x). Let us denote 0+x=x by B(x). First, we must prove B(0), i.e. 0+0=0. This is simply an instance of the axiom x+0=x. Now we must prove that B(x)→B(x+1):

1)	0+x=x	B(x), hypothesis.
2)	0+(x+1)=x+1	B(x+1), to be proved.
3)	0+x=x → (0+x)+1=x+1	An instance of the axiom x=y → x+1=y+1.
4)	(0+x)+1=x+1	By MP, from 1) and 3).
5)	0+(x+1)=(0+x)+1	An instance of the axiom x+(y+1)=(x+y)+1).
6)	0+(x+1)=x+1	By transitivity of identity, from 5) and 4).

Hence, by the Deduction Theorem, B(x)→B(x+1), i.e. by Gen: $\forall x(B(x)\to B(x+1))$. And, by our induction principle, $\forall x B(x)$. Q.E.D.

In a similar way we could prove many other simple theorems of PA. The main problem is to find the optimal order of proving. Try to prove directly, for example, the commutativity of multiplication (x*y=y*x). It seems to be a hard task. Still, do the

Exercise 3.3. Prove the following theorems of PA (see Mendelson [1997]):

x+z=y+z → x=y,
0+x=x, (x+1)+y=(x+y)+1, x+y=y+x, (x+y)+z=x+(y+z),
0*x=0, (x+1)*y=(x*y)+y, x*y=y*x, x*(y*z)=(x*y)*z.

Exercise 3.3a. Verify the following property of the natural number identity: $F(x,x)\wedge x=t\to F(x,t)$ (i.e. prove this theorem schema in PA). Here, F is any formula, and t is any term that does not contain variables bound by quantifiers in F. The designation F(x, x) means that the occurrences of the free variable x are split into two groups. In F(x, y), the occurrences of the second group have been replaced by t (which equals to x). (Hint: use induction by the structure of F.)

In PA we can prove all the necessary properties of the relation x<y (it can be defined by the formula $\exists z(x+z+1=y)$. In particular, we could prove the following schema of theorems:

$$\neg\forall x C(x)\to\exists x(\neg C(x)\wedge\forall y(y<x\to C(y)))\ .$$

I.e. if not all natural numbers possess the property C, then there is some **minimum number** that does not possess C.

In PA we can discuss freely the properties of the **division** operation. Let us denote by R(x, y, z) the formula $\exists u(x=y*u+z\wedge z<y)$, i.e. *x mod y* = *z* in Pascal. Then we could prove in PA that:

$$0<y\rightarrow\exists z\,R(x,y,z) \quad ,$$

$$R(x,y,z_1)\wedge R(x,y,z_2)\rightarrow z_1=z_2 \quad .$$

All these (and many more) formal proofs you can find in Mendelson [1997]. In this book, formal proving of theorems about natural numbers is performed to the extent that you can start proving in PA more serious theorems of the (intuitive) elementary number theory. For example, you can try to prove that:

there are infinitely many prime numbers;

$\sqrt{2}$ is not a rational number;

e and π are transcendental numbers;

if p(n) is the number of primes in {1, 2, ..., n}, then $\lim\limits_{x\rightarrow\infty}\frac{p(n)}{\ln n}=1$.

Don't be surprised at the use of some real numbers and the function *ln x* in the above statements. If in a statement or a proof only a fixed list of *computable* real numbers and *computable* real functions is used, then this statement/proof can be translated into PA (as in Exercise 3.2 and Section 3.3).

Let us introduce shortcuts for some specific terms of PA: bold **0** will denote 0, bold **1** will denote 1, bold **2** – (1+1), bold **3** – ((1+1)+1) etc. These terms are called **numerals**; they are used as standard representations of particular natural numbers. To denote numerals in schemas of PA formulas we will use bold letters **k**, **l**, **m**, **n**, **p**, **q**, **r**, ...

Exercise 3.4. Verify that, if *k* is a natural number, *k>0*, then:

PA proves: $x<\boldsymbol{k}\leftrightarrow(x=\boldsymbol{0})\vee(x=\boldsymbol{1})\vee\ldots\vee(x=\boldsymbol{k-1})$;

PA proves: $(\exists x<k)C(x)\leftrightarrow C(\boldsymbol{0})\vee C(\boldsymbol{1})\vee\ldots\vee C(\boldsymbol{k-1})$;

PA proves: $(\forall x<k)C(x)\leftrightarrow C(\boldsymbol{0})\wedge C(\boldsymbol{1})\wedge\ldots\wedge C(\boldsymbol{k-1})$.

Note. $(\exists x<\boldsymbol{k})C(x)$ is a shortcut for $\exists x(x<\boldsymbol{k}\wedge C(x))$.

And $(\forall x<\boldsymbol{k})C(x)$ is a shortcut for $\forall x(x<\boldsymbol{k}\rightarrow C(x))$.

Exercise 3.4a. If some atomic formula (t_1=t_2) of PA contains variables x_1, x_2, ..., x_n, then by moving all the components of t_2 to the left hand side we can obtain a Diophantine equation $t_1-t_2=0$ (see Section 4.1). Our concern is

solving of these equations in natural numbers. Show that, if we have a particular solution (b_1, b_2, ..., b_n) of the equation $t_1 - t_2 = 0$, then

PA proves: $\exists x_1 \exists x_2 ... \exists x_n (t_1 = t_2)$.

Hint: show that PA proves every "true" atomic formula $s_1 = s_2$, where the terms s_1 and s_2 do not contain variables.

Exercise 3.4b (for smart students). Suppose, a formula G(x_1, ... x_n) contains only bounded quantifiers and has exactly *n* free variables x_1, ... x_n. Verify that then, if, for some numbers a_1, ..., a_n, G(a_1, ..., a_n) is "true", then PA proves G(**a_1**, ..., **a_n**), else PA proves ¬G(**a_1**, ..., **a_n**).

Note. By *bounded quantifiers* we understand $(\exists x < t)$ and $(\forall x < t)$, where *t* is any term that does not contain x.

3.2. How to Find Arithmetic in Other Formal Theories

In first order arithmetic (PA), the simplest way of mathematical reasoning is formalized, where only natural numbers (i.e. discrete objects) are used. Other, more complicated mathematical notions (real numbers, Cantor's arbitrary infinite sets) are formalized (as it should be) in more complicated theories. These more complicated theories are more "powerful" than PA in the sense that they are able to discuss more complicated objects (real numbers, arbitrary infinite sets). Still, how about their "power" in discussing the properties of natural numbers? Could they prove a theorem about natural numbers that cannot be proved in PA? For example, could it happen that the twin prime conjecture will be proved in ZFC, yet it cannot be proved in PA? At first glance, this may seem impossible, because the notion of natural numbers seems to be independent of (and "more fundamental than") other mathematical notions. Unfortunately (indeed?), this is not the case... (see Section 6.5 and Appendix 2).

How to determine, is some formal theory T able to discuss natural numbers? If T is a traditional first order theory, we could try the following:

a) First, we must define as natural numbers some of the "objects " of T, i.e. we must provide, in the language of T, a formula N(x) that "asserts" that "x is a natural number".

b) The second component to be provided is an algorithm Tr transforming atomic formulas of PA (i.e. Diophantine equations) into formulas of T. If F is an atomic formula of PA, then Tr(F) must be a formula of T having exactly the

free variables of F.

c) Then, this algorithm Tr can be extended to cover non-atomic formulas of PA:

$Tr(\neg F)=\neg Tr(F)$,

$Tr(F \to G)=Tr(F) \to Tr(G)$,

$Tr(F \wedge G)=Tr(F) \wedge Tr(G)$,

$Tr(F \to G)=Tr(F) \to Tr(G)$,

$Tr(\exists x\, F(x))=\exists x(N(x) \wedge Tr(F(x)))$,

$Tr(\forall x\, F(x))=\forall x(N(x) \to Tr(F(x)))$.

Now, we have "T-translations" for all formulas of PA, and the formula Tr(F) always has exactly the free variables of F (verify!).

d) After this, we must verify that T proves at least those "facts" about natural numbers that can be proved in PA. To establish this, we need not to check all the formulas provable in PA. It is sufficient to check only the **axioms of PA**. Let us consider, for example, the axiom $\neg(x+1=y+1) \to \neg(x=y)$, or, equivalently, $x=y \to x+1=y+1$. We must show that

T proves: $N(x) \wedge N(y) \to Tr(x+1=y+1 \to x=y)$, i.e.
T proves: $N(x) \wedge N(y) \to (Tr(x+1=y+1) \to Tr(x=y))$.

Or, consider the axiom $\neg(0=x+1)$, we must show that

T proves: $N(x) \to Tr(\neg(0=x+1))$, i.e.
T proves: $N(x) \to \neg\, Tr(0=x+1)$.

If we have established this for all axioms of PA, then (since T – as a first order theory – contains 100% of the traditional axioms and inference rules of the classical first order logic) we have established this for all **closed** formulas F:

If PA proves F, then T proves Tr(F).

If T is consistent, then T cannot "say wrong things about natural numbers". Indeed, assume, that for some closed PA-formula F, T would prove Tr(¬F), while PA proves F (i.e. ¬F is a "wrong thesis" about natural numbers). Then, of course, T proves Tr(F), but T would prove ¬Tr(F) as well, i.e. T would be an inconsistent theory.

However, to prove the famous theorems of Section 5, we will need only some of the properties of the translation algorithm Tr. The above approach to translation can be generalized by introducing the following notion of **relative interpretation** (of PA in some other theory T). It is any algorithm Tr transforming each **closed** formula F of PA into a closed formula Tr(F) of T such that:

Fu$_1$) If PA proves F, then T proves Tr(F).

Fu$_2$) T proves Tr(¬F), if and only if T proves ¬Tr(F).

Fu$_3$) If T proves Tr(F), and T proves Tr(F→G), then T proves Tr(G).

Let us say that PA is **relatively interpretable** in the theory T, if and only if there is a relative interpretation of PA in T.

Exercise 3.5. Verify that the above "first order" approach yields, indeed, a relative interpretation of PA in T.

Fundamental theories

Acknowledging the fundamental role of natural numbers in mathematics, let us call a formal theory T a **fundamental theory**, if and only if PA is relatively interpretable in T.

Important! Thus, T can be here any formal theory containing the negation connective. On the side of T, no particular set of other connectives, logical axioms, or inference rules (first order, second order or other) is required (provided that T is, indeed, a formal theory according to the definition in Section 1.4).

The simplest fundamental theory is, of course, PA itself. And so are all the extensions of PA that are using the same or extended language (of PA).

The set theories ZF and ZFC (of course) also are fundamental theories. How could one build a relative interpretation of PA in ZF (even in ZF minus Axiom of Infinity, in fact, in an even weaker set theory *Ext*+*Ext'*+*Separation*+*Pairing*+*Union* of Section 2.3)?

As the formula N(x) we can take von Neumann's formula $x \in N$ asserting that "x is natural number" (see Section 2.3). As you established in Exercise 2.11, N(x) is a very long formula in the language of ZF.

The formula translation algorithm Tr from PA to ZF also is somewhat complicated. We must show how to build Tr(t_1=t_2) for any terms t_1, t_2 of PA.

Of course, we will take Tr(x=y) = (x=y). Since **0** is defined in ZF as the empty set, then Tr(x=**0**) will be $\forall y \neg(y \in x)$. Since **1** is defined as the set {o}, Tr(x=**1**) = $\forall y(y \in x \leftrightarrow Tr(y = \mathbf{0}))$. After this, Tr(x=**2**) can be obtained as $\forall y(y \in x \leftrightarrow Tr(y = \mathbf{0}) \vee Tr(y = \mathbf{1}))$. Etc.

To define formulas x+y=z, x*y=z, we must apply the recursion theorem of Exercise 2.22.

The last step is easy. For example, to translate $x + y * z = u$, first, convert it

into $\exists w(y*z=w \wedge x+w=u)$. Etc.

Exercise 3.5a. Verify that, under the conditions Fu_1 and Fu_3, for any closed PA-formulas A, B, C:

a) If T proves Tr(A→B) and T proves Tr(B→C), then T proves Tr(A→C).
b) If T proves Tr(A→B), then T proves Tr(¬B→¬A).
c) If T proves Tr(A→B) and T proves Tr(¬B), then T proves Tr(¬A).
d) If T proves Tr(¬¬A), then T proves Tr(A).
e) If T proves Tr(A→(B→C)), then T proves Tr(B→(A→C)).
f) If T proves Tr(A→(B→C)) and T proves Tr(A→B), then T proves Tr(A→C).

Exercise 3.5b. Generalize the above definition of relative interpretation for arbitrary two formal theories T_1 and T_2. Verify that, under the conditions Fu_1 and Fu_2, if T_1 is relatively interpretable in T_2, and T_1 is an inconsistent theory, then so is T_2 (hence, if T_2 is consistent, then so is T_1).

Now, we can reformulate the question of the first paragraph of this section as follows: is it possible that there is a fundamental theory T and a PA-formula F such that PA cannot prove F, yet T proves Tr(F)? See affirmative answers in Section 6.5 and Appendix 2.

Exercise 3.6. Generalize the result of the Exercise 1.4 by proving that the set $Tr^{-1}(T)$ of "arithmetical theorems" of any fundamental formal theory T is computably enumerable. **(**Hint: use the computability of Tr.)

For a complete treatment of relative interpretability see:

S. Feferman. Arithmetization of metamathematics in a general setting. *Fund. Math.*, 1960, vol. 49, pp.35-92

See also: **S. Feferman.** My route to arithmetization. *Theoria,* 63, 1997, pp. 168-181 (online copy available).

The most striking result is here the following one:

Theorem. Any formal theory T is relatively interpretable in PA+Con(T), i.e. in PA plus one more axiom – an arithmetical translation of the assertion "T is a consistent theory". In particular, if the translation of some arithmetical statement S (a closed formula in the language of PA) can be proved in T, then S can be proved in PA+Con(T).

For details of the formula Con(T) see Section 5.4.

A weaker version of this theorem was obtained in Vol. 2 of Hilbert, Bernays [1934]. The full version is due to Hao Wang:

H. Wang. Arithmetical models for formal systems. *Methodos*, 3, 1951, pp. 217-232.

The proof of this theorem (further refined in the above paper of S. Feferman) can be obtained as an "arithmetization" of Henkin's Model Existence Theorem (an equivalent of Gödel's Completeness Theorem): if T is a consistent formal theory, then there exists a finite or

countable model of T (see Appendix 1 for details of these theorems).

3.3. Representation Theorem

In this section we will show that PA is "computationally universal", i.e. that any Turing machine “in action” (and, hence, any digital computer program) can be reproduced in PA.

How could we verify that some formula F(x) "asserts" that x is a prime number? Of course, if F(x) is the formula

$$1<x\wedge\neg\exists y\exists z(y<x\wedge z<x\wedge x=y*z) \quad ,$$

we could say that it "corresponds" to the definition of prime numbers. Still, this is not the only formula "expressing" that x is a prime number. How to identify formulas that are “expressing” something useful?

As the first step, we could introduce the following "definition": formula F(x) "expresses" the predicate "x is prime number", if and only if for all n: F(n) is "true", if and only if n is indeed a prime number.

The next step would be to replace the vague notion "F(n) is true" by a more exact notion of provability in PA: formula F(x) "expresses" in PA the predicate "x is prime number", if and only if for all n: n is a prime number, if and only if PA proves F(**n**) (where **n** is the numeral representing n, i.e. 1+1+...+1 n times).

This definition involves unprovability (if n is not prime, then F(**n**) must be unprovable in PA). Establishing of unprovability is a very hard task. Indeed, if PA would be inconsistent, then every formula would be provable in PA, and thus, the predicate "x is prime number" could not be "expressed" at all. Since we do not know exactly, is PA consistent or not (for details see Section 5.4), the latter definition of "expressibility" is not satisfactory.

A much better solution: let us say that a formula F(x) expresses the predicate "x is prime number" in PA, if and only if for all n:

a) If n is a prime number, then PA proves F(**n**).

b) If n is not prime number, then PA proves ¬F(**n**).

This definition is 100% positive in the sense that it involves only provability of formulas, and does not use unprovability. The expressibility according to this definition can be established independently of our (missing) knowledge, is PA consistent or not.

Let us adopt this definition as a general one. Assume, p(x, y) is some predicate of natural numbers. Let us say that a formula P(x, y) **expresses** p(x, y) in PA, if and only if P has exactly two free variables x, y, and for all pairs m, n of

natural numbers:

a) If p(m, n), then PA proves P(**m**, **n**).

b) If not p(m, n), then PA proves ¬P(**m**, **n**).

The definition of expressibility for unary, ternary etc. predicates is similar.

You could prove easily, for example, that the formula x=y expresses the identity predicate of natural numbers. Indeed, if m=n, then PA proves **m**=**n** (since the terms **m**, **n** are identical). If m, n are different numbers, then PA proves ¬(**m**=**n**). (Hint: apply to the formula **m**=**n** the axiom $x+1=y+1\rightarrow x=y$ as many times as you can, and then apply the axiom $\neg(0=x+1)$.)

If PA would be an inconsistent theory, then (according to our final definition) any formula would express any predicate, i.e. then all predicates would be expressible. But, if PA is consistent, then each formula can express only one predicate.

Let us assume that PA is consistent. Then **only computable predicates are expressible in PA**. Indeed, let some formula P(x, y) express in PA the predicate p(x, y). How to determine, is p(m, n) true or false for given numbers m, n? If p(m, n) is true, then PA proves P(**m**, **n**), and if p(m, n) is false, then PA proves ¬P(**m**, **n**). Hence, let us take a computer that prints out all theorems of PA one by one. (Such a computer does exist, since the set of all theorems of any formal theory is computably enumerable – see Exercise 1.4). Let us stay sitting beside the output tape of this computer waiting for one of the formulas – P(**m**, **n**) or ¬P(**m**, **n**). If P(**m**, **n**) appears, then ¬P(**m**, **n**) will not appear (PA is assumed to be consistent), i.e. p(m, n) is true. If ¬P(**m**, **n**) appears, then P(**m**, **n**) will not appear, and hence, p(m, n) is false. Thus we have a procedure solving p(m, n) for any given numbers m, n, i.e. the predicate p(x, y) is computable.

We do not know exactly, is PA consistent or not. Later in this section **we will prove (without any consistency conjectures!) that each computable predicate can be expressed in PA.**

For our crucial proofs of famous theorems in Section 5 we will need a somewhat stronger definition of "expressibility" of **functions** in PA. The straightforward definition (the function f(x, y) is expressible if and only if the predicate f(x, y)=z is expressible) will be too weak.

Let us say that the formula F(x, y, z) **represents** in PA the natural number **function** f(x, y), if and only if F has exactly three free variables x, y, z, and for every natural numbers k, m, n such that $f(k,m)=n$:

a) PA proves: F(**k**, **m**, **n**).

b) PA proves: $\forall z(\neg(z=n)\rightarrow\neg F(\boldsymbol{k},\boldsymbol{m},z))$.

For simple expressibility of the predicate f(x, y)=z we would need instead of b) the following

b_1) If $f(k,m)\neq n$, then PA proves ¬F(**k**, **m**, **n**),

i.e. for each n we could provide a **separate proof** of ¬F(**k**, **m**, **n**), yet b) requires instead of these separate proofs a **single general proof** for all values of n.

The definition of representability for unary, ternary etc. functions is similar.

If PA is inconsistent, then all natural number functions are representable in PA.

Exercise 3.7. a) Verify that if PA is consistent, then only computable functions can be represented in PA.

b) Prove that a predicate p(x) can be expressed in PA, if and only if the following function $h_p(x)$ can be represented in PA:

If p(x), then $h_p(x)=1$; else $h_p(x)=0$.

Thus, we would prove that all computable predicates are expressible in PA, if we would prove the following

Representation Theorem. Every computable function can be represented in PA.

Proof. The rest of this section.

Corollary. Every computable predicate can be expressed in PA.

Note. The formulas that we will build to represent functions in PA, will contain the conjunction and disjunction letters, but **not** the negation letter "¬", and the implication letter – only in one specific context. They will contain existential quantifiers $\exists x$, and only **restricted** universal quantifiers $\forall x(x<t\rightarrow\ldots)$, where t are linear terms of PA (and this is the only context where the implication letter can appear). This observation will allow us to apply the Representation Theorem as the starting point for the solution of Hilbert's Tenth Problem in Section 4. (Why should we avoid negations and unrestricted universal quantifiers? Because by applying these constructs to a computably (recursively) enumerable predicate we can obtain a predicate that is not computably enumerable.)

Let us start the proof. We have a computable function f(x, y) mapping pairs or natural numbers into natural numbers. And we must build a “good” PA formula F(x, y, z) for the predicate f(x, y)=z in PA. I.e. we must provide an algorithm that allows converting **computer programs** computing natural number functions into formulas representing these functions.

The generalization of the proof for unary, ternary etc. functions is straightforward.

What kind of computers should we choose for this purpose? For the simplicity of the proof let us use the so-called **Turing machines** invented in 1936 by Alan M.Turing.

A. Turing. On computable numbers, with an application to the Entscheidungsproblem. "Proc. London Math. Soc.", 1936, vol. 42, pp. 230-265 (received May 28, 1936)

Independently and almost simultaneously, Emil L. Post proposed a similar explicit concept of abstract machines:

E. L. Post. Finite combinatory processes – formulation 1. "Journ. Symb. Logic", 1936, vol.1, pp. 103-105 (received October 7, 1936)

See also: Turing machine by Wikipedia.

Formally, a (somewhat modernized version of a) Turing machine M consists of:

a) A finite set of internal states:

$$S_M = \{s_{start}, s_{stop}, s_1, ..., s_m\}.$$

Programmers can think of S_M as the main memory of M: $2+m=2^k$, where k is the number of memory bits.

b) A finite set of letters:

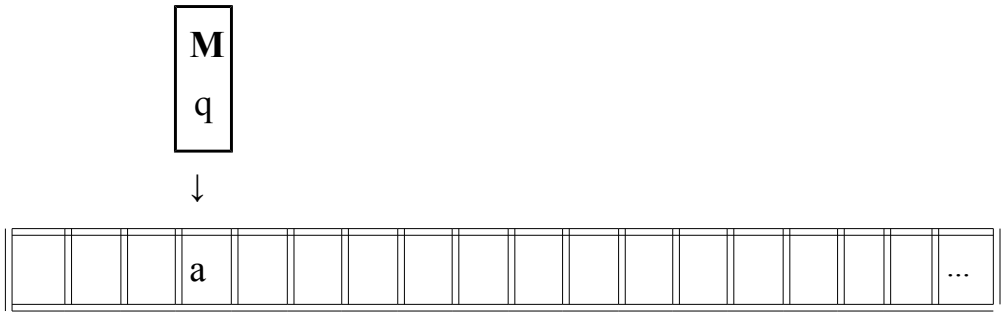
$$B_M = \{b_1, ..., b_n\}.$$

c) A finite set (not sequence!) P_M of instructions (the "program" of M) each having the form:

$$s, b \rightarrow s', b', e,$$

where s and s' are states, b and b' – letters, e = 0, +1, or −1. Two instructions of P_M should not have the same left-hand side (s, b).

This formal object works as follows. Imagine:



a) An infinite tape (the "hard disk" of M) consisting of fixed size cells, each cell containing a letter from B_M.

b) A box encapsulating some state from S_M, and attached to some cell on the tape.

Every second the following happens: if the Box is in the state s, and if the cell it is attached to contains the letter b, and if the program P_M contains the instruction s, b → s', b', e, then the Box changes its state from s to s', the letter b in the cell is replaced by the letter b', and the Box moves by e cells. I.e. if e = −1, then it moves one cell to left, if e = +1, it moves one cell to right, if e = 0, it does not change the position. If the program P_M does not contain an appropriate instruction, then nothing happens. If e = −1, but the Box is attached to the leftmost cell of the tape, then it does not move.

As you can see, Turing did not use the von Neumann's principle (invented some time later) according to which data and programs should be kept in the same memory space.

Let us say that the **machine M computes the function** f(x, y), if and only if for each pair x, y of natural numbers the following happens. Starting in the situation where:

a) The Box is in the state s_{start} and is attached to the leftmost cell of the tape.

b) The tape contains the following sequence of letters:

1 1 ... 1 0 1 1 ... 1 0 0 0 ...,
x times “1” ... y times “1” ...

the machine M performs a finite number of steps according to its program and after this a situation occurs where:

a) The Box is in the state s_{stop}.

b) The tape contains the following sequence of letters:

1 1 ... 1 0 ...
f(x, y) times “1” ...

The rest of the tape may contain arbitrary letters.

Let us say that a function f(x, y) is a **computable function**, if and only if it can be computed in the above way by some Turing machine.

As an example, let us build a machine computing the function f(x) = x+2. This machine must simply cross the array of 1's and append another two 1's to it.

$S_M = \{ s_{start}, s_{stop}, s \}$,

$B_M = \{0, 1\}$,

$P_M = \{$

$s_{start}, 1 \rightarrow s_{start}, 1, +1$; // skip 1's

$s_{start}, 0 \rightarrow s, 1, +1$; // write the first additional 1, register this as done

$s, 0 \rightarrow s_{stop}, 1, 0$; // write the second additional 1, and stop

$\}$.

Exercise 3.8. a) Build Turing machines computing the following functions: x+y, x*2, x*y, 2^x, $[\log_2 x]$ (or int(log2(x)) in Pascal).

b) Maybe, in your local stores, you cannot buy a real Turing machine, still, you can surely force your PC to emulate these machines. Write (using your favorite programming language) an **interpreter of Turing machines**. It should be a program, receiving as inputs S_M, B_M, P_M and initial states of the tape cells. As outputs the program should print out final states of the tape cells. (For ready to use Turing machine simulators see Turing machine by Wikipedia).

Thus, your PC can easily emulate Turing machines. Much more striking is the converse statement: Turing machines can (not easily, yet they can!) emulate your PC, with your Pascal, C++, Lisp, Prolog etc. included. All the necessary techniques for proving this statement can be found, for example, in Mendelson [1997] or Kleene [1952].

Turing machines represent one of the possible formal reconstructions of the intuitive notion of computability (the concept of algorithm). Since 1930s, besides Turing machines, several other very different formal reconstructions of this notion were proposed: recursive functions, lambda-calculus by A. Church, canonical systems by E. Post, normal algorithms by A. A. Markov, etc. And the equivalence of all these reconstructions was proved (see Mendelson [1997] or Kleene [1952]).

The equivalence of different formal reconstructions of the same intuitive concept means that the volume of the reconstructed formal concepts is not an accidental one. It is the best reason to abandon the (vague) intuitive concept of computability, and replace it by the formal concept, for example, by the concept of computability by Turing machines. This decision is known as **Church's Thesis** (or, Church-Turing thesis):

If some function is computable in the intuitive sense of the word, then an appropriate Turing machine can compute it.

Alonzo Church stated (an equivalent of) this thesis in 1936:

A. Church. An unsolvable problem in elementary number theory. "American Journal of Mathematics", 1936, vol. 58, pp.345-363.

In the original form of Church's Thesis recursive functions were used instead of Turing machines.

See also: Church-Turing thesis by Wikipedia.

Let us return to our proof of the Representation Theorem. We must represent the predicate f(x, y)=z by a formula F(x, y, z) in the language of PA. Since f(x, y) is a computable function, we can try to build F(x, y, z) by describing in PA the computation process that leads from the value pair (k, m) to the value f(k, m). Let us denote by M some Turing machine performing this computation process.

Our task would be much easier, if the language of PA contained some additional constructs. The following sequence could be called a **situation**:

$$(s, p, a_0, a_1, ..., a_{q-1}),$$

where s is a state from S_M, p is the number of the cell to which the box M is currently attached, and $a_0, a_1, ..., a_{q-1}$ are letters in the first q cells of the tape (all the other cells contain the letter 0). Let us introduce a new kind of the so-called **situation variables** C, C_1, C_2, ..., their domain will consist of all the possible situations. Let us introduce also some additional function letters:

s(C) = s in C,

p(C) = p in C,

q(C) = q in C (i.e. the number of cells in C),

$a_i(C) = a_i$ in C.

If we had all these symbols in the language of PA, our task of representing computable functions by formulas would be much easier.

Our first formula START(C, x, y) will assert that C is the initial situation having the values of arguments x and y on the tape. Let us represent it as a conjunction of the following formulas:

$$s(C)=s_{start}; p(C)=0; q(C)=x+y+2 \quad ;$$

$$\forall i\,(i<x+y+2 \rightarrow a_i(C)=1 \vee (a_i(C)=0 \wedge (i=x \vee i=x+y+1))) \quad .$$

(I'm sorry, but we need this trick to avoid negations).

The second formula STOP(C, z) will assert that C is a final situation having the function value z on the tape. Let us represent it as the following formula:

$$s(C)=s_{stop}; z<q(C); a_z(C)=0; \forall i\,(i<z \rightarrow a_i(C)=1) \quad .$$

As the next step, we build for each instruction I: s, b → s', b', e the formula $STEP_I(C_1, C_2)$ asserting that by applying the instruction I in the situation C_1 we will obtain the situation C_2.

Exercise 3.9. Write these formulas yourselves ignoring my next few paragraphs.

First let us consider the case when e = 0. Then $STEP_I(C_1, C_2)$ looks as follows:

$$s(C_1)=s \wedge s(C_2)=s' \wedge \exists k \exists n F \quad ,$$

where F is the conjuction of the following formulas:

$$p(C_1)=k \wedge p(C_2)=k \wedge q(C_1)=n \wedge q(C_2)=n \wedge a_k(C_1)=b \wedge a_k(C_2)=b' \quad ;$$
$$\forall i\,(i<n \rightarrow i=k \vee \exists j\,(a_i(C_1)=j \wedge a_i(C_2)=j)) \quad .$$

We did not use expressions like as $p(C_1)=p(C_2)$ in order to simplify our next steps.

Now, the case when e = −1. Then $STEP_I(C_1, C_2)$ looks as follows:

$$s(C_1)=s \wedge s(C_2)=s' \wedge \exists k \exists m \exists n F \quad ,$$

where F is the conjuction of the following formulas:

$$p(C_1)=k \wedge p(C_2)=m \wedge q(C_1)=n \wedge q(C_2)=n \wedge a_k(C_1)=b \wedge a_k(C_2)=b' \quad ;$$
$$((k=0 \wedge m=0) \vee m+1=k) \wedge \forall i\,(i<n \rightarrow i=k \vee \exists j\,(a_i(C_1)=j \wedge a_i(C_2)=j)) \quad .$$

The formula $(k=0 \wedge m=0) \vee m+1=k$ says that, if in C_1 the Box is attached to the leftmost cell of the tape, then e = −1 works as e = 0.

And finally, the case e = +1. Then $STEP_I(C_1, C_2)$ looks as follows:

$$s(C_1)=s \wedge s(C_2)=s' \wedge \exists k \exists m \exists n \exists r F \quad ,$$

where F is the conjuction of the following formulas:

$$p(C_1)=k \wedge p(C_2)=m \wedge q(C_1)=n \wedge q(C_2)=n \wedge a_k(C_1)=b \wedge a_k(C_2)=b' \quad ;$$
$$k+1=m \wedge (m<n \wedge n=r) \vee (m=n \wedge n+1=r \wedge a_m(C_2)=0) \quad ;$$
$$\forall i\,(i<n \rightarrow i=k \vee \exists j\,(a_i(C_1)=j \wedge a_i(C_2)=j)) \quad .$$

The condition $a_m(C_2)=0$ in the second row says that the "unregistered" rest of the tape contains only letters 0.

The next formula $COMPUTE_M(C_1, C_2)$ will assert that starting the program P_M in the situation C_1 after a finite number of steps we willl obtain the

situation C_2. To simplify the task let us introduce one more variable L taking as its values **finite sequences of situations**. We will need also the corresponding function symbols:

d(L) = the length of the sequence L;

g_i(L) = the i-th situation in L.

Now we can easily write the formula $COMPUTE_M(C_1, C_2)$:

$$\exists L \exists w (d(L) = w+1 \wedge g_0(L) = C_1 \wedge g_w(L) = C_2 \wedge F) \quad ,$$

where F is the following formula:

$$\forall i (i < w \rightarrow \exists C_3 \exists C_4 (g_i(L) = C_3 \wedge g_{i+1}(L) = C_4 \wedge STEP_M(C_3, C_4)))$$

and where $STEP_M(C_3, C_4)$ is the following formula:

$$STEP_{I_1}(C_3, C_4) \vee STEP_{I_2}(C_3, C_4) \vee ... \vee STEP_{I_k}(C_3, C_4) \quad ,$$

assuming that $P_M = \{I_1, I_2, ..., I_k\}$.

And, finally, we can write the formula F(x, y, z) asserting that f(x, y)=z as follows:

$$\exists C_1 \exists C_2 (START(C_1, x, y) \wedge COMPUTE_M(C_1, C_2) \wedge STOP(C_2, z)) \quad .$$

This formula is not 100% a PA formula since it contains symbols denoting states and tape letters, situation variables, and even a variable for sequences of situations, and a lot of function symbols missing in the language of PA. Hence, to complete our proof we must show how to eliminate these constructs.

As the first step, let us replace the symbols denoting states (s_{start}, s_{stop}, s, s', etc.) and tape letters (0, 1, b, b', etc.) of the machine M by some natural numbers.

But how to replace the situation variables? If states and tape letters are already replaced by numbers, then situations are simply finite sequences of numbers. Hence, our situation variable problem would be solved, if we could find a good coding algorithm that allowed to represent any finite sequence of natural numbers by a single natural number (or, at least by two or three numbers). This algorithm must be "good" in the sense that it must allow representation of the functions s(C), a_i(C) etc. by formulas of PA.

It was Gödel's idea to use for this purpose the so-called Chinese Remainder Theorem. See

Eric W. Weisstein. "Chinese Remainder Theorem." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/ChineseRemainderTheorem.html

Could you find a number X such that (in the *Pascal* language):

X mod 3 = 2, X mod 5 = 3, and X mod 7 = 4?

Let us consider the numbers 7k+4 for k=0, 1, 2, ...:

4, 11, 18, 25, 32, 39, 46, 53, ...

Here 11 mod 3 = 2, 32 mod 3 = 2, 53 mod 3 = 2, yet only the number 53 possesses the property 53 mod 5 = 3. Hence, the least number that we can take is X = 53.

In general, if we have a sequence of divisors u_1, u_2, ..., u_n (i.e. $u_i \geq 2$ for all i), and a sequence of remainders v_1, v_2, ..., v_n (i.e. $0 \leq v_i < u_i$ for all i), could we find a number X such that X mod $u_i = v_i$ for all i? If some of the numbers u_i have a common divisor, then this problem may have no solutions. For example, if $u_1 = 6$ and $u_2 = 10$, then $X = 6y_1 + v_1 = 10y_2 + v_2$, and thus $v_1 - v_2$ must be an even number, i.e. if $v_1 = 1$ and $v_2 = 2$, then our problem has no solutions. Still, if two of the numbers u_i never have common divisors, then the solution always exists. This is the asserted by the

Chinese Remainder Theorem. Let u_1, u_2, ..., u_n be a sequence of pairwise relatively prime natural numbers ($u_i \geq 2$ for all i), i.e. two of them never have common divisors greater than 1. And let v_1, v_2, ..., v_n be a sequence of natural numbers such that $0 \leq v_i < u_i$ for all i. Then there is a natural number X (less than the product $u_1 u_2 ... u_n$) such that X mod $u_i = v_i$ for all i.

Proof. Let us associate with every number x such that $0 \leq x < u_1 u_2 ... u_n$, the "remainder vector" (x mod u_1, x mod u_2, ..., x mod u_n). Show that if two such numbers have equal remainder vectors, then their difference is a multiple of the product $u_1 u_2 ... u_n$. Q.E.D.

Using this theorem we can try to organize a coding of sequences of natural numbers v_0, v_1, ..., v_{n-1} by representing each number v_i as X mod u_i, where X is the "code" (possibly large, yet a fixed number) and the sequence u_0, u_1, ..., is generated in some simple way. For example, we can try a linear function: $u_i = yi+z$. How to choose y and z? Two numbers u_i should not have common divisors. If d is a common divisor of u_i and u_j, then d divides also $u_i - u_j = y(i-j)$. If we take $z = y+1$, i.e. $u_i = y(i+1)+1$, then divisors of y cannot divide neither u_i, nor u_j. Thus our common divisor d must divide i−j, i.e. a number less than n. Hence, if we take as y a multiple of (n−1)! (i.e. $1 \cdot 2 \cdot 3 \cdot ... \cdot (n-1)$),

then the numbers $u_0, u_1, ..., u_{n-1}$ will have no common divisors. And finally, if we take y large enough to ensure that

$$u_0>v_0, u_1>v_1, ..., u_{n-1}>v_{n-1},$$

then, according to Chinese Remainder Theorem, we can find a number x such that x mod $u_i = v_i$ for all i = 0, 1, ..., n−1.

Hence, we could use the pair (x, y) as a code of the sequence $v_0, v_1, ..., v_{n-1}$. Such a code does not include the number n, so, it would be better to code the sequence of n, $v_0, v_1, ..., v_{n-1}$ instead of $v_0, v_1, ..., v_{n-1}$ alone.

The function:

$$\beta(x, y, i) = x \bmod (1+y(i+1))$$

is called **Gödel's β-function**. As we have proved, for each sequence of natural numbers $v_1, ..., v_n$ a pair of natural numbers x, y can be found such that

$$\beta(x, y, 0) = n, \beta(x, y, 1) = v_1, ..., \beta(x, y, n) = v_n.$$

Note also, that we can represent β-function in PA by the following formula BETA(x, y, i, j) (it asserts that β(x, y, i) = j):

$$\exists z(x=(1+y*(i+1))*z+j \wedge j<1+y*(i+1)) \quad .$$

Now we can start rewriting of our formulas START, STOP, STEP etc. in the language of PA. We have already replaced by natural numbers all states of the machine M and all tape letters. Hence, any situation $(s, p, a_0, a_1, ..., a_{q-1})$ is now a sequence of natural numbers that we can replace by two numbers x, y such that:

$\beta(x, y, 0) = q, \beta(x, y, 1) = s, \beta(x, y, 2) = p, \beta(x, y, 3) = a_0, ...,$

$\beta(x, y, q+2) = a_{q-1}.$

Hence, we can replace any quantifier $\exists C$ by two quantifiers $\exists x \exists y$, where x, y are variables of PA. The additional function symbols we have introduced:

$$q(C)=q_1, s(C)=s_1, p(C)=p_1, a_i(C)=b,$$

we can replace now by:

$$\beta(x, y, 0) = q_1, \beta(x, y, 1) = s_1, \beta(x, y, 2) = p_1, \beta(x, y, 3) = a_0, \beta(x, y, i+3) = b.$$

The "illegal" inequalities such as $q_1<q(C)$ also can be eliminated:

$$\exists q_2(\beta(x, y, 0)=q_2 \wedge q_1<q_2) \quad .$$

Exercise 3.10. Rewrite the formulas START, STOP, $STEP_I$ and $STEP_M$, and calculate the length of each.

In the formula $COMPUTE_M$ we introduced the variable L for finite sequences of situations, and function letters d(L) and $g_i(L)$. For each situation we have now a code consisting of two numbers x, y. Hence, if the code of the situation C_i is (c_i, d_i), then we can code the sequence $L = (C_0,..., C_{n-1})$ as the sequence of numbers:

$$n, c_0, d_0, c_1, d_1, ..., c_{n-1}, d_{n-1},$$

i.e. by two numbers x, y such that:

$$\beta(x, y, 0) = n, \beta(x, y, 2i+1) = c_i, \beta(x, y, 2i+2) = d_i.$$

Now we can replace the quantifier $\exists L$ by two quantifiers $\exists x \exists y$, where x, y are variables of PA. Our two last additional function symbols can be eliminated as follows. We will replace the formula d(L)=w by $\beta(x, y, 0) = w$, and $g_i(L)=C$ – by

$$\beta(x, y, 2*i+1)=c_1 \wedge \beta(x, y, 2*i+2)=d_1 \ ,$$

where (c_1, d_1) is the code of the situation C.

Exercise 3.11. Rewrite the formulas $COMPUTE_M$ and F(x, y, z), and calculate the length of each.

Thus we have an algorithm allowing to convert a Turing machine M computing the function f(x, y) into a PA formula F(x, y, z) asserting that f(x, y) = z. **To complete the proof of the Representation Theorem we must show** that for every natural numbers k, m, n such that f(k, m)=n:

a) PA proves: F(**k**, **m**, **n**).

b) PA proves: $Az(\neg(z=\mathbf{n}) \rightarrow \neg F(\mathbf{k}, \mathbf{m}, z))$.

This would take a lot of time and space. Read Mendelson [1997] or Kleene [1952] instead.

Let us think we have proved the Representation Theorem. Q.E.D.

4. Hilbert's Tenth Problem

Statement of the problem:

10. **Determination of the solvability of a Diophantine equation.** Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers. (Quoted after Hilbert's Tenth Problem page at the Steklov Institute of Mathematics at St.Petersburg.)

(See the original statement in German at http://logic.pdmi.ras.ru/Hilbert10/stat/stat.html).

4.1. History of the Problem. Story of the Solution

Linear Diophantine equations

Problems that can be solved by solving of algebraic equations in the domain of integer numbers were known since the very beginning of mathematics. Some of these equations do not have solutions at all. For example, the equation $2x-2y=1$ cannot have solutions in the domain of integer numbers since its left-hand side is always an even number. Some other equations have a finite set of solutions. For example, the equation $3x=6$ has only one solution $x=2$. And finally, some equations have an infinite set of integer solutions.

For example, let us solve the equation $7x-17y=1$:

$$x=\frac{17y+1}{7}=2y+\frac{3y+1}{7} \quad .$$

The number $\frac{3y+1}{7}$ must be an integer, let us denote it by z. Then $3y+1=7z$ and $x=2y+z$. Thus we have arrived at the equation $3y-7z=-1$ having smaller coefficients than the initial one. Let us apply our coefficient reduction idea once more:

$$y=\frac{7z-1}{3}=2z+\frac{z-1}{3} \quad .$$

The number $\frac{z-1}{3}$ must be an integer, let us denote it by t. Then $z=3t+1$, and

$$y=2z+t=7t+2,$$

$$x=2y+z=2(7t+2)+3t+1=17t+5.$$

By taking t = 0, 1, −1, 2, −2, ... we obtain an infinite set of solutions of the initial equation 7x−17y=1 (moreover, we obtain in this way **all** the solutions of this equations):

x = 5, y = 2;

x = 22, y = 9;

x = −12, y = −5;

x = 39, y = 16;

...

In general, the above "algebraic equations in the domain of integer numbers" can be defined as P=0, where P is a polynomial with integer coefficients and one, two or more variables (the "unknowns"). For example, $7x^2-5xy-3y^2+2x+4y-11=0$, or $x^3+y^3=z^3$. The problem to be solved is: given an equation P(x, y, ...) = 0, how could we determine, has it solutions in the domain of integer numbers, and, if it has, how to find all of them efficiently? Such equations are called **Diophantine equations -** after Diophantus of Alexandria (III century AD).

Exercise 4.0. Verify that the class of equalities of the form $Q_1=Q_2$, where Q_1 and Q_2 are expressions built of 0, 1, variable names, + and * (i.e. terms of PA, see Section 3.1), yields exactly the class of Diophantine equations.

The above method of solving the equation 7x−17y=1 can be used to solve an arbitrary linear equation ax+by=c. If one of the coefficients is 0, for example, if b=0, then the equation ax=b has one or no integer solutions. So, let us assume that a, b are not 0. If the coefficients a, b have a common divisor d, then we have two possibilities:

a) If d does not divide the coefficient c, then the equation has no integer solutions.

b) If d divides c, then let us divide both sides of the equation by d. In this way we can arrive at an equivalent equation $a_1x+b_1y=c_1$, where the coefficients a_1, b_1 do not have common divisors. Equations of this kind all have an infinite set of integer solutions that can be found by iterating the above "coefficient reduction method". At the end of the process we arrive at two formulas: x = et+f, y = gt+h, where e, g are not 0, and by taking t = 0, +1, −1, +2, −2, ..., we obtain all the solutions of the equation.

Thus we have a simple general method allowing to determine, given an

arbitrary linear Diophantine equation with two unknowns, has it solutions in integer numbers or not. A similar algorithm solves this problem for linear Diophantine equations with three and more unknowns.

Second-degree Diophantine equations

The next step would be to consider second-degree Diophantine equations:

$$ax^2+bxy+cy^2+dx+ey+f=0, \qquad (1)$$

where a, b, c, d, e, f are integer numbers, and at least one of the numbers a, b, c is not 0. This is a much more complicated task than solving linear equations. The general method of solving the second-degree equations involves some smart ideas by different people such as Bhaskara and Pierre Fermat, yet a complete solution is due to Joseph-Louis Lagrange (published in 1769).

See also:

John P. Robertson. Solving the equation $ax^2+bxy+cy^2+dx+ey+f=0$. Online text, May 8, 2003, pp.1-19.

About computer programs for solving the equation (1) see Methods by Dario Alpern.

In the (x,y)-plane, *t*he equation (1) always represents a curve (an ellipse, a hyperbola, or a parabola), one or two straight lines, one isolated point, or nothing. In the case of ellipse our equation can have only a finite set or no integer solutions. In the case of an isolated point our equation can have only one or no integer solutions. In the case of straight lines our equation can be reduced to one or two separate linear equations. Hence, the most interesting cases are the "hyperbolic", and the "parabolic" ones.

If a=b=c=0, then we have a linear equation. So, let us assume that at least one of the numbers a, b, c is not 0. Moreover, we can assume that a is not 0. Indeed, if a=0 and c is not 0, then we can substitute x for y and y for x. If a=c=0, then a smart idea is necessary: substitute: x = y−X, thus obtaining an equivalent equation $by^2-bXy-dX+(d+e)y+f=0$. So, let us assume that a is not 0.

Let us follow the excellent book

H. M. Edwards. Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory. Springer-Verlag, 1977 (Russian translation available).

As the first step, Lagrange rewrites (1) as a quadratic equation for x:

$$ax^2+(by+d)x+(cy^2+ey+f)=0,$$

then he multiplies it by 4a:

$$4a^2x^2 + 2*2ax(by+d) + 4a(cy^2+ey+f) = 0,$$

$$(2ax+by+d)^2 - (by+d)^2 + 4a(cy^2+ey+f) = 0.$$

Now we can introduce a new unknown Y=2ax+by+d:

$$Y^2 = (by+d)^2 - 4a(cy^2+ey+f),$$

$$Y^2 = (b^2-4ac)y^2 + 2(bd-2ae)y + (d^2-4af).$$

The number $D=b^2-4ac$ is called the **discriminator** of the equation (1).

Exercise 4.1a. If D=0, then we have the "parabolic" case. As a rule, this case is ignored in textbooks of number theory. Maybe, you would like to fill the gap? You could develop a simple "theory" of solving the "parabolic" equation (1) in integer numbers.

Or, see see Methods by Dario Alpern.

So, let us ignore the "parabolic" case (i.e. let us assume that D is not 0), and multiply the latter equation by D:

$$DY^2 = D^2y^2 + 2Dy(bd-2ae) + D(d^2-4af),$$

$$DY^2 = (Dy+bd-2ae)^2 - (bd-2ae)^2 + D(d^2-4af).$$

Now let us introduce the second new unknown X=Dy+bd−2ae:

$$X^2 - DY^2 = (bd-2ae)^2 - D(d^2-4af).$$

Hence, if the discriminator $D=b^2-4ac$ is not 0, then each integer solution (x, y) of the equation (1) yields an integer solution

$$X=Dy+bd-2ae,$$

$$Y=2ax+by+d$$

of the equation

$$X^2 - DY^2 = M, \qquad (2)$$

where D>0, or D<0, and $M = (bd-2ae)^2 - D(d^2-4af)$.

Of course, we can revert our definition of (X, Y), i.e. we can express (x, y) by (X, Y):

$$y=\frac{X-bd+2ae}{D}, \qquad (3)$$

$$x=\frac{Y-by-d}{2a}=\frac{1}{2a}\left(Y-b\frac{X-bd+2ae}{D}-d\right).$$

Since D and a are not 0, this means that a solution (X, Y) of the reduced equation (2) yields a solution (x, y) of the equation (1), if and only if X−bd+2ae is divisible by D and Y−by−d is divisible by 2a (else x and y would not be integer numbers).

Of course, this reduction process resembles the well-known reduction process of the equation (1) to its canonical form $Ax^2+By^2=1$ by a linear transformation in the field of rational numbers. The above process is "smarter" than the canonical one in that at least the coefficients of the "forward" transformation are integer numbers.

D<0 − the "elliptic" case

If D<0, then we have the "elliptic" case. Since ellipses are "finite" curves, the equation (2) has in this case a finite number or no integer solutions. Hence, so does the equation (1). All integer solutions of (1) (if any) can be found by the following process. First, let us note, that if $X^2 - DY^2 = M$, then $|X| \le \sqrt{|M|}$, and $|Y| \le \sqrt{\left|\frac{M}{D}\right|}$. Let us scan all pairs (X, Y) satisfying these conditions, checking for each pair the equality (2). If $X^2 - DY^2 = M$, then let us calculate from (3) the corresponding pair (x, y). If x and y both are integer numbers, then we have found a solution of the equation (1). In this way we will found all integer solutions of (1).

D>0 − the "hyperbolic" case

If D>0, then we have the "hyperbolic" case. Since hyperbolas are "infinite" curves, then, perhaps, the equation (2) may have (for some D and M) an infinite number of solutions.

If $D=k^2$ for some integer k, then the equation (2) can be transformed in the following way:

$$(X-kY)(X+kY) = M.$$

Exercise 4.1b. Show that if M is not 0, then this equation has a finite number or no integer solutions, and define a process allowing to find all these solutions. Consider also the case M=0.

Thus, the most complicated (i.e. the most interesting) is the case when the discriminator D is a non-square positive integer.

Thus, let us consider the equation $x^2-Dy^2=M$, where D is a positive non-square integer. The next smart idea allowing to proceed is the following. Let us rewrite $x^2-Dy^2=M$ as follows:

$$(x+ y\sqrt{D})(x - y\sqrt{D}) = M \quad . \qquad (4)$$

And let us denote by R_D the set of all real numbers having the form $x+ y\sqrt{D}$ for some integers x, y. It appears that the numbers from R_D behave like a kind of "semi-integers".

Exercise 4.1c. Verify that:

a) For each u in R_D there is only one pair of integers x, y such that $u = x + y\sqrt{D}$.

b) For each pair u, v from R_D the numbers u+v, u−v, uv also belong to R_D.

c) Let us introduce the following notion of "norm" for numbers of R_D: if $u = x + y\sqrt{D}$, then let us define: Norm(u) = $x^2 - Dy^2$. Now, verify the most remarkable fact:

Norm(uv) = Norm(u)Norm(v). Hint: multiply the two corresponding equalities (4).

Using Norm, our equation $x^2 - Dy^2 = M$ containing two unknowns can be reformulated as Norm(u)=M, i.e. as an equation containing only **one** unknown! (Indeed, there is a one-to-one correspondence between u's and x, y's.) The second remarkable fact!

Combining these two remarkable facts we can conclude the following: if Norm(u)=M and Norm(i)=1 then:

$$\text{Norm}(i^2)=1,\ \text{Norm}(i^3)=1,\ \text{Norm}(i^4)=1,\ \ldots$$

$$\text{Norm}(u)=M,\ \text{Norm}(ui)=M,\ \text{Norm}(ui^2)=M,\ \text{Norm}(ui^3)=M,\ \ldots$$

Of course, always Norm(1)=Norm(−1)=1, i.e. the equation Norm(i)=1 always has two trivial solutions i=1 and i=−1. Still, if the equation Norm(i)=1 has at least one non-trivial solution i (in R_D), then it has an infinite number of such solutions: i, i^2, i^3, i^4, ... And in this case, if for some non-zero integer M, the equation Norm(u)=M has at least one solution u (in R_D), then it has an infinite number of such solutions: u, ui, ui^2, ui^3, ... !

Moreover:

$$x + y\sqrt{D} = \frac{x - y\sqrt{D}}{x^2 - Dy^2} \quad ,$$

Hence, if $i = x + y\sqrt{D}$ and Norm(i)=1, then $\frac{1}{i} = x - y\sqrt{D}$, i.e. for each pair i, j from R_D, if Norm(j)=1, then the fraction $\frac{i}{j}$ also belongs to R_D. And: if Norm(i)=M, and Norm(j)=1, then $\frac{i}{\boldsymbol{j}}$ is another solution of the equation Norm(i)=M.

Exercise 4.1d. Let $i = x + y\sqrt{D}$ be a solution of the equation Norm(i)=1. Verify that: a) if x<0, then i<0, b) if x>0 and y<0, then i<1. Hence, if i>1, then

x>0 and y>0, i.e. $i \geq 1+\sqrt{D}$. Now, let j be another solution such that j>i. Then j/i>1 also is a solution, hence, $\frac{j}{i} \geq 1+\sqrt{D}$, $j \geq i+i\sqrt{D} > i+\sqrt{D}$. I.e. the distance between two different solutions >1 is greater than $\sqrt{D}$. Thus, among the solutions >1 there exists the least one, let us denote it by i_1.

These simple facts yield fantastic consequences! We have denoted by i_1 the least i from R_D such that i>1 and Norm(i)=1. Let i<j be two solutions of the equation Norm(i)=1. Then $\frac{j}{i} > 1$ is also a solution, hence $\frac{j}{i} \geq i_1$, i.e. $j \geq i \cdot i_1$. Thus, $i \cdot i_1$ is the least solution greater than **i**. Hence, the sequence i_1, i_1^2, i_1^3, i_1^4, ... represents all >1 solutions of the equation Norm(i)=1! Each non-trivial solution of the equation $x^2-Dy^2=1$ can be obtained − simply by changing signs − from a solution (x, y) where x, y are positive integers, i.e. from a solution >1 of the equation Norm(i)=1. Thus we have almost a complete picture!

Only one problem remains: how to detect for a given non-square integer D, has the equation $x^2-Dy^2=1$ a non-trivial solution or not? If it has, then we can take the least one: $i_1 = x_1 + y_1\sqrt{D}$, and calculate other solutions simply as i_1^2, i_1^3, i_1^4, ...!

Thus, it seems that the equation $x^2-Dy^2=1$ plays a key role in the analysis of second-degree Diophantine equations. This is because this equation was given a separate name − Pell equation. Unfortunately, Euler assigned this name accidentally, ignoring the real history. To restore Justice, Fermat's equation or Bhaskara's equation would be better terms.

Bhaskara in XII century and Pierre Fermat in XVII century knew that for a non-square D the equation $x^2-Dy^2=1$ always has an infinite set of integer solutions, they knew also how to calculate efficiently the least non-trivial solution (the so-called cyclic method, see H. M. Edwards [1977]). Still, the first complete proof of its existence obtained J. L. Lagrange − some 100 years later...

See also:

Pell's Equation at The MacTutor History of Mathematics archive

Eric W. Weisstein. "Pell Equation." From *MathWorld*--A Wolfram Web Resource.

http://mathworld.wolfram.com/PellEquation.html

John P. Robertson. Solving the generalized Pell equation $x^2 - Dy^2=N$. Online text, July 31, 2004, pp.1-26.

About the algorithmical complexity of solving the Pell equation, see

Hendrik W. Lenstra, Jr. Solving the Pell Equation. *Notices of the AMS*, Vol. 49, N 2, pp. 182-192 (online copy available).

The problem

The next step would be considering Diophantine equations of the 3rd-degree, the 4th-degree etc., and equations wiht more than two unknowns. Consider, for example, the following famous sequence of equations:

$x^3+y^3=z^3$,
$x^4+y^4=z^4$,
$x^5+y^5=z^5$,
...

Fermat's 350 years old hypothesis that none of these equations has positive integer solutions, was 100% proved as late as in September 19, 1994 (the last step is due to Andrew Wiles). See

Eric W. Weisstein. "Fermat's Last Theorem." From *MathWorld*--A Wolfram Web Resource.

http://mathworld.wolfram.com/FermatsLastTheorem.html

Solving Fermat: Andrew Wiles in NOVA Online

Until now, we still have no general method of solving an arbitrary 3rd-degree Diophantine equation. All the sophisticated methods invented by smartest number theorists apply only to very specific types of the 3rd-degree equations. Why?

Eric W. Weisstein et al. "Diophantine Equation--3rd Powers." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/DiophantineEquation3rdPowers.html
Eric W. Weisstein et al. "Diophantine Equation--4th Powers." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/DiophantineEquation4thPowers.html
Eric W. Weisstein. "Diophantine Equation--5th Powers." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/DiophantineEquation5thPowers.html
etc.

In August 6-12, 1900 in Paris the Second International Congress of Mathematicians took place. In his Wednesday morning lecture of August 8 David Hilbert stated his famous 23 mathematical problems for the coming XX century (see full text at

http://aleph0.clarku.edu/~djoyce/hilbert/problems.html). The 10th of these 23 Hilbert's problems was the following:

10. Determining the solvability of a Diophantine equation.

Given a Diophantine equation with any number of unknowns and with

rational integer coefficients: devise a process, which could determine by a finite number of operations whether the equation is solvable in rational integers.

(See the original statement in German at http://logic.pdmi.ras.ru/Hilbert10/stat/stat.html).

Note. During his lecture Hilbert mentioned only 10 of 23 problems. The remaining 13 problems (the10^{th} problem included) were formulated in a paper distributed among the participants of the congress. At first, Hilbert intended to include one more problem − the 24^{th} − about proof complexity (see a posting by Teun Kötsier on the FOM List).

In 1900 Hilbert could speak only of a **positive solution** of the problem ("devise a process..."). This was due not only to his young man's (in 1900 he was 38) optimism of the moment (entering a new century!). In 1900 none of even the smartest people could imagine that, maybe, a "process" detecting the solvability of such an enormous variety of equations is impossible? The idea that problems like Hilbert's, maybe, have **negative solutions** could appear only in 1930s, when the notion of algorithm ("process, which could determine by a finite number of operations...") was formalized. Until the class of all possible "processes" is not defined explicitly, you cannot come to the idea of proving that some "process" is impossible!

A problem is called a **mass problem**, if and only if it contains an infinite number of cases. For example, the problem of determining, is n a prime number or not, is a mass problem, since it must be solved for an infinite set of values of n. This problem is solvable: you know many algorithms for solving it (some are simple and slow, some other − faster and more complicated).

In 1936, when Turing, Post and Church introduced the first formalized concepts of algorithm, of course, they discovered also the first unsolvable mass problems. For example, the following problem appeared unsolvable: given a Turing machine M, and a natural number n, determine, will M halt (i.e. reach the final state s_{stop}) after starting its work on a tape containing the number n? (For details, see Section 3.3). This "halting problem" was proved unsolvable in the following sense: there is no Turing machine that: a) starting on the tape containing the program of a Turing machine M and a natural number n, will: b) print 1, if M halts on n, and c) print 0, if M does nor halt on n. Referring to Church's Thesis, we can say, that the halting problem of Turing machines is unsolvable for any concept of algorithm.

Another kind of unsolvable mass problems (discovered in the same 1936) are the so-called **decision problems** for formal theories. If T is a formal theory, then the following problem is associated with it: given a formula F, determine whether T proves F or not. In Section 6.3 we will prove that for PA, ZF, ZFC, etc. for any consistent fundamental theory T this problem is unsolvable.

The first mass problem of the traditional mathematics that was proved

unsolvable, is the famous **word identity problem for semigroups**. Axel Thue stated this problem in 1914, and it was proved unsolvable in 1947 by E. L. Post and A.A.Markov. For details see Mendelson [1997] or Kleene [1952].

Soon after this, in his Ph.D. theses of 1950 Martin Davis made the first step to prove that also Hilbert's Tenth Problem is unsolvable. (Martin Davis was a student of E. L. Post at New York City College and his doctorate supervisor was A. Church.)

M. Davis. On the theory of recursive unsolvability. Ph.D. Theses. Princeton University, 1950

M. Davis. Arithmetical problems and recursively enumerable predicates (abstract). "J. Symbolic. Logic", 1950, vol.15, pp.77-78

M. Davis. Arithmetical problems and recursively enumerable predicates. "J. Symbolic. Logic", 1953, vol.18, N1, pp.33-41

Still, the entire process took exactly 20 years − the last step was made in 1970 (see below).

First of all, instead of solving Diophantine equations in integer numbers we can restrict ourselves to solving of them in natural numbers − a more customary domain for mathematical logic.

Exercise 4.2. For each Diophantine equation $P(x_1, ...,x_m)=0$ build another Diophantine equation $Q(x_1, ...,x_n)=0$ such that P=0 has a natural solution, if and only if Q=0 has an integer solution. (Hint: every natural number can be expressed as a sum of 4 squares − a theorem proved by Lagrange in 1770).

Hence, if we had an algorithm determining the solvability of Diophantine equations in integer numbers, then we had also an algorithm determining their solvability in natural numbers. So, let us try disproving the existence of the latter algorithm.

Exercise 4.2a. Prove the converse: if we had an algorithm determining the solvability of Diophantine equations in natural numbers, then we had also an algorithm determining their solvability in integer numbers.

Exercise 4.3. Let $P(b, x_1, ..., x_n)=0$ be Diophantine equation containing a parameter b. Verify, that the set $S=\{b|\exists x_1 ... \exists x_n P(b, x_1, ..., x_n)=0\}$, (i.e. the set of all values of b such that the equation $P(b, x_1, ..., x_n)=0$ has a natural solution) is computably enumerable. (Hint: write a program modeling a "parallel" checking of P=0 for all possible values of b and the unknowns, printing out the required values of b, one by one.)

Some of computably enumerable sets are unsolvable (for such sets there is no algorithm determining for a given number n, is n in S, or not. For details see Mendelson [1997] or Kleene [1952].). If we could construct an equation with a parameter such that that set S would be unsolvable, then we had proved that

Hilbert's Tenth Problem is unsolvable. The simplest way to build such an equation is (surprisingly): build the corresponding equation $P(b, x_1, ..., x_n)=0$ for **every** computably enumerable set S of natural numbers.

Therefore (following M. Davis's theses), if $R(b_1, ..., b_m)$ is a predicate for natural numbers, then let us call **Diophantine representation** of R any formula

$$\exists x_1 ... \exists x_n P(b_1, ..., b_m, x_1, ..., x_n)=0 \quad ,$$

where P is a polynomial with integer coefficients, such that this formula is true for some values $(b_1, ..., b_m)$, if and only if $R(b_1, ..., b_m)$ is true. For example, the predicate "b is even number" has the following Diophantine representation: $\exists x(b-2x=0)$. Hence, Diophantine representation of a predicate $R(b_1, ..., b_m)$ is, in fact, a Diophantine equation $P(b_1, ..., b_m, x_1, ..., x_n)=0$ with parameters $b_1, ..., b_m$ that has solutions in natural numbers, if and only if $R(b_1, ..., b_m)$ is true.

M. Davis conjectured that each computably enumerable predicate has a Diophantine representation. If this would be true, then we could take an computably enumerable, unsolvable predicate S(b), and build its Diophantine representation:

$$\exists x_1 ... \exists x_n \; P(b, x_1, ..., x_n)=0.$$

Then there would be no algorithm determining for a given value of b, has the equation $P(b, x_1, ..., x_n)=0$ natural solutions or not. I.e. Hilbert's 10th problem would be proved unsolvable! Q.E.D.

As the first step, M. Davis proved in 1950 the following theorem: each computably enumerable predicate $R(b_1, ..., b_m)$ can be represented by a formula

$$\exists y \forall z (z< y \rightarrow \exists x_1 ... \exists x_n P(b_1, ..., b_m, y, z, x_1, ..., x_n)=0) \quad .$$

The elimination of the remaining (one and restricted!) universal quantifier $\forall z(z< y \rightarrow ...)$ took 20 years!

Julia Robinson made another important step in 1952:

J. Robinson. Existential definability in arithmetic. "Trans. Amer. Math. Soc.", 1952, vol. 72, N3, pp.437-449.

The problem was proposed to her by A. Tarski who had just produced his (non-trivial!) decision method for elementary algebra and geometry. Perhaps, this was the reason why Julia Robinson tried the opposite (to Davis's) way of solving the problem. Instead of trying to prove that every computably

enumerable predicate has a Diophantine representation she tried to construct Diophantine representations for particular important predicates: the exponentiation (i.e. the predicate $x=y^z$), binomial coefficients ($x=C_y^z$), the factorial function (x=y!) and the predicate "x is prime number". She was not 100% successful, yet she proved that all these predicates had Diophantine representations, if at least one "exponentially growing" function had such representation (see below).

Martin Davis and Hilary Putnam made the next step in 1960. They proved that each computably enumerable predicate $R(b_1, ..., b_m)$ can be represented by a formula

$$\exists x_1 ... \exists x_n T(b_1, ..., b_m, x_1, ..., x_n)=0 \quad ,$$

where the expression T is composed of the letters $b_1, ..., b_m, x_1, ..., x_n$, natural numbers, addition letter "+", subtraction letter "−", multiplication letter "·", and a letter representing **exponentiation** (i.e. x^y). For example, $x^{by+z}-yz+3=0$. In their proof an unproved number-theoretic hypothesis was used ("there exist arbitrary long arithmetic progressions of prime numbers"). Julia Robinson removed the need for this extra hypothesis and simplified the proof. The final result was published in 1961:

M. Davis, H. Putnam, J. Robinson. The decision problem for exponential Diophantine equations. "Annals of Mathematics", 1961, vol.74, N3, pp.425-436.

The equations $T(b_1, ..., b_m, x_1, ..., x_n)=0$ are called **exponential Diophantine equations**. Thus, in 1961 the unsolvability of (modified) Hilbert's 10th problem for exponential Diophantine equations was proved.

This was a great success (and a wonderful piece of mathematics − see Section 4.7 below), still, even it could not remove serious doubts in the perspective of the entire process (i.e. that for each computably enumerable predicate a "true" Diophantine representation will be obtained). For example, let us take the predicates "x is prime number" and "x is power of 2", and imagine that we have Diophantine representations of them:

$$\text{"b is prime number"} \equiv \quad \exists x_1 ... \exists x_k P_1(b, x_1, ..., x_k)=0 \quad ;$$

$$\text{"b is power of 2"} \equiv \quad \exists x_1 ... \exists x_m P_2(b, x_1, ..., x_m)=0 \quad .$$

Then the equation $P_1(b, x_1, ..., x_k)=0$ has solutions, if and only if b is prime, and $P_2(b, x_1, ..., x_m)=0$ has solutions, if and only if b is power of 2.

Exercise 4.4. (H. Putnam, 1960). Let the set of natural numbers A have a Diophantine representation:

$$x \in A \leftrightarrow \exists x_1 ... \exists x_n P(x, x_1, ..., x_n)=0 \quad .$$

Take the polynomial $Q = x(1-P^2)$. Verify that the set of all positive values of Q is exactly the set A. (Thanks to Milos Puzovic, who discovered an error in the previous version of this text.)

Hence, if the set of all primes or the set of all powers of 2 had Diophantine representations, then these sets could be represented as sets of positive values of appropriate polynomials. The actual number-theoretic intuition even of 1969 did not believe that this could be 100% possible.

Nevertheless, in 1970 Yuri Matiyasevich succeeded in building a Diophantine representation of an "exponentially growing" function, and hence − of the exponentiation itself:

$$a = b^c \leftrightarrow \exists x_1 \ldots \exists x_n P(a, b, c, x_1, \ldots, x_n) = 0 \quad .$$

Y. Matiyasevich. Diophantovost perechislimikh mnozhestv. "Doklady Akad. Nauk SSSR", 1970, vol.191, pp.279-282. (Enumerable sets are Diophantine, in Russian, translated in: Soviet Math. Doklady, 11(2):354-358, 1970)

This paper was presented by I. M. Vinogradov, February 5, 1970 (at that time your paper could be published in "Doklady" only if you had a recommendatory visa of a Member of Academy on it). A post factum exposition of the entire story (with some improvements in proofs etc. − another wonderful piece of mathematics, see Sections 4.3, 4.4 and 4.5 below) was published in the paper:

Y. Matiyasevich. Diophantovi mnozhestva. "Uspekhi Math. Nauk", 1972, vol.27, pp.185-222 (Diophantine sets, in Russian, translated in: Russian Mathematical Surveys, 27(5):124-164, 1972)

Using its Diophantine representation, the exponentiation could be excluded from the representations by Davis, Putnam, and Robinson, and thus for each computably enumerable predicate a Diophantine representation could be obtained. And thus, since February 5, 1970 we know 100% that **Hilbert's Tenth Problem is unsolvable**.

This result explains why solving of Diophantine equations of higher degrees is so difficult: because a **general** method of doing this is impossible. Any method determining solvability of higher-degree equations in integer numbers can be successful only for some **specific types** of equations. At the same time, this sad conclusion makes the field of Diophantine equations an inexhaustible source of challenge for mathematicians!

Exercise 4.5. Show that the solvability problem of an arbitrary Diophantine equation can be reduced: a) To the problem of solvability of a **system of second-degree** Diophantine equations consisting of one linear equation, and a set of simple second-degree equations having the form $x^2=y$ or $xy=z$. b) To the problem of solvability of a **4th-degree** Diophantine equation.

Hence, small wonder at the fact, that until now no general methods of solving are known neither for systems of second-degree equations, nor for 4th-degree equations. But what about the 3rd-degree equations? And 2nd-degree − with more than two unknowns?

Since 1970 many improvements were invented allowing, on the one hand, to shorten the chain of manipulations leading from Turing machines to Diophantine equations, and, on the other hand, allowing to reduce the "size" (number of unknowns, power, sum of coefficient modules etc.) of equations representing important predicates ("x is prime number", "x is power of 2" etc.). See, for example:

Y. Matiyasevich, J. Robinson. Reduction of an arbitrary Diophantine equation to one in 13 unknowns. "Acta Arithmetica", 1975, vol. 27, pp.521−553

Still, I find the initial versions of constructions and proofs proposed by Davis, Putnam, Julia Robinson, and Matiyasevich extremely beautiful.

See their portraits at http://logic.pdmi.ras.ru/Hilbert10/portrait/portrait.html).

This is why I present in the subsequent sections not the latest record achievements, yet the original (with only minor changes) beautiful chain of reasoning that has led to the solution of Hilbert's Tenth Problem.

For authentic comments by Martin Davis see
http://www.informatik.uni-stuttgart.de/ifi/ti/personen/Matiyasevich/H10Pbook/foreword.htm.

4.2. Plan of the Proof

The starting point is an arbitrary computably enumerable predicate $R(b_1, ..., b_m)$ for natural numbers $b_1, ..., b_m$. At the end we must obtain a Diophantine representation of R, i.e. a formula

$$\exists x_1 ... \exists x_n P(b_1, ..., b_m, x_1, ..., x_n) = 0$$

(where P is a polynomial with integer coefficients), which is true for some $(b_1, ..., b_m)$, if and only if $R(b_1, ..., b_m)$ is true.

So let us start from a computer program B_R that is printing out one by one all tuples $(b_1, ..., b_m)$ such that $R(b_1, ..., b_m)$ is true. Then the following function f_R is computable:

$f_R(b_1, ..., b_m, s) = 1$, if the program B_R prints the tuple $(b_1, ..., b_m)$ within the first s seconds of its work, and

$f_R(b_1, ..., b_m, s) = 0$, otherwise.

By Church's Thesis, if f_R is computable, then an appropriate Turing machine can compute it. Let M_R be this Turing machine. By the Representation Theorem (see Section 3.3), in the language of first order (Peano) arithmetic there is a formula $F_R(b_1, ..., b_m, s, u)$ representing the function f_R. Hence,

$$R(b_1, \dots, b_m) \leftrightarrow \exists s\, F_R(b_1, \dots, b_m, s, 1) \quad . \qquad (1)$$

This is the first representation of our predicate R by some formula. We will transform it into a Diophantine representation.

As we know from the proof of the Representation Theorem (see Section 3.3) the formula F_R is built by using only the following means:

a) Atomic formulas $t_1=t_2$ and $t_1<t_2$, where t_1, t_2 are polynomials with natural coefficients.

b) Logical operations "and" and "or" (**not** the negation!).

c) Existential quantifiers $\exists x$.

d) Only **restricted** universal quantifiers $\forall x(x< U \rightarrow ...)$, where U are linear functions of variables with natural coefficients.

Note. **Negations and unrestricted universal quantifiers are unwelcome** as means of representing computably enumerable predicates: if $R(b,c)$ is computably enumerable, then the predicates $\neg R(b,c)$ and $\forall c\, R(b,c)$ may be not computably enumerable.

Let us start the process of transforming (1) into a Diophantine representation.

Atomic formulas $t_1<t_2$ can be converted as $\exists x(t_1 + x + 1 = t_2)$. This formula is a Diophantine representation.

Exercise 4.6. Let ∃(P=0) and ∃(Q=0) be two Diophantine representations (∃'s represent blocks of existential quantifiers). Show how the conjunction $\exists(P=0)\wedge\exists(Q=0)$ and the disjunction $\exists(P=0)\vee\exists(Q=0)$ can be converted into a Diophantine representation.

And, of course, if ∃(P=0) is a Diophantine representation, then $\exists x\, E(P=0)$ is also a Diophantine representation.

Thus the only hard problem that occurs during our process of transformation is the case d) − **how to eliminate restricted universal quantifiers**? I.e. how to convert some formula

$$\forall z(z< U \rightarrow \exists x_1 \dots \exists x_n P(b_1, \dots, b_k, z, x_1, \dots, x_n)=0) \quad , \qquad (2)$$

where U is a linear function of b_1, ..., b_k with natural coefficients, into an equivalent formula

$$\exists y_1 ... \exists y_q Q(b_1, ..., b_k, y_1, ..., y_q) = 0 \quad ?$$

If we will succeed in solving this problem, then the above process of transforming (1) will yield a Diophantine representation of the predicate R. Q.E.D.

So, let us show how to eliminate $\forall z(z < U \rightarrow ...)$. This will take the rest of Section 4. Our plan is as follows:

1) A detailed investigation of solutions of Fermat's equation $x^2 - (a^2 - 1)y^2 = 1$ in natural numbers. For any a>1 this equation has an infinite sequence of solutions ($x_n(a)$, $y_n(a)$), n=0, 1, 2, ... As functions of n, $x_n(a)$ and $y_n(a)$ are growing exponentially.

2) Using the results of the investigation, we will build a Diophantine representation of the predicate

$$F(a, x, y, n) \leftrightarrow a \geq 3 \wedge x = x_n(a) \wedge y = y_n(a) \quad .$$

3) Using the Diophantine representation of the predicate F(a, x, y, n) we will build a Diophantine representation of the exponential function $x=y^z$.

4) Using the Diophantine representation of the exponential function we will build Diophantine representations of binomial coefficients ($x=C_y^z$) and the factorial function (x=y!).

5) Using the above Diophantine representations we will show how to eliminate the restricted universal quantifier from (2).

Matiyasevich solved the problems 1), 2) in 1970, Julia Robinson − the problems 3) and 4) in 1952, the problem 5) was solved by Davis, Putnam and Julia Robinson in 1961.

In subsequent sections we will follow the practice of number theorists by using the so-called **congruencies**. Congruencies are a kind of equalities, yet not exact equalities. The record

$$x \equiv y \bmod z$$

means that x−y is divisible by z (the module). (In Pascal we would write x mod z = y mod z). In other words, $x \equiv y \bmod z$ means that x=y+kz, but we wish to ignore items divisible by z. For example, $18 \equiv 78 \bmod 10$, since $78=18+6 \cdot 10$. A number x is congruent to 0 mod m ($x \equiv 0 \bmod m$), if and only if x is divisible by m.

Exercise 4.7. Prove the following properties of congruencies (allowing treating them in most cases as "normal" equalities):

$x \equiv x \bmod m$;

$x \equiv y \bmod m \rightarrow y \equiv x \bmod m$;

$x \equiv y \bmod m$, $y \equiv z \bmod m \rightarrow x \equiv z \bmod m$;

$x_1 \equiv y_1 \bmod m$, $x_2 \equiv y_2 \bmod m \rightarrow x_1+x_2 \equiv x_1+y_2 \bmod m$;

$x_1 \equiv y_1 \bmod m$, $x_2 \equiv y_2 \bmod m \rightarrow x_1x_2 \equiv x_1y_2 \bmod m$;

$xz \equiv yz \bmod mz \rightarrow x \equiv y \bmod m$.

If z has no common divisors with m, then

$xz \equiv yz \bmod m \rightarrow x \equiv y \bmod m$.

4.3. Investigation of Fermat's Equation

We will investigate only a special (the simplest!) case of Fermat's equation − where $D=a^2-1$ for some natural number a>1:

$$x^2-(a^2-1)y^2=1 \quad .$$

No problems to prove the existence of non-trivial solutions for this equation: you can simply take x=a, y=1. After this, all the other natural solutions we can calculate by using the following smart idea. Let us note that

$$x^2-(a^2-1)y^2=(x+y\sqrt{a^2-1})(x-y\sqrt{a^2-1})=1 \quad .$$

Take our first non-trivial solution x=a, y=1:

$$a^2-(a^2-1)=(a+\sqrt{a^2-1})(a-\sqrt{a^2-1})=1 \quad .$$

Consider the n-th power:

$$(a+\sqrt{a^2-1})^n(a-\sqrt{a^2-1})^n=1 \quad .$$

Now, apply the Newton's binomial formula to the expression $(a+\sqrt{a^2-1})^n$. For example, if n=2, then

$$(a+\sqrt{a^2-1})^2=a^2+2a\sqrt{a^2-1}+(a^2-1) \quad .$$

I.e. some of the items do contain $\sqrt{(a^2-1)}$, and some don't. Let us sum up either kind of the items:

$$(a+\sqrt{a^2-1})^n=x_n(a)+y_n(a)\sqrt{a^2-1} \quad , \qquad (1)$$

where x_n (a), y_n (a) are natural numbers. For example, $x_2(a)=2a^2-1$, y_2 (a)=2a. Still, in this way we can obtain also

$$(a-\sqrt{a^2-1})^n = x_n(a) - y_n(a)\sqrt{a^2-1} \qquad (2)$$

with the same x_n (a) and y_n (a) (verify!). Now multiply (1) by (2):

$$(a^2-a^2+1)^n = x_n^2 - (a^2-1)y_n^2,$$

$$x_n^2 - (a^2-1)y_n^2 = 1.$$

Hence, for any number $n \geq 0$ the pair

$x = x_n(a)$,

$y = y_n(a)$

is a solution of the equation $x^2-(a^2-1)y^2=1$. The values n=0, 1 yield the solutions that we already know: x=1, y=0, and x=a, y=1. Still, n=2 yields a new solution; $x=2a^2-1$, y=2a.

From our definition of the numbers x_n (a), y_n (a) the following recurrent identities can be derived (m, $n \geq 0$):

$$x_{m+n}(a) = x_m(a)\,x_n(a) + y_m(a)\,y_n(a)(a^2-1),$$
$$y_{m+n}(a) = x_m(a)\,y_n(a) + y_m(a)\,x_n(a) \quad .$$

For m=1 this means:

$$x_{n+1}(a) = a\,x_n(a) + (a^2-1)\,y_n(a) \quad ,$$
$$y_{n+1}(a) = x_n(a) + a\,y_n(a) \quad .$$

Exercise 4.8. Prove these identities. Verify also that x_n (a) and y_n (a) are increasing functions of n (i.e. that they really yield an infinite set of solutions of the equation $x^2-(a^2-1)y^2=1$).

It appears that the sequence $\{(x_n(a), y_n(a) \mid n \geq 0\}$ covers **all** natural solutions of Fermat's equation.

Lemma 1. If a>1, then

$$x^2-(a^2-1)y^2=1 \leftrightarrow \exists n(x=x_n(a) \wedge y=y_n(a)) \quad .$$

Proof. 1) Leftwards. This we already have proved.

2) Rightwards. Let x, y be a solution of our equation. If $x \leq 1$, then x=1 and y=0, i.e. $x=x_0(a)$, $y=y_0(a)$. Now let x>1. Then y>0. If x, y would be $x_n(a)$, $y_n(a)$, and u, v would be $x_{n-1}(a)$, $y_{n-1}(a)$, then we would have:

$x = au+(a^2-1)v$, (3)

y = u+av.

Let us express u, v from these equations:

u = ax−(a^2−1)y, (3a)

v = −x+ay.

Now forget about x_n, y_n, x_{n-1}, y_{n-1}: let the numbers u, v are simply be calculated from x, y by formulas (3a).

Exercise 4.9. Verify that $u^2-(a^2-1)v^2=1$, i.e. that (u, v) is a solution. Verify also that $0<u<x$ and $v\geq 0$.

Thus, if (x, y) is a solution of our equation, x>1, then these numbers can be expressed by formulas (3) through another solution (u, v) such that u<x. If u>1, again, we can express (u, v) through another solution (u', v') such that u'<u, etc. until we reach the solution (1, 0). If n is the number of these downward steps, then $x=x_n(a)$ and $y=y_n(a)$. Q.E.D.

Thus we have an elegant (more than 300 years old) algorithm allowing to calculate the sequence of all natural solutions of the equation $x^2-(a^2-1)y^2=1$. What makes this algorithm important in the context of Hilbert's 10th problem?

Lemma 2. If a>1 and n≥0, then

$$a^n \leq x_n(a) \leq (a+\sqrt{a^2-1})^n \quad .$$

Proof.

$$x_n(a)+y_n(a)\sqrt{a^2-1}=(a+\sqrt{a^2-1})^n \quad ,$$

$$x_n(a)=a\,x_{n-1}(a)+(a^2-1)\,y_n(a)\geq a\,x_{n-1}(a) \quad .$$

Q.E.D.

Hence, as function of n, $x_n(a)$ is growing exponentially. And this is achieved by a Diophantine condition F on x:

$$F(x)\leftrightarrow \exists y\,(x^2-(a^2-1)\,y^2=1) \quad .$$

Not bad as the first step − if we wish to find, among others, a polynomial P(x, z_1, ..., z_m) such that

$$\exists y\,(x=2^y)\leftrightarrow \exists z_1 \ldots \exists z_m P(x, z_1, \ldots, z_m) \quad .$$

(These considerations were proposed by J.Robinson in her 1952 paper.)

Now let us follow the idea due to Matiyasevich: let us investigate the remainders from dividing the numbers $x_n(a)$, $y_n(a)$ by each other.

First, let n be fixed, n>0, and let us observe the remainders from dividing $x_N(a)$ and $y_N(a)$ by $x_n(a)$ as N = 0, 1, 2, ... For this purpose we will consider mod $x_n(a)$ the above recurrent identities for x_{m+n}, y_{m+n}. I.e. we will ignore items divisible by x_n (a):

$$x_{m+n}(a)=x_m(a)x_n(a)+y_m(a)y_n(a)(a^2-1)\equiv y_m y_n(a^2-1) \bmod x_n \ ,$$

$$y_{m+n}(a)=x_m(a)y_n(a)+y_m(a)x_n(a)\equiv x_m y_n \bmod x_n \ .$$

Substitute m+n for m:

$x_{m+2n} = (a^2-1)y_{m+n}y_n \equiv (a^2-1)x_m y_n^2 \bmod x_n$,

$y_{m+2n} = x_{m+n}y_n \equiv (a^2-1)y_m y_n^2 \bmod x_n$.

Now let us note that $x_n^2-(a^2-1)y_n^2=1$, hence $(a^2-1)y_n^2 = x_n^2-1 \equiv -1 \bmod x_n$. Thus, we can replace $(a^2-1)y_n^2$ by −1:

$x_{m+2n} \equiv -x_m \bmod x_n$, (4)

$y_{m+2n} \equiv -y_m \bmod x_n$.

Substitute m+2n for m:

$x_{m+4n} \equiv -x_{m+2n} \equiv x_m \bmod x_n$,

$y_{m+4n} \equiv -y_{m+2n} \equiv y_m \bmod x_n$.

Thus, the remainders of $x_N(a)$ and $y_N(a)$ mod $x_n(a)$ are changing by the period 4n, and we can concentrate on investigating these remainders for N = 0, 1, 2, ..., 4n−1.

According to (4) we have (mod x_n):

$x_0 = x_0$, $x_1 = x_1$, ..., $x_{2n-1} = x_{2n-1}$,

$x_{2n} \equiv -x_0$, $x_{2n+1} \equiv -x_1$, ..., $x_{4n-1} \equiv -x_{2n-1}$,

$y_0 = y_0$, $y_1 = y_1$, ..., $y_{2n-1} = y_{2n-1}$,

$y_{2n} \equiv -y_0$, $y_{2n+1} \equiv -y_1$, ..., $y_{4n-1} \equiv -y_{2n-1}$.

Since the numbers x_{n+1}, ..., x_{2n-1} exceed the divisor x_n, our analysis is not yet complete. To complete it, let us consider the recurrent identities expressing x_{2n}, y_{2n} through x_{2n-m}, y_{2n-m} and x_m, y_m:

$x_{2n} = x_{2n-m}x_m + (a^2-1)y_{2n-m}y_m$,

$y_{2n} = x_{2n-m}\, y_m + y_{2n-m}\, x_m$.

Let us express x_{2n-m}, y_{2n-m} from these equations:

$x_{2n-m} = x_{2n}\, x_m - (a^2-1) y_{2n}\, y_m$,

$y_{2n-m} = y_{2n}\, x_m - x_{2n}\, y_m$.

By mod x_n: $x_{2n} \equiv -x_0 \equiv -1$ and $y_{2n} \equiv -y_0 \equiv 0$, thus we obtain:

$x_{2n-m} \equiv -x_m \bmod x_n$,

$y_{2n-m} \equiv y_m \bmod x_n$.

Now we can complete our analysis by mod x_n:

$x_0 = x_0$, $x_1 = x_1$, ..., $x_{n-1} = x_{n-1}$,

$x_n \equiv -x_n$, $x_{n+1} \equiv -x_{n-1}$, ..., $x_{2n-1} \equiv -x_1$,

$x_{2n} \equiv -x_0$, $x_{2n+1} \equiv -x_1$, ..., $x_{3n-1} \equiv -x_{n-1}$,

$x_{3n} \equiv x_n$, $x_{3n+1} \equiv x_{n-1}$, ..., $x_{4n-1} \equiv x_1$,

$y_0 = y_0$, $y_1 = y_1$, ..., $y_{n-1} = y_{n-1}$,

$y_n = y_n$, $y_{n+1} \equiv y_{n-1}$, ..., $y_{2n-1} \equiv y_1$,

$y_{2n} \equiv -y_0$, $y_{2n+1} \equiv -y_1$, ..., $y_{3n-1} \equiv -y_{n-1}$.

$y_{3n} \equiv -y_n$, $y_{3n+1} \equiv -y_{n-1}$, ..., $y_{4n-1} \equiv -y_1$.

This result allows proving of the following lemma (due to Matiyasevich):

Lemma 3. Let $a \geq 3$, $n \geq 1$, $0 < m < n$. Then for all N:

$$x_N(a) \equiv x_m(a) \bmod x_n(a) \leftrightarrow (N \equiv +m \bmod 4n) \vee (N \equiv -m \bmod 4n) \quad .$$

Note. Thanks to Milos Puzovic for discovering an error in the previous version of this text.

Proof. 1) Leftwards. If $N=4kn+m$ or $N=4kn-m$, then $x_N \equiv x_m \bmod x_n$ follows from the results of the above analysis.

2) Rightwards. Let $x_N \equiv x_m \bmod x_n$, where $0 < m < n$. Let us divide N by 4n: $N=4kn+m'$, where $0 \leq m' < 4n$.

If $m' < n$, then (according to the results of the above analysis) $m'=m$, and $N=4kn+m$. Q.E.D.

If 3n<m', then (according to the results of the above analysis) m'=4n−m, and N=4(k+1)n−m. Q.E.D.

If m'=0, m'=n, m'=2n, or m'=3n, then (according to the results of the above analysis) m=0 or m=n. This is impossible.

Exercise 4.10. Verify that the remaining alternatives n<m'<2n, 2n<m'<3n are impossible as well. (Hint: see the results of the above analysis, and note that if a>2 and i<n, then $x_i(a) < \frac{x_n(a)}{2}$.)

End of proof.

Now we must perform a similar investigation of remainders from dividing $y_N(a)$ by $y_n(a)$ (n is fixed, n≥1, N = 0, 1, 2, ...).

Exercise 4.11. Perform this investigation yourself. You will obtain that $y_N(a)$ mod $y_n(a)$ is changing with the period 2n, and (mod y_n):

$y_0 = y_0, y_1 = y_1, ..., y_{n-1} = y_{n-1}$,

$y_n \equiv -y_n, y_{n+1} \equiv -y_{n-1}, ..., y_{2n-1} \equiv -y_1$.

From this result we can derive another lemma (due to Matiyasevich):

Lemma 4. Let a≥2, n≥1. Then $y_N(a)$ is divisible by $y_n(a)$, if and only if N is divisible by n.

Proof. Immediately from the results of Exercise 4.11.

The following very important (see below) lemma also is due to Matiyasevich:

Lemma 5. Let a≥2, n≥1. Then $y_N(a)$ is divisible by $y_n^2(a)$, if and only if N is divisible by $n\,y_n(a)$.

Proof. You can easily verify (induction by k) that:

$x_{kn} \equiv x_n^k \bmod y_n^2$,

$y_{kn} \equiv k x_n^{k-1} y_n \bmod y_n^2$.

1) Rightwards. If $y_N(a)$ is divisible by $y_n^2(a)$, then by lemma 4: N=kn. If y_{kn} is divisible by y_n^2, then $kx_n^{k-1}y_n$ also is divisible by y_n^2, i.e. kx_n^{k-1} is divisible by y_n. Since $x_n^2-(a^2-1)y_n^2=1$, the number x_n cannot have common divisors with y_n, hence, k is divisible by y_n. And since N=kn, N is divisible by ny_n.

2) Leftwards. If N is divisible by ny_n, then N=kn, where k is divisible by y_n. Hence, $kx_n^{k-1}y_n$ is divisible by y_n^2, i.e. $y_N=y_{kn}$ also is divisible by y_n^2.

Q.E.D.

We will need also the following three lemmas (Lemma 6 is from the 1952 paper by J.Robinson):

Lemma 6. Let a≥2, n≥1. Then:

$x_n(a) \equiv 1 \bmod(a-1)$,

$y_n(a) \equiv n \bmod(a-1)$.

Lemma 7. Let a, a' ≥2, b≥1. Then, if a≡a' mod b, then for all n:

$x_n(a) \equiv x_n(a') \bmod b$,

$y_n(a) \equiv y_n(a') \bmod b$.

Lemma 8. Let a≥2, k≥0. Then:

$x_{2k}(a) \equiv 1 \bmod 2$, $x_{2k+1}(a) \equiv a \bmod 2$,

$y_{2k}(a) \equiv 0 \bmod 2$, $x_{2k+1}(a) \equiv 1 \bmod 2$.

Exercise 4.12. Prove these lemmas by induction.

4.4. Diophantine Representation of Solutions of Fermat's Equation

Now, following Matiyasevich, we must build a Diophantine representation of the predicate

$$F(a,x,y,n) \leftrightarrow a \geq 3 \wedge x = x_n(a) \wedge y = y_n(a) \quad .$$

I.e. we must put on x, y some "Diophantine conditions" forcing x equal to $x_n(a)$, and y − equal to $y_n(a)$. Of course, we will begin with the condition

F_1: $x^2-(a^2-1)y^2=1$.

Hence, there is m such that $x=x_m(a)$ and $y = y_m(a)$, and we must force m equal to n.

By Lemma 6, $y_m(a) \equiv m \bmod(a-1)$, hence, we could try putting the second condition

y≡n mod(a−1), then we would have m≡n mod(a−1). Unfortunately, if n≥a−1,

then we will not be able to conclude that m=n.

To avoid this difficulty, a turning movement (literally!) is necessary. Let us introduce another Fermat's equation with a free parameter A:

F_2: $X^2-(A^2-1)Y^2=1$.

And now we will require not y≡n mod(a−1), but

F_3: $Y=n \bmod (A-1)$.

(Since A is free, we may hope to ensure n<A−1). Since, for some M, $X=x_M(A)$ and $Y=y_M(A)$, then by Lemma 6, Y≡M mod(A−1), hence,

$$M \equiv n \bmod(A-1). \qquad (1)$$

This conclusion will be useful only, if we will be able to connect the new numbers (X, Y) with our initial numbers (x, y). So, let us introduce an additional module U, and let us require

F_4: $A \equiv a \bmod U \wedge X \equiv x \bmod U$.

By Lemma 7, A ≡ a mod U implies

$$x = x_m(a) \equiv x_m(A) \bmod U,$$

$$X = x_M(A) \equiv x_M(a) \bmod U.$$

From F_4 we have X ≡ x mod U, hence

$$x_M(a) \equiv x_m(a) \bmod U. \qquad (2)$$

We could apply here Lemma 3, yet then U must be a solution of Fermat's equation with the same parameter a. So, let us introduce another number V, and let us require

F_5: $U^2-(a^2-1)V^2=1$.

Hence, for some N: $U=x_N(a)$ and $V=y_N(a)$, and we can rewrite (2) as

$$x_M(a) \equiv x_m(a) \bmod x_N(a).$$

To apply Lemma 3, we must ensure that 0<m<N. This can be achieved by putting the condition

F_6: $0< x< U$

(since $x_i(a)$ is increasing by i, $0<x_m(a)=x<U=x_N(a)$ means 0<m<N). Finally, we can apply Lemma 3:

$$(M \equiv m \bmod 4N) \vee (M \equiv -m \bmod 4N). \qquad (3)$$

Now we are at the end of our turning movement. Let us compare (3) with (1):

$$M \equiv n \bmod(A-1).$$

Our intention was to force m=n. We would have achieved this, if 4N would exceed M and m (then (3) would yield M=m or M=−m), and if A−1 would exceed M and n (this would yield M=n, i.e. m=n). The way to ensure both "exceed-s" would be to force a large common divisor of A−1 and 4N. Still, we do not know the number N, how could we find a large divisor of 4N? On the other hand, we have Lemma 5: $y_N(a)$ is divisible by $y_m^2(a)$, if and only if N is divisible by $my_m(a)$. Or simply, V is divisible by y^2, if and only if N is divisible by my. Hence, if we will put the condition

F_7: V is divisible by y^2,

then 4y will be a divisor of 4N (we omit m as an unknown number that we could not force to divide A−1). Now we must put the condition

F_8: A−1 is divisible by 4y

to force 4y to be a common divisor of 4N and A−1. After this, (1) and (3) yield:

$$(M \equiv n \bmod 4y) \wedge ((M \equiv m \bmod 4y) \vee (M \equiv -m \bmod 4y)) \quad .$$

Hence,

$$(n = m \bmod 4y) \vee (n = -m \bmod 4y).$$

Since $y=y_m(a)$ is increasing by m, we have y≥m. On the other hand, we may put the condition

F_9: $\quad n \le y \quad .$

Finally, we must consider two possibilities:

1) n ≡ m mod 4y, i.e. n−m is divisible by 4y. Since |n−m|≤y, this is possible, if and only if n=m. Q.E.D.

2) n ≡ −m mod 4y, i.e. n+m is divisible by 4y. Since n+m≤2y, this is possible, if and only if n=m=0. Q.E.D.

Thus we have established that the condition

$$a \ge 3 \wedge \exists A \exists X \exists Y \exists U \exists V (F_1 \wedge F_2 \wedge F_3 \wedge F_4 \wedge F_5 \wedge F_6 \wedge F_7 \wedge F_8 \wedge F_9) \quad (4)$$

implies that $x=x_n(a)$ and $y=y_n(a)$, i.e. F(a, x, y, n).

Our task will be completed, if we will show that F(a, x, y, n) also implies (4). So, having a≥3; $x=x_n(a)$; $y=y_n(a)$, we must find the numbers A, X, Y, U, V

such that F_i are satisfied for all i=1, 2, ..., 9.

F_1: $x^2-(a^2-1)y^2=1$ is satisfied by Lemma 1.

F_9: $n \le y$ is satisfied, since $y_n(a)$ is increasing by n.

The numbers U, V (a solution of the same equation as x, y) we can choose in the following way: let N be the least even (see below!) multiple of ny, such that $x_N(a) \ge x$ (see F_6!), and let $U=x_N(a)$; $V=y_N(a)$. Then:

F_6: $x \le U$ is satisfied.

F_5: $U^2-(a^2-1)V^2=1$ is satisfied.

And by Lemma 5, V is divisible by y^2, i.e. F_7 is satisfied.

It remains to determine the parameter A of our auxiliary equation and its solution X, Y. The following conditions must be satisfied:

F_2: $X^2-(A^2-1)Y^2=1$,

F_3: $Y \equiv n \bmod (A-1)$,

F_4: $A \equiv a \bmod U \wedge X \equiv x \bmod U$,

F_8: $A-1$ is divisible by 4y.

1) **Case n=0.** Then x=1, y=0. F_4 is satisfied, since U=1. F_8 will be satisfied, if and only if we take A=1. After this, F_2 will be satisfied, if and only if we take X=1, and F_3 − if and only if we take Y=0. Q.E.D.

2) **Case n>0.** Then y>0. As the first step, let us use F_4 and F_8 to choose A. If the numbers U and 4y would have no common divisors, then we could obtain A from Chinese remainder theorem (see Section 3.3) − as a number A>1 that satisfies simultaneously $A \equiv a \bmod U$ and $A \equiv 1 \bmod 4y$. Then F_8 and the first part of F_4 would be satisfied.

So, let us prove that U and 4y have no common divisors. On the one hand, U is an odd number (by Lemma 8, since N is even number, see above). On the other hand, V is divisible by y^2, and

$$U^2-(a^2-1)V^2=1,$$

hence, U and y have no common divisors.

It remains to choose X, Y. Let us choose $X=x_n(A)$ and $Y=y_n(A)$. Then F_2 is

satisfied. By Lemma 6, F_3 also is satisfied. And finally, since $x=x_n(a)$ and $A \equiv a \bmod U$, by Lemma 7 we obtain $x_n(A) = x_n(a) \bmod U$, and $X \equiv x \bmod U$, i.e. the second part of F_4 also is satisfied. Q.E.D.

Thus, we have established the equivalence of F(a, x, y, n) and (4).

Exercise 4.13. Transform (4) into a Diophantine representation $\exists(P=0)$. Determine the number of quantifiers, the degree and the sum of coefficient modules of the polynomial P.

4.5. Diophantine Representation of the Exponential Function

Now we will use the Diophantine representation of "Fermat's" predicate F(a, x, y, n) from the previous section to obtain a Diophantine representation of the exponential function, i.e. of the predicate

$$E(u, v, n) \leftrightarrow u = v^n \wedge v \geq 3$$

(assuming that $0^0=1$).

Let us start with our fundamental equality

$$(a + \sqrt{a^2-1})^n = x_n(a) + y_n(a)\sqrt{a^2-1} \quad .$$

Let us denote $v = a + \sqrt{a^2-1}$. Then we will have simply v^n on the left hand side. On the right hand side we can replace $\sqrt{a^2-1}$ by v−a:

$$v^n - x_n(a) - y_n(a)(v-a) = 0.$$

Hence, this equation has the solution $v_1 = a + \sqrt{a^2-1}$. Since all the coefficients of it are rational numbers, the number $v_2 = a - \sqrt{a2-1}$ also is its solution. On the other hand, v_1, v_2 are solutions of the equation

$$v^2 - 2av + 1 = 0.$$

Hence, the polynomial $v^n - x_n(a) - y_n(a)(v-a)$ is divisible by $v^2 - 2av + 1$ in the field of rational numbers. Moreover, the coefficients of this fraction polynomial are integer numbers (because the leading coefficient of the divisor is 1). Thus, if v is integer, then the number $v^n - x_n(a) - y_n(a)(v-a)$ is divisible by the number $v^2 - 2av + 1$. This is the main lemma from the 1952 paper by Julia Robinson:

Lemma 9. If $a \geq 1$ and $n \geq 0$, then

$$v^n \equiv x_n(a)+y_n(a)(v-a) \bmod(v^2-2av+1).$$

Exercise 4.14. a) Verify Lemma 9 for n=0 and n=1 (the above argument is working only for n≥2).

b) Verify that

$$v^n-x_n(a)-y_n(a)(v-a) = (v^2-2av+1)\,(y_1v^{n-2}+y_2v^{n-3}+...+y_{n-2}v+y_{n-1}).$$

(This will be a direct proof of Lemma 9 − without the above "smart" algebraic considerations.)

Lemma 9 allows to connect the power v^n with the numbers $x_n(a)$, $y_n(a)$ by using polynomials of **restricted** degree ($v-a$ and $v^2-2av+1$). Having this result, we can easily obtain a Diophantine representation of $u=v^n$.

Indeed, having the variables u, v, n, we must put some Diophantine conditions that will force $u=v^n$. As the first step, let us take some numbers a, x, y, n under the condition

E_1: F(a, x, y, n).

Then $x=x_n(a)$ and $y=y_n(a)$, and by Lemma 9:

$$v^n = x+y(v-a) \bmod(v^2-2av+1).$$

In order to "bind" u and v^n, let us put the condition

E_2: $u = x+y(v-a) \bmod(v^2-2av+1)$.

Then

$$u = v^n \bmod(v^2-2av+1). \qquad (1)$$

We could derive $u=v^n$ from this congruence, if the module $v^2-2av+1$ would be greater than both u and v^n. This can be achieved by increasing the free parameter a − then $|v^2-2av+1|$ will grow as $2av-v^2-1$. Thus the condition

E_3: $u < 2av-v^2-1$

ensures one half of the necessary. Still, how to ensure $v^n<2av-v^2-1$ − by using Diophantine conditions? I.e. we must force the parameter a to grow exponentially by n. We know already from Lemma 2, that $x_n(v)$ is growing exponentially by n: $x_n(v)\geq v^n$. Hence, we can try to force $x_n(v)<2av-v^2-1$ instead of $v^n<2av-v^2-1$. So, let us introduce the numbers X, Y such that

E_4: F(v, X, Y, n),

i.e. $X=x_n(v)$ and $Y=y_n(v)$. If we add also

E_5: $X < 2av-v^2-1$,

then $v^n \le x_n(v) = X < 2av-v^2-1$. Having this result plus E_3 and (1) we obtain $u=v^n$.

Thus, we have succeeded in deriving $u=v^n$ from the condition

$$\exists a \exists x \exists y \exists X \exists Y (E_1 \wedge E_2 \wedge E_3 \wedge E_4 \wedge E_5) \quad . \qquad (2)$$

Since, $v \ge 3$ is included in E_4, we have derived also E(u, v, n) from (2).

Exercise 4.15. a) To complete the proof, derive (2) from E(u, v, n).

b) Transform (2) into a Diophantine representation $\exists (P=0)$. Determine the number of quantifiers, the degree and the sum of coefficient modules of the polynomial P.

Thus, following the work by Matiyasevich and Julia Robinson, we have obtained for the predicate $u=v^n \wedge v \ge 3$ a Diophantine representation

$$\exists z_1 ... \exists z_k P(u, v, n, z_1, ..., z_k)=0 \quad .$$

If we substitute v=3 and add the quantifier $\exists n$, we obtain a Diophantine representation

$$\exists v_1 ... \exists v_s P_1(u, v_1, ..., v_s)=0$$

of the predicate "u is a power of 3". Hence, the equation P_1 (u, v_1, ..., v_s)=0 has solutions in natural numbers, if and only if the parameter u is 3^n. This result was qualified as unexpected by some (anonymous?) number-theorists.

4.6. Diophantine Representation of Binomial Coefficients and the Factorial Function

C_y^z denotes the coefficient at p^z in the Newton's binomial formula for $(1+p)^y$.

The factorial function y! is defined as follows: 0!=0, and if y>0, then $y!=1 \cdot 2 \cdot ... \cdot y$.

Julia Robinson showed in 1952 how the predicates $z \le y \wedge x = C_y^z$ and $x=y!$ can be "Diophantine expressed" through the predicate $x=y^z$. Now, using that methods, we can obtain Diophantine representations of these predicates.

Matiyasevich improved the first method in the following way. Let us start with the Newton's binomial formula for $(1+p)^y$:

$$(1+p)^y = \sum_{z=0}^{y} C_y^z p^z \quad . \qquad (1)$$

For p=1 we would have

$$2^y = \sum_{z=0}^{y} C_y^z \quad .$$

Thus, $C_y^z \le 2^y$ for all $z \le y$.

From (1) we can obtain also:

$$(1+p)^y = u + (C_y^z + vp)p^z,$$

where

$$u = \sum_{i=0}^{z-1} C_y^i p^i \quad , \quad v = \sum_{i=z+1}^{y} C_y^i p^{i-z-1} \quad .$$

If we had $u<p^z$, then we could compute u as $(1+p)^y \bmod p^z$. And if we had also $C_y^z < p$, then we could compute C_y^z as $\frac{(1+p)^y - u}{p^z} \bmod p$, i.e. we had reduced computing of C_y^z to computing of the exponential function.

Of course, if p would be large enough (for example, $p=3^y+1$), then $C_y^z < p$ would be ensured. Still, how about $u<p^z$? Fortunately, for $p=3^y+1$:

$$u \le \sum_{i=0}^{z-1} 2^y p^i = 2^y \sum_{i=0}^{z-1} p^i = 2^y \frac{p^z - 1}{p-1} = \left(\frac{2}{3}\right)^y (p^z - 1) < p^z \quad .$$

Hence, if we wish to force $x=C_y^z$ and $z \le y$ by putting Diophantine conditions, we may try to put

$$z \le y \wedge \exists p \exists u \exists v \left(p = 3^y + 1 \wedge (1+p)^y = u + (x+vp)p^z \wedge x < p \wedge u < p^z\right) \quad (2)$$

We have already established that $x= C_y^z$ and $z \le y$ imply (2). The converse also is true. Indeed, according to (2), we can compute the value of u as $(1+p)^y \bmod p^z$, and the value of x − as $\frac{(1+p)^y - u}{p^z} \bmod p$. This is the way C_y^z is computed (see above), hence $x=C_y^z$.

Exercise 4.16. Transform (2) into a Diophantine representation $\exists(P=0)$.

Determine the number of quantifiers, the degree and the sum of coefficient modules of the polynomial P.

Now let follow another idea due to Julia Robinson to obtain a Diophantine representation of the predicate x=y!. As you may know:

$$C_w^y = \frac{w(w-1)...(w-y+1)}{y!} \quad .$$

If w would be much greater than y, then the product w(w−1)...(w−y+1) would be approximately w^y, and hence, y! would be approximately $\frac{w^y}{C_w^y}$. Let us examine this fraction more closely:

$$\frac{w^y}{C_w^y} = y! \frac{w}{w} \cdot \frac{w}{w-1} \cdot ... \cdot \frac{w}{w-y+1} \quad .$$

Let us replace w, w−1, ..., w−y+1 by w−y, then we will have:

$$y! \le \frac{w^y}{C_w^y} \le y! \left(\frac{w}{w-y}\right)^y = y! \left(1 + \frac{y}{w-y}\right)^y \quad .$$

Now, take w=y+yt:

$$y! \le \frac{w^y}{C_w^y} \le y! \left(1 + \frac{1}{t}\right)^y = y! \left(1 + \sum_{i=1}^{y} C_y^i t^{-i}\right) \quad .$$

Since $C_y^i \le 2^y$, let us take t=u2^y, then

$$y! \le \frac{w^y}{C_w^y} \le y! \left(1 + \frac{y}{u}\right) \quad .$$

And finally, by taking u=2yy^y we will have (since y!≤y^y):

$$y! \le \frac{w^y}{C_w^y} \le y! + \frac{1}{2} \quad .$$

Hence, if w=y+2$y^2 2^y y^y$, then y! can be computed as the integer part of the fraction $\frac{w^y}{C_w^y}$, and we can represent the predicate x=y! as follows:

$$\exists w \left(w = y + 2y^2 2^y y^y \wedge x = \left[\frac{w^y}{C_w^y}\right]\right) \quad . \qquad (3)$$

Exercise 4.17. Transform (3) into a Diophantine representation $\exists(P=0)$. Determine the number of quantifiers, the degree and the sum of coefficient modules of the polynomial P.

Exercise 4.18. Build a Diophantine representation of the predicate "x is prime number". Hint (J.Robinson, 1952): x is prime, if and only if x and (x−1)! do not have common divisors. You can use also J.Wilson's theorem: *x is prime number ↔ x>1 and (x−1)!+1 is divisible by x*. Which way is better?

Putnam's idea (Exercise 4.4) allows to obtain from this representation a polynomial $Q(x_1, ..., x_n)$ such that the set of positive values of Q is exactly the set of all prime numbers. Hence, despite the current number-theoretic intuition of 1969, some kind of a "formula for prime numbers" does exist!

4.7. Elimination of Restricted Universal Quantifiers

Now we have arrived at our target − producing a method that will allow converting any formula

$$\forall z\left(z< U \rightarrow \exists x_1 ... \exists x_n P\left(b_1, ..., b_k, z, x_1, ..., x_n\right)=0\right) \quad , \qquad (1)$$

where U is a linear function of $b_1, ..., b_k$ with natural coefficients, into an equivalent formula

$$\exists y_1 ... \exists y_q Q\left(b_1, ..., b_k, y_1, ..., y_q\right)=0 \quad .$$

We will follow mainly the 1961 paper by Davis, Putnam and Julia Robinson with some later improvements proposed by Matiyasevich and Julia Robinson.

For any fixed values of $b_1, ..., b_k$ the formula (1) is an **existential assertion** (despite the universal quantifier $\forall z\left(z< U \rightarrow ...\right)$) − it asserts the existence of nU numbers: the values of $x_1, ..., x_n$ for each z = 0, 1, ..., U−1. Let us denote these nU numbers by $x_i^{(z)}$:

for z=0: $x_1^{(0)}, x_2^{(0)}, ..., x_n^{(0)}$,

for z=1: $x_1^{(1)}, x_2^{(1)}, ..., x_n^{(1)}$,

...

for z=U−1: $x_1^{(U-1)}, x_2^{(U-1)}, ..., x_n^{(U-1)}$.

We could eliminate the universal quantifier $\forall z\left(z< U \rightarrow ...\right)$, if we could find some coding that allowed to represent this table by a sequence of m natural numbers $y_1, ..., y_m$ (where m does not depend on U). Then we could try to replace $\forall z\left(z< U \rightarrow ...\right)$ by $\exists y_1 ... \exists y_m$ (plus solving, of course, all the other remaining technical problems).

For example, let us try to code each of the n columns of our table by a single

number using the Chinese Remainder Theorem. If we had numbers u_0, u_1, ..., u_{U-1} such that two of them never had common divisors, then we could obtain n numbers w_1, ..., w_n such that each $x_i^{(z)}$ would be $w_i \bmod u_z$, i.e.

$$x_i^{(z)} < u_z \wedge w_i \equiv x_i^{(z)} \bmod u_z \qquad (2)$$

for all z<U and i = 1, ..., n. Of course, the numbers u_z must be large enough to serve this purpose.

Still, even if we will succeed in finding u_0, u_1, ..., u_{U-1}, then how to force the remainders $x_1^{(z)}$, ..., $x_n^{(z)}$ to satisfy the equation of (1) for all z = 0, 1, ..., U−1? Let us simply try to substitute the numbers w_1, ..., w_n for x_1, ..., x_n into the equation of (1). For z let us substitute some number Z to be determined later. What could we say about the value of $P(b_1, ..., b_k, Z, w_1, ..., w_n)$? If we added to (2) the condition

$$Z \equiv z \bmod u_z \text{ for all } z = 0, 1, ..., U-1, \qquad (3)$$

then we could conclude that

$$P(b_1, ..., b_k, Z, w_1, ..., w_n) \equiv P(b_1, ..., b_k, z, x_1^{(z)}, ..., x_n^{(z)}) \bmod u_z.$$

Since all the right hand side values of P are 0, we obtain that

$$P(b_1, ..., b_k, Z, w_1, ..., w_n) \equiv 0 \bmod u_z$$

for all z<U, i.e. the left hand side number is divisible by all the numbers y_z. Since two of these numbers never have common divisors, the left hand side number is divisible also by the product of them, i.e.

$$P(b_1, ..., b_k, Z, w_1, ..., w_n) \equiv 0 \bmod u_0 u_1 ... u_{U-1}. \qquad (4)$$

Now let us view (4) not as a consequence of some assumptions, but as a **condition** that is put on the numbers w_1, ..., w_n. If the numbers $x_i^{(z)}$ are defined as $w_i \bmod u_z$, then from (2), (3) and (4) we obtain that for all z<U:

$$P(b_1, ..., b_k, z, x_1^{(z)}, ..., x_n^{(z)}) \equiv 0 \bmod u_z.$$

We would like to force an "absolute" 0 on the right hand side instead of 0 mod u_z. This would be achieved, if the left hand side number would be less than u_z.

Exercise 4.19. Let N be the degree of the polynomial P, M − the sum of its coefficient modules, z<U, and let X exceed all $x_i^{(z)}$. Verify that

$$|P(b_1, ..., b_k, z, x_1^{(z)}, ..., x_n^{(z)})| \le T,$$

where $T = M((b_1+1)...(b_k+1)(X+1)U)^N$.

Hence, we must produce a (possibly simple) generator of divisors u_z ($z = 0, 1, ..., U-1$) such that:

a) $u_z > T$ for all $z<U$.

b) The module of (4), i.e. the product $u_0u_1...u_{U-1}$ is a possibly simple (i.e. "Diophantine") function. Otherwise we will have problems with finding a Diophantine representation of $u_0u_1...u_{U-1}$.

c) Two of the numbers u_z never have common divisors.

The following idea of producing u_z is due to Matiyasevich and Julia Robinson. Let V be a large number (to start, let $U \le V$), then we can generate u_z in such a way that $u_0u_1...u_{U-1} = C_V^U$ (i.e. b) will be satisfied). Indeed,

$$C_V^U = \frac{V(V-1)...(V-U+1)}{U!} = (\frac{V+1}{1}-1)(\frac{V+1}{2}-1)...(\frac{V+1}{U}-1) \quad .$$

Let us take

$$u_z = \frac{V+1}{z+1} - 1 \quad .$$

If we put the condition "V+1 is divisible by U!", then all u_z will be integer numbers. If we put a stronger condition "V+1 is divisible by $(U!)^2$", then two of these numbers will never have common divisors (i.e. c) will be satisfied).

Exercise 4.20. Verify that this is the case. (Hint: let d be a common prime divisor of u_i and u_j, consider u_i and u_i-u_j.)

If we put also the condition $u_{U-1}>T$ (note that u_{U-1} is the least of all u_z), i.e.

$$u_{U-1} > M((b_1+1)...(b_k+1)(X+1)U)^N,$$

then a) also will be satisfied.

Now let us sum up all the conditions we have put on the numbers we have introduced, i.e. $w_1, ..., w_n$, Z, X, V:

G_1: $P(b_1, ..., b_k, Z, w_1, ..., w_n) = 0 \ mod \ C_V^U$,

G_2: $\forall z(z < U \rightarrow Z \equiv z \ mod \ uz)$,

G_{3i}: $\forall z(z< U \to w_i \, mod \, u_z < X)$ for each i = 1, ..., n,

G_4: $u_{U-1} > M((b_1+1)...(b_k+1)(X+1)U)^N$,

G_5: V+1 is divisible by $(U!)^2$,

where, of course, $u_z = \frac{V+1}{z+1} - 1$.

About G_{3i}: since T depends on X, we must ensure also: $w_i \, mod \, u_z < X$ for all z<U and i = 1, ..., n (otherwise the estimate of the exercise 4.19 will not hold).

Exercise 4.21. Verify that (1) is equivalent to the following formula:

$$\exists Z \exists X \exists V \exists w_1 ... \exists w_n G_1 \wedge G_2 \wedge G_4 \wedge G_5 \wedge G_{31} \wedge ... \wedge G_{3n} \quad . \qquad (5)$$

(Hints. Rightwards: first choose X to satisfy G_{3i}'s, then choose V to satisfy G_5 and G_4, generate the divisors u_z, obtain the number Z by using Chinese Remainder theorem to satisfy G_2, obtain the numbers w_1, ..., w_n by using Chinese Remainder theorem to satisfy (2), and finally, derive G_1. Leftwards: having the numbers w_1, ..., w_n, Z, X, V take for each z<U: $x_i^{(z)} \equiv w_i \, mod \, u_z$, etc.)

Why should we view (5) as a step forward from (1), when G_2 and G_{3i} contain the same quantifier $\forall z(z< U \to ...)$? In (1) this quantifier stands over an arbitrary Diophantine representation, but in G_2 and G_{3i} it stands over simple specific formulas!

First, we need not to eliminate Az<U from G_2, we can eliminate the entire G_2. Indeed, we can take Z equal to V: since V−z is divisible by

$$u_z = \frac{V+1}{z+1} - 1 = \frac{V-z}{z+1}$$

(the fraction is equal to z+1), we have $V \equiv z \bmod u_z$ for all z<U.

So, we can delete G_2 from our list of conditions, replace G_1 by

G_1': $P(b_1, ..., b_k, V, w_1, ..., w_n) \equiv 0 \bmod C_V^U$,

and delete the quantifier $\exists Z$ from (5).

Now let us set to eliminating $\forall z(z< U \to ...)$ from G_{3i}. If $w_i \bmod u_z < X$, then one of the numbers w_i, w_i-1, ..., w_i-X+1 is divisible by u_z, i.e. their product

$$w_i(w_i-1)\ldots(w_i-X+1)=\frac{w_i!}{(w_i-X)!} \qquad (6)$$

also is divisible by u_z for all z<U. Since two of the numbers u_z never have common divisors, the number $\frac{w_i!}{(w_i-X)!}$ is divisible by their product $u_0u_1\ldots u_{U-1}=C_V^U$. Hence, if G_{3i}, then

G_{3i}': $\frac{w_i!}{(w_i-X)!}$ is divisible by C_V^U .

Thus we have got rid of the quantifier Az<U by introducing well-known functions! Still, unfortunately, G_{3i}' does not imply G_{3i}, i.e. these conditions are not equivalent! Indeed, if we know only that the product (6) is divisible by another product $C_V{}^U$, then we cannot guarantee that for each z<U the factor u_z will divide one of the factors w_i, w_i-1, ..., w_i-X+1.

If the number R divides the product $P_1P_2\ldots P_k$, then $R=R_1R_2\ldots R_k$, where each factor R_i divides the corresponding P_i. If R_j is maximum among the factors R_i, then $R_j^k\geq R$, i.e. $R_j\geq\sqrt[k]{R}$. Hence, if R divides the product $P_1P_2\ldots P_k$, then R and one of the factors P_j have a common divisor $\geq \sqrt[k]{R}$. This is the maximum we can guarantee!

Thus, if we replace G_{3i} by G_{3i}', then we can guarantee only that some w_i-j (where $0\leq j<X$) and u_z have a common divisor $\geq \sqrt[k]{R}$. Fortunately, this is enough to solve our problem completely!

Indeed, for a fixed z<U let us proceed from w_1 to w_n in the following way. We know that the product $w_1(w_1-1)\ldots(w_1-X+1)$ always is divisible by u_z. Then, first, for some number $x_1^{(z)}<X$ the difference $w_1-x_1^{(z)}$ is divisible by some divisor $S_1\geq\sqrt[X]{u_z}$ of the number u_z. Of course, the product $w_2(w_2-1)\ldots(w_2-X+1)$ also is divisible by S_1. Hence, next, for some number $x_2^{(z)}<X$ the difference $w_2-x_2^{(z)}$ is divisible by some divisor $S_2\geq\sqrt[X]{S_1}\geq\sqrt[X^2]{u_z}$ of the number S_1 (and of u_z). Etc., finally, for some number $x_n^{(z)}<X$ the difference $w_n-x_n^{(z)}$ is divisible by some divisor $S_n\geq\sqrt[X]{S_{n-1}}\geq\sqrt[X^n]{u_z}$ of the number S_{n-1} (and of u_z).

Hence, for all i = 1, ..., n:

$$w_i \equiv x_i^{(z)} \bmod S_n, \qquad (7)$$

where S_n divides u_z (and hence, C_V^U), and $S_n \geq \sqrt[X^n]{u_z}$. From G_1' we have:

$$P(b_1, ..., b_k, V, w_1, ..., w_n) \equiv 0 \bmod S_n,$$

hence, by (7) and, since $V \equiv z \bmod u_z$,

$$P(b_1, ..., b_k, z, x_1^{(z)}, ..., x_n^{(z)}) \equiv 0 \bmod S_n.$$

Since $z<U$ and all $x_i^{(z)}<X$, the left hand side value of P does not exceed

$$T = M((b_1+1)...(b_k+1)(X+1)U)^N.$$

Hence, this value of P will be forced to be an "absolute" 0, if $\sqrt[X^n]{u_z}$ will be greater than T. Thus, we must replace G_4 by a stronger condition

G_4': $\sqrt[X^n]{u_z} > M\left((b_1+1)...(b_k+1)U(X+1)U\right)^N$,

and our problem finally is 100% solved!

Exercise 4.22. Verify once more that (1) is equivalent to the formula

$$\exists X \exists V \exists w_1 ... \exists w_n G_1' \wedge G_4' \wedge G_5 \wedge G_{31}' \wedge ... \wedge G_{3n} \quad .$$

Transform this formula into a Diophantine representation.

Q.E.D.

4.8. 30 Ans Apres

Further reading:

Hilbert's 10th problem database in St. Petersburg

Hilbert's 10th Problem. By Yuri Matiyasevich. MIT Press, 1993, 288 pp. For details see http://logic.pdmi.ras.ru/~yumat/H10Pbook/ (Russian original available).

Yuri Matiyasevich. A direct method for simulating partial recursive functions by Diophantine equations. *Annals of Pure and Applied Logic*, 67(1-3): 325-348, 17 May 1994

Yuri Matiyasevich. Elimination of Quantifiers from Arithmetical Formulas Defining Recursively Enumerable Sets. ACA'2002: 8th International Conference on Applications of Computer Algebra. Volos, Greece, June 25-28, **2002**. (See online Abstract.)

Jones, J.P. Universal diophantine equation. *Journal of Symbolic Logic,* 47 (1982), 549-571. MR 84e:10070.

For the 1982 state of art, see online Abstract of this paper, for example:

Theorem (Matiyasevich, 1977). Every computably (recursively) enumerable set A is Diophantine definable **in 9 unknowns, degree $1.6*10^{45}$**:

$$x \in A \leftrightarrow \exists x_1 \exists x_2 \ldots \exists x_9 \, P(x, x_1, x_2, \ldots, x_9) = 0 \quad .$$

Theorem. Every computably enumerable set A is Diophantine definable **in 26 unknowns, degree 24**:

$$x \in A \leftrightarrow \exists x_1 \exists x_2 \ldots \exists x_{26} \, P(x, x_1, x_2, \ldots, x_{26}) = 0 \quad .$$

Theorem. Every computably enumerable set A is Diophantine definable **in 58 unknowns, degree 4**:

$$x \in A \leftrightarrow \exists x_1 \exists x_2 \ldots \exists x_{58} \, P(x, x_1, x_2, \ldots, x_{58}) = 0 \quad ;$$

etc.

See also Section 6.5 (about the "Diophantine Incompleteness Theorem").

5. Incompleteness Theorems

5.1. Liar's Paradox

Epimenides (VI century BC) was a Cretan angry with his fellow-citizens. And he suggested that "All Cretans are liars". Is this statement true or false?

a) If Epimenides' statement is true, then Epimenides also is a liar, i.e. he is lying permanently (?), hence, his statement about all Cretans is false (and there is a Cretan who is not a liar). We have come to a contradiction.

b) If Epimenides' statement is false, then there is a Cretan, who is not a liar. Is Epimenides himself a liar? No contradiction here.

Hence, there is no direct paradox here, only an amazing chain of conclusions: if a Cretan says that "All Cretans are liars", then there is a Cretan who is not a liar.

Still, do not allow a single Cretan to slander all the Cretans. Let us assume that Epimenides was speaking about himself only: "I am a liar". Is this true or false?

a) If this is true, then Epimenides is lying permanently, and hence, his statement "I am a liar" also is false. I.e. Epimenides is not a liar (i.e. sometimes he does not lie). We have come to a contradiction.

b) If Epimenides' statement is false, then he is not a liar, i.e. sometimes he does not lie. Still, in this particular case he **is** lying. No contradiction here.

Again, there is no direct paradox here, only an amazing chain of conclusions: if someone says "I am a liar", then he is not a (permanent) liar.

The next step in this story is due to Eubulides (IV century BC) who suggested, "I am lying". I.e. he said that he is lying right now. Is this true or false?

a) If this is true, then Eubulides is lying (right now!), and hence, his statement must be false. We have come to a contradiction.

b) If this is false, then Eubulides is not lying, and hence, his statement must be true. We have come to a contradiction.

Thus we have arrived at a real paradox, the famous **Liar's paradox.**

We would believe that any sentence like as "I am writing" or "I am reading" must be either true or false. Still, the sentence "I am lying" cannot be qualified as true or false without contradictions. During the past two thousand years many people have thought that such paradoxes should be "solved" by

inventing appropriate "rules of correct speaking". They have never been 100% successful, since any such "rules" always prohibit not only (some, but not all) paradoxes, but also many harmless and even useful sentences. For me, **the creative potential hidden in paradoxes seems much more interesting** than the "rules of correct speaking".

The "development process" of the Liar's paradox described above ended in XIV century when Jean Buridan stated it in an absolutely clear form:

"All statements on this folio are false."

P.S. There is only this one statement on "this folio".

Today's Buridan would say simply:

p: p is false.

If p is true, then p must be false. If p is false, then p must be true.

Note. Buridan is known also as the owner of the famous donkey ("Buridan's Ass"), who starved to death standing equidistant from two identical piles of hay being unable to find "sufficient arguments" to choose one of them.

For those people who believe that the "rules of correct speaking" do not allow statements referring to themselves, Albert of Saxony proposed in XIV century the following paradoxes (see Styazhkin [1967]):

p_1: p_2 is false,
p_2: p_1 is true.

q_1: q_2 is false,
q_2: q_3 is false,
q_3: q_1 is false.

Exercise 5.1. Today, following these examples, mathematicians could invent much more sophisticated paradoxes... Try yourself. End of Exercise 5.1.

Let us try "accepting" the Liar's paradox by extending the usual classification of statements as true or false only:

a) True statements,

b) False statements,

c) Statements having no truth-value.

Now consider the statement:

q: q is false or q has no truth-value.

a) If q is true, then either q is false or q has no truth-value, i.e. q is not true. We have come to a contradiction.

b) If q is false, then q is true. We have come to a contradiction.

c) If q has no truth-value, then q is true. We have come to a contradiction.

Hence, our extended classification of statements is incomplete again. The above statement q is called the **Extended Liar's paradox.**

Exercise 5.2. In some sense, the Liar is a paradox of the usual two-valued logic, and q is a paradox of three-valued logic. Formulate an analogous paradox of four-valued logic etc. How far can we go this way?

For historical details see:

N. I. Styazhkin. Formation of the Mathematical Logic. Nauka Publishers, Moscow, 1967, 400 pp. (in Russian, see also the English translation: Styazhkin, N. I. History of Mathematical Logic from Leibniz to Peano. MIT Press, Cambridge, MA, 1969)

Curry's Paradox

Exercise 5.2A. The idea of the following paradox was proposed in 1942 by Haskell B. Curry – in our notation, **p: if p is true, then q is true** (i.e. p denotes the statement "if p, then q"). Do not read the explanation below. Try analyzing yourself.

Explanation. Is p true, or false? If p is false, then "if p, then q" (since p is false) is a true statement, i.e. p is true. Contradiction, i.e. p must be true. But then "if p, then q" (as a true statement) implies that q is true. Hence, we have proved that q is true. What is q? An arbitrary assertion! "The world is trivial!" – as you can read in the online article Curry's Paradox in Stanford Encyclopedia of Philosophy.

Exercise 5.2B (for smart students). One may wish to try generating a paradox **p: F(p, q)** from any 2-argument Boolean function F. There are 16 such functions. Which of these functions generate a real paradox? (Hint: at least 7, i.e. 1 Liar's and 6 Curry's?)

5.2. Arithmetization and Self-Reference Lemma

Would it be possible to formulate the paradoxes of the previous section in a formal theory like PA?

Taken directly, Buridan's statement should mean a formula Q in the language of PA that is... equivalent to ¬Q. Thus, as a statement about natural numbers, Q must be true and false simultaneously. Is this possible? We do not believe that, but do not know how to prove it.

Thus, if we wish to reconstruct the classical Liar's paradox in a formal theory, then we must speak not about "truth", but about the more well defined notion

of provability. Could we build a formula Q "asserting" that PA proves ¬Q:

Q: PA proves ¬Q.

How could one force a formula to "assert" its own properties? Moreover, how at all we could force a formula to "speak" about formulas? Normally, formulas of first order arithmetic are "speaking" about natural numbers. In order to force these formulas to "speak" about themselves we must introduce some **numerical coding** of formulas.

First let us fix some enumeration of basic symbols of PA (let us build variable names via the following pattern: x, xa, xaa, xaaa...):

x	a	0	1	+	*	'=	(	)	¬	′∧′	′∨′	→	∃	∀
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

Now, each formula can be represented as a sequence of natural numbers. For example, the formula x=(xa+1)+1 can be represented as 0, 6, 7, 0, 1, 4, 3, 7, 4, 3. By using Gödel β-function (see Section 3.3) each sequence of natural numbers can be represented by two numbers. For example, the code of the formula x=(xa+1)+1 will consist or two numbers m, n such that:

β(m, n, 0)=10 (length of the formula);

β(m, n, 1)=0; β(m, n, 2)=6; β(m, n, 3)=7; β(m, n, 4)=0; β(m, n, 5)=1;
β(m, n, 6)=4; β(m, n, 7)=3; β(m, n, 8)=7; β(m, n, 9)=4; β(m, n, 10)=3.

From Section 3.3 we know that such two numbers m, n do exist. As the last step, we can represent the pair (m, n) by a single number k, for example, by

$$k = (m+n)^2+m.$$

Exercise 5.3. Show how to restore m and n from a given k.

Therefore, we can represent each PA-formula F by a single natural number. Let us denote by bold **F** the PA-term corresponding to this number, and let us call it **Gödel number of F**. (It was one of Gödel's crucial ideas – representing formulas by numbers, thus making possible to discuss formulas in the language of arithmetic.). Having a formula F we can calculate its Gödel number **F**, and having the number **F**, we can restore F.

Note. Today, the idea of a numerical coding of formulas may seem almost trivial (just "another coding" among many of them used on computers every second). However, in 1930, when Gödel invented such a coding for the first time, it was, perhaps, **one of the crucial and most difficult ideas** of his famous incompleteness proof – the first step in **arithmetization of syntax**.

As remembered by Janis Barzdins, in 1960s, Andrey N. Kolmogorov described his own feelings of 1930s about Gödel's Theorem as follows: would I had received a telegram containing the idea of arithmetization, I had been proved Gödel's Theorem myself.

Now let us take two PA-formulas C(x) and B. We can view the formula C(**B**) as an assertion "formula B possess the property C". If we could prove in PA that B↔C(**B**), we could say that B "asserts" that it possess the property C.

Self-Reference Lemma. If a PA-formula C(x) contains exactly one free variable x, then one can build a closed PA-formula B such that:

PA proves: B↔C(**B**).

Note. In other textbooks, this lemma is called also *Diagonalization Lemma*, or *Fixed-Point Lemma*.

Proof. Let us introduce the so-called **substitution function** sub(x, y). We define the value sub(x, y) as follows: if x is Gödel number of of some formula F(u, v, w,...), then we substitute the number-term **y** for all free variables of F, i.e. we obtain the formula F(**y**, **y**, **y**,...), then we calculate its Gödel number n, and set sub(x, y)=n. If x is not Gödel number of a formula, then we set sub(x, y)=0.

No doubt, sub(x, y) is a computable function. Given x and y, we determine first, is x number of some formula or not. If not, the function returns 0. If yes, we restore the formula, substitute y for all of its free variables and return the number of the formula obtained. No problem to code this program, for example, in Pascal (it would be an extensive work, yet not a hard one). Somewhat more tedious work would be coding the program of sub(x, y) for a **Turing machine**. We will not do this work here, using the **Church's Thesis** instead: any function that seems to be computable can be coded for an appropriate Turing machine.

So, let us assume that we already have a Turing machine computing sub(x, y). Using the algorithm from the proof of the Representation Theorem (Section 3.3) we can build a PA-formula SUB(x, y, z) such that for all k, m, n: if sub(k, m)=n, then

a) PA proves: SUB(**k**, **m**, **n**),

b) PA proves: ¬(z=**n**)→¬SUB(**k**, **m**, z).

First step. Having two formulas SUB(x, y, z) and C(x) let us introduce the following formula $C_1(x)$: C(sub(x, x)). Or more precisely (since we do not have in PA the function symbol *sub*):

∀z(SUB(x, x, z)→C(z)).

The main idea is here the repetition of x in sub! Now, what is "asserted" in the formula $C_1(x)$? Literally, the following: "Take the number x, restore from x the formula $F_x(u, v, w,...)$ having this x as a Gödel number, then substitute x (i.e. the number of F_x itself) for all free variables of F_x, i.e. obtain the formula

$F_x(x, x, x,...)$, and this formula will possess the property C".

Second step. Let us try to apply this operation to the formula $C_1(x)$ itself! I.e., if k is the number of $C_1(x)$, let us denote by B the formula $C_1(\mathbf{k})$. What is the "assertion" of B? "If you take the formula having the number k (i.e. the formula $C_1(x)$), and substitute its number k for x, then you will obtain a formula (in fact, the formula $C_1(\mathbf{k})$, i.e. the formula B) that possess the property C." Hence, B asserts; "I possess the property C"!

Warning! Do not try to follow the above argument more than twice. It may cause health problems – the Self-Reference Lemma is a kind of fixed-point theorems!

Now, to complete the proof, we must prove in PA that B↔C(**B**).

1. Let us prove in PA that B→C(**B**). Let us assume B, i.e. $C_1(\mathbf{k})$, or

$$\forall z(\mathrm{SUB}(\mathbf{k}, \mathbf{k}, z)\rightarrow C(z)). \qquad (1)$$

Since sub(k, k)= **B**, then:

PA proves: SUB(**k**, **k**, **B**), and PA proves: ¬(z=**B**)→¬SUB(**k**, **k**, z). (2)

Hence, z in (1) equals to **B**, and we obtain C(**B**). The Deduction theorem does the rest: PA proves: B→C(**B**).

2. Let us prove in PA that C(**B**)→B. Let us assume C(**B**). Then we have SUB(**k**, **k**, **B**)→C(**B**). Add (2) to this, and you will have ∀z(SUB(**k**, **k**, z)→C(z)), and this is exactly the formula B. The Deduction theorem does the rest: PA proves: C(**B**)→B.

Q. E. D.

So, for any property of formulas we can build a formula that "asserts" that it possess this property.

About the authors. Kurt Gödel invented the argument used in the proof of Self-Reference Lemma to prove his famous incompleteness theorem in 1930. Still, he did not formulate the Self-Reference Lemma as a general statement. In later notes, he attributed it to Rudolf Carnap. See copies of all the relevant papers in:

Martin Davis. The Undecidable. Basic papers on undecidable propositions, unsolvable problems and computable functions. – *Raven Press*, New York, 1965, 440 pp.

Exercise 5.4 (inspired by the paper of Andrzej Mostowski mentioned below). Show that, if B(x,y) and C(x,y) are two PA-formulas containing exactly two free variables, then one can build two closed PA-formulas D and E such that:

PA proves: D↔B(**D**, **E**), and PA proves: E↔C(**D**, **E**).

If B contains only y, and C contains only x then D↔B(**E**) and E↔C(**D**), i.e.

formulas D, E "slander" each other. (Hint: Introduce the substitution function $sub_2(x, y, z)$ – define the value $sub_2(x, y, z)$ as follows: if x is Gödel number of of some formula F(u, v, w,...), then substitute the number-term **y** for u, and the number term **z** – for all the other free variables of F, i.e. obtain the formula F(**y**, **z**, **z**,...), then calculate its Gödel number n, and set $sub_2(x, y, z)=n$. After this, consider $B(sub_2(x, x, y), sub_2(y, x, y))$ and $C(sub_2(x, x, y), sub_2(y, x, y))$, etc.).

A. Mostowski. A generalization of the incompleteness theorem. "Fundamenta Mathematicae", 1961, vol.49, N2, pp.205-232.

5.3. Gödel's Incompleteness Theorem

It seems that Self-Reference Lemma allows formulating the Liar's paradox in PA. In this way, inconsistency of PA will be proved?

The formal version of Liar's paradox would be a formula L that asserts "PA proves ¬L". Then ¬L would assert "PA cannot prove ¬L". Hence, instead of L we could use a formula G asserting, "PA cannot prove G" (i.e. "I am not provable in PA"). This version of Liar's paradox was used in the original Gödel's proof. Let us follow the tradition.

We could obtain Gödel's formula:

G: PA cannot prove G

from Self-Reference Lemma, if we had a formula PR(x) asserting "the formula number x can be proved in PA". Indeed, by applying this lemma to the formula ¬PR(x) we would obtain the formula G such that

PA proves: $G \leftrightarrow \neg PR(\mathbf{G})$,

i.e. G would be equivalent to "PA cannot prove G". So, let us first build the formula PR(x). Each proof (in PA) is a sequence of formulas. Replace all the formulas of the sequence by their Gödel numbers, this converts each proof into a sequence of natural numbers. You can code this sequence by a single number (using the techniques of the previous section). Let us call this number the **Gödel number of the proof**. Given a natural number y, you can:

a) Determine whether y is a number of some sequence of formulas or not.

b) If it is, you can restore the sequence and its formulas.

c) Having the sequence of formulas you can check whether it is a proof in PA or not. In a PA-proof each formula must be either an axiom of PA, or a logical axiom, or it must be derived from some previous formulas of the proof by using one of the logical inference rules.

Hence, the following predicate seems to be computable:

prf(x, y) = "y is a number of a PA-proof ending with the formula number x".

According to Church's Thesis we can construct a Turing machine checking correctly the truth value of prf(x, y) for arbitrary x and y. After this, according to Representation Theorem (Section 3.3) we can construct a PA-formula PRF(x, y) expressing the predicate prf(x, y) in the following formal sense:

a) If k is a number of a PA-proof ending with the formula F, then PA proves PRF(**F**, **k**), where **F** is the Gödel number of F.

b) If k is not a number of a PA-proof ending with the formula F, then PA proves ¬PRF(**F**, **k**).

This completes the **arithmetization of syntax** started in Section 5.2.

Now we can take the formula ∃yPRF(x, y) as the formula asserting "the formula number x can be proved in PA". By applying Self-Reference Lemma to the formula ¬∃yPRF(x, y) we obtain Gödel's formula G such that

PA proves: G ↔ ¬∃yPRF(**G**, y). (1)

I.e. G says, "PA cannot prove G".

Let us try to check whether the assertion of G is true or false.

1. First, let us assume that **PA proves G**, and k is the number of this proof. Then prf(**G**, k) is true and hence,

PA proves: PRF(**G**, **k**),

PA proves: ∃yPRF(**G**, y),

PA proves: ¬G

(see (1)). Therefore, if we had a PA-proof of G, then we could build also a PA-proof of ¬G, i.e. PA would be an inconsistent theory. Is PA consistent? I do not know. Still, if it is, then G cannot be proved in PA.

2. Now, let us assume that – on the contrary – **PA proves ¬G**. Then PA proves ∃yPRF(**G**, y) (see (1)). Intuitively, ∃yPRF(**G**, y) says that there exists PA-proof of G, i.e. it seems that PA is inconsistent also in this case? Still, we must be careful: if PA proves ∃yPRF(**G**, y), does it mean that by substituting for y one by one of all numbers 0, 1, 2, 3,... , and checking each case, we will find the proof of G?

We would like to think so, yet we are not able to prove that this is the case. If, by the above-mentioned substituting and checking we will really find a proof of G, then PA will be proved inconsistent. Still, what if PA is consistent? Then, in this way, we will never find a proof of G. But, nevertheless, we will have an **unpleasant situation**: there is a formula PRF(**G**, y) such that:

a) PA proves: ∃y PRF(**G**, y).

b) PA proves ¬PRF(**G**, **k**) for each particular natural number k (since none of these k-s is Gödel number of a PA-proof of G).

To clean up, if PA is consistent, and PA proves ¬G, then there is a formula C(y) such that:

a) PA proves: ∃yC(y),

b) For each k, PA proves: ¬C(**k**).

This is not a "direct" contradiction. To obtain a "direct" contradiction we should prove ∀y¬C(y). But what we have is a *separate* proof of ¬C(**k**) for each particular value of k. Are you able to replace this infinite sequence of separate PA-proofs by a **single (finite!)** PA-proof of ∀y¬C(y)? I am not. And Gödel was not, too. He was forced to introduce the notion of **ω-inconsistency** (weak inconsistency, or omega-inconsistency) to designate the above unpleasant situation.

Exercise 5.5. Show that if PA is inconsistent, then it is also ω-inconsistent.

Therefore, in the second part of our investigation (assuming that PA can prove ¬G), we were able to establish only the ω-inconsistency of PA.

Nevertheless, we have proved the famous

Gödel's Incompleteness Theorem (for PA). One can build a closed PA-formula G such that:

a) If PA proves G, then PA is inconsistent.

b) If PA proves ¬G, then PA is ω-inconsistent.

Why is this theorem considered as one of the most revolutionary results in mathematical logic?

Let F be a closed formula of some formal theory T. If neither F, nor ¬F can be proved by using the axioms of T, then F is called **undecidable** in T (or T-undecidable). I.e. F predicts some "absolutely definite" property of the "objects" of T, yet this prediction can be neither proved by means of T, nor refuted by means of T. A theory containing undecidable formulas is called an **incomplete theory**. Hence the term "incompleteness theorem": if PA is ω-consistent, then PA is incomplete.

Do not think, however, that we have **proved** the incompleteness of PA. We can prove the undecidability of Gödel's formula G only after we have proved that PA is ω-consistent. Until this, we have proved only that PA **is not perfect**: PA is either ω-inconsistent, or incomplete. I.e., when developing PA, we will run inevitably either into a ω-contradiction, or into a natural number problem that cannot be solved by using the axioms of PA. (One of such problems might be

expressed by the Gödel's formula G. It only seems that G is busy with its own provability, actually, as a closed PA-formula, G asserts some property of natural numbers!)

In Carnap's minutes for a January 15, 1931 discussion at Schlick's circle: "Gödel stellt dem gegenüber fest, das die von ihm angegebene unentscheidbare Formel wirklich konstruierbar ist. Ihr Inhalt ist finit wie der des Goldbachschen oder Fermatschen Satzes." – "...its contents is finitary just like that of Goldbach's or Fermat's conjectures"), quoted after Mancosu [1999]).

If our axioms are not perfect, we can try to **improve them**. Perhaps, we have missed some essential axioms? Let us add these missing axioms to PA, and we will obtain... a perfect theory?

Unfortunately, this is impossible. Even if, by extending the axioms too radically, we will not run into contradictions. Because, **Gödel's proof remains valid for any extensions of PA**. An extension of PA is nevertheless some formal theory T (in the language of PA). I.e. by definition, the predicate

$$prf_T(x, y) = \text{"y is a T-proof-number of the formula number x"}$$

must be computable (a theory is called formal, if and only if we have a "mechanical" procedure for checking the proof correctness in this theory). Hence, we can build a formula $PRF_T(x, y)$ expressing this predicate in PA. Let us apply, again, the Self-Reference Lemma, and we will have a closed formula G_T such that

$$\text{PA proves: } G_T \leftrightarrow \neg\exists y PRF_T(\mathbf{G_T}, y),$$

i.e. G_T "asserts" its own unprovability in T.

Exercise 5.6. Prove that if T is an extension of PA (i.e. if T can prove all theorems of PA), then:

a) If T proves G_T, then T is inconsistent.

b) If T proves $\neg G_T$, then T is ω-inconsistent.

Therefore, Gödel's method allows to prove that a **perfect axiom system of natural number arithmetic is impossible: any such system is either ω-inconsistent, or it is insufficient for solving some natural number problems.**

From the History

A chronology of some facts about this turning point in the human intellectual history:

1930

	August					September					October				November			
Mo	28	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	**17**	24
Tu	29	5	12	19	**26**	2	9	16	23	30	7	14	21	28	4	11	18	25
We	30	6	13	20	27	**3**	10	17	24	1	8	15	22	29	5	12	19	26
Th	31	7	14	21	28	4	11	18	25	2	9	16	**23**	30	6	13	20	27
Fr	1	8	15	22	**29**	5	12	19	26	3	10	17	24	31	7	14	21	28
Sa	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29
Su	3	10	17	24	31	**7**	14	21	28	5	12	19	26	2	9	16	23	30

April 28, 1906	Gödel, Kurt born
1928	March 10 and 14, 1928: “[Brouwer delivers – K. P.] two lectures in Vienna. Gödel is in the audience, as is Wittgenstein. It is said that the first lecture made Wittgenstein return to philosophy. Brouwer spends a day with Wittgenstein.” See: Mark van Atten. Luitzen Egbertus Jan Brouwer, *Stanford Encyclopedia of Philosophy*, 2011. D. Hilbert, W. Ackermann. Grundzüge der theoretischen Logik, *Berlin: Springer*, 1928. D. Hilbert. “Probleme der Grundlegung der Mathematik”. Lecture given at the International Congress of Mathematicians, Bologna, 3 September 1928. Published in: *Mathematische Annalen*, 1929, 102: 1-9. “Apparently Gödel started to concentrate on mathematical logic in the autumn of 1928, when he also began to attend Rudolf Carnap's lectures on “the philsophical foundations of arithmetic”... In the autumn of 1928 his library requests are mostly for works in logic; ...” (Hao Wang [1996], pp. 70-71.)
1929	“Early in 1929 he obtained and studied the newly published *Grundzüge der theoretischen Logik* (1928) by Hilbert and W. Ackermann, in which the completeness of predicate logic was formulated and presented as an open problem.” (Hao Wang [1996], p. 72.) “Shortly after I had read Hilbert-Ackermann, I found the proof [of

	the completeness of predicate logic." (From Gödel's late reminiscencies, reported in Hao Wang [1996], p. 82.) He presented the proof in his 1929 doctoral dissertation "Über die Vollständigkeit des Logikkalküls". Was Gödel thinking about the possibility of the incompleteness phenomenon already at that time? One can read in the Introduction of the dissertation: "Nun ist aber ein Beweis der Unlösbarkeit eines Problems durchaus nicht von vorneherein auszuschließen, wenn man bedenkt, daß es sich dabei nur um Unlösbarkeit mit gevissen *genau anzugebenden formalen* Schlußweisen handelt." "We cannot at all exclude out of hand, however, a proof of the unsolvability of a problem if we observe that what is at issue here is only unsolvability by certain *precisely stated formal* means of inference." Quoted after pp. 62-63 of: K. Gödel. Collected Works. Volume I. Publications 1929-1936. *Oxford University Press*, 1986, 881 pp.
July 6, 1929	Gödel's doctoral dissertation approved by his supevisors Hans Hahn and Philipp Furtwängler. (Dawson [1997])
October 22, 1929	A revised version of Gödel's dissertation received at "Monatshefte für Mathematik und Physik" (published in 1930).(Dawson [1997])
February 6, 1930	Doctor's degree granted to Gödel at the University of Vienna.
Summer, 1930	Gödel arrived at the Incompleteness Theorem. "In summer 1930 I began to study the consistency problem of classical analysis... By an enumeration of symbols, sentences and proofs of the given system, I quickly discovered that the concept of arithmetic truth cannot be defined in arithmetic... I reached the conclusion that in any reasonable formal system in which provability in it can be expressed as a property of certain sentences, there must be propositions which are undecidable in it." (From Gödel's late reminiscencies, reported in Hao Wang [1996], pp. 82-83.)
Tuesday, August 26, 1930	[According to Carnap's diary], "...Carnap was probably the first one to learn about the [Gödel's] results on August 26, 1930 during a conversation at the Cafe Reichsrat in Vienna [Austria]. Feigl was apparently also there and Waismann joined the the group later that afternoon." (from Mancosu [1999]).
August 29	A second discussion at the *Cafe Reichrat*. (Dawson [1997]). Trying to find the August 1930 meeting place in Vienna: *Cafe Reichrat* in 2008: see Gödel's Viennese Hangouts -- Cafes

	Arkaden, Josephinum and Reichsrat by Paul Raymont. K. Podnieks. Visiting Gödel: Vienna, September 2010, Searching for *Cafe Reichsrat.*
September 3	Vienna, *Stettiner Bahnhof*: Carnap, Feigl, Gödel and Waismann start their travel to Königsberg (Dawson [1997]).
Saturday, September 6, 3 – 3:20 pm (Dawson [1997])	Gödel's talk about Completeness Theorem at the Conference on Epistemology of the Exact Sciences (Königsberg, Germany). At the end of it, Gödel planned (?) to announce his incompleteness result. In the preparatory notes of the presentation it is formulated as follows: "... wie ich ihn in letzter Zeit bewiesen habe, ... es gibt mathematische Probleme, die sich in den *Principia mathematica* zwar ausdrücken aber mit den logischen Hilfsmitteln der *Principia mathematica* nicht lösen lassen." "... as I have recently proved; ..., there are mathematical problems which, though they can be expressed in *Principia Mathematica*, cannot be solved by the logical devices of *Principia Mathematica*." Quoted after pp. 27-28 of: K. Gödel. Collected Works. Volume III. Unpublished Essays and Lectures. *Oxford University Press*, 1995, 560 pp.
Sunday, September 7	"... on Sunday the meeting concluded with a round table discussion of the first day's addresses. During the latter event, without warning and almost offhandedly, Gödel quietly announced that "one can even give examples of propositions (and in fact of those of the type of Goldbach or Fermat) that, while contentually true, are unprovable in the formal system of classical mathematics..." (Dawson [1997], p. 69)" "Only von Neumann immediately grasped their [Gödel's remarks – K.P.] significance..." (G.J.Chaitin's lecture, Buenos Aires, 1998). "I had a private talk with von Neumann, who called it a most interesting result and was enthusiastic." (From Gödel's late reminiscencies, reported in Hao Wang [1996], p. 83.)
Monday, September 8	*Wir müssen wissen -- wir werden wissen!* David Hilbert's Radio Broadcast in Königsberg. See audio record published by James T.Smith, and translations in 7 languages published by Laurent Siebenmann. "...according to Gödel's biographer John Dawson, Hilbert and Gödel never discussed it, they never spoke to each other. The story is so dramatic that it resembles fiction. ... On September 7th Gödel off-handedly announced his epic results during a round-table discussion. Only von Neumann immediately grasped their significance... *The very next day,* September 8th, Hilbert delivered his famous lecture

	on ``Logic and the understanding of nature." As is touchingly described by Hilbert's biographer Constance Reid, this was the grand finale of Hilbert's career and his last major public appearance. Hilbert's lecture ended with his famous words: ``*Wir müssen wissen. Wir werden wissen.*" We must know! We shall know!" (from a G.J.Chaitin's lecture, Buenos Aires, 1998).
September	Gödel and von Neumann arrived at Gödel's Second Incompleteness Theorem (about unprovability of consistency). (Dawson [1997]) "Shortly after the Königsberg meeting, I discovered the improved undecidable proposition and the second theorem [about consistency proofs]. Then I received a letter from von Neumann noting independently the indemonstrability of consistency as a consequence of my first theorem." (From Gödel's late reminiscencies, reported in Hao Wang [1996], p. 84.)
October 23, 1930	Gödel's Abstract presented by Hans Hahn at a section meeting of the Vienna Academy of Sciences (see "Akademie der Wissenschaften in Wien, Mathematisch-Naturwissenschaftliche Klasse, Anzeiger", 1930, N 76, pp.214-215).
November 17, 1930	Gödel's famous paper received at "Monatshefte für Mathematik und Physik" (published in 1931).

K. Gödel [1931]. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme. "Monatshefte für Mathematik und Physik", 1931, Vol. 38, pp. 173-198.

See also English translations in Davis [1965] or Heijenoort [1967], online comments by Stanley Burris.

"Historians and Mathematicians agree, 1930 was Gödel's most profound year – if one was to include the latter part of 1929 as well. It is in this year that Gödel states he first heard of Hilbert's proposed outline of a proof of the continuum hypotheses. In the summer, Gödel began work on trying to prove the relative consistency of analysis. Gödel soon discovered that truth in number theory is undefinable – he later went on to prove a combinational form of the Incompleteness Theorem.

In 1930, Gödel traveled several days to attend the Second Conference on Epistemology of the Exact Sciences (September 5-7). Towards the end of the Conference on the last day, Gödel spoke for the first time and, "criticized the formalist assumption that consistency of 'transfinite' axioms assures the nonderivability of any consequence that is 'contentually false.' He concluded, 'For of no formal system can one affirm with certainty that all contentual considerations are representable in it.' And then v. Neumann interjected, 'It is not a foregone conclusion whether all rules of inference that are intuitionistically permissible may be formally reproduced.'" It was after this statement, that Gödel made the announcement of his incompleteness result, "Under the assumption of the consistency of classical mathematics, one can give examples of propositions…that are contentually true, but are unprovable in the formal system of classical mathematics." It was these events which preceded the formal 1931 publishing of Gödel's article *Über formal unentscheidbare Sätze der Principia Mathematica*

*und verwandter Systeme." (*A fragment from Gödel, and his Incompleteness Theorem by Mark Wakim).

About this event, see also

Paolo Mancosu. Between Vienna and Berlin: The Immediate Reception of Gödel's Incompleteness Theorems. History and Philosophy of Logic, 1999, Vol.20, N1, pp.33-45 (available online from Taylor & Francis Group).

Since 1940 Gödel lived in the U.S. See:

John W. Dawson Jr. Max Dehn, Kurt Gödel, and the Trans-Siberian Escape Route. *Notices of the AMS*, 2002, Vol.49, N9, pp1068-1075 (available online at

http://www.ams.org/notices/200209/fea-dawson.pdf and

http://www.mat.univie.ac.at/~oemg/IMN/imn189.pdf).

Gödel's 1942 summer vacations in Blue Hill, Maine: "...Throughout the summer Louise Frederick received agitated telephone calls from people of the town. Who was this scowling man with a thick German accent walking alone at night along the shore? Many thought Gödel was a German spy, trying to signal ships and submarines in the bay..." (**Peter Suber**, "Kurt Gödel in Blue Hill").

Gödel died on January 14, 1978.

For a complete biography see

John W. Dawson Jr. Logical Dilemmas. The Life and Work of Kurt Gödel. A. K. Peters, 1997.

See also:

Hao Wang. A Logical Journey: From Gödel to Philosophy. MIT Press, 1996, 391 pp.

Kurt Gödel Papers at Princeton University Library.

Photo gallery by BVI.

Exhibition photos from Gödel Centenary 2006. An International Symposium Celebrating the 100th Birthday of Kurt Gödel.

Emil Leon Post "... in the 1920s ...proved results similar to those which Gödel, Church and Turing discovered later, but he did not publish them. He reason he did not publish was because he felt that a 'complete analysis' was necessary to gain acceptance... In a postcard written to Gödel in 1938, just after they had met for the first time, Post wrote: *... As for any claims I might make perhaps the best I can say is that I would have proved Gödel's Theorem in 1921 – had I been Gödel.*" (according to MacTutor History of Mathematics archive).

C. Reid. Hilbert. *Springer-Verlag*, 1996 (Russian translation available)

Rosser's Version

In 1936 John Barkley Rosser (1907-1989) improved Gödel's proof. He removed the notion of ω-consistency from the formulation, replacing it by the (usual) consistency:

J. B. Rosser. Extensions of some theorems of Gödel and Church. "Journ. Symb. Logic", 1936, vol.1, N1, pp.87-91 (received September 8, 1936)

Incompleteness Theorem (for extensions of PA, Rosser's version). If T is an extension of PA (i.e. if T can prove all theorems of PA), then one can build a closed PA-formula R_T (i.e. a formula asserting some property of natural numbers) such that if T proves R_T or T proves $\neg R_T$, then T is inconsistent.

Proof. Immediately – from the extended version below.

Until now, all our versions of incompleteness theorems were bound to the specific language of PA. One could suspect, therefore, that the incompleteness phenomenon could be caused by an improper choice of the language and/or the logical system (axioms and rules of inference). Still, as will be established below, **the incompleteness theorem can be proved for any fundamental formal theories – based on arbitrary languages and/or logical systems (first order, second order, or any other).**

Recall (Section 3.2), that a formal theory T is called a **fundamental formal theory**, if and only if there is a translation algorithm Tr from PA into T such that, for all closed PA-formulas F, G:

Fu_1) If PA proves F, then T proves Tr(F).

Fu_2) T proves Tr(¬F), if and only if T proves ¬Tr(F).

Fu_3) If T proves Tr(F), and T proves Tr(F→G), then T proves Tr(G).

Note. We will not need the condition Fu_3 in the proof below.

Gödel's Incompleteness Theorem (extended version). If T is a fundamental formal theory (only conditions Fu_1, Fu_2 are necessary), then one can build a closed PA-formula R_T (i.e. a formula asserting some property of natural numbers) such that if T proves $Tr(R_T)$ or T proves $\neg Tr(R_T)$, then T is inconsistent.

Proof. Rosser's key idea was as follows. Gödel's formula G_T asserts "I cannot be proved in T". Let us consider, instead, a formula R_T asserting "I can be **easier** refuted than proved in T". Which kind of "proof complexity measure" could be used here?

We know from the Exercise 3.6 that any particular fundamental formal theory T can prove only a computably enumerable set of closed PA-formulas. So, let us construct a Turing machine, which enumerates all these formulas:

$$F_0, F_1, F_2, F_3, \ldots \qquad (1)$$

Thus, for all k, T proves $Tr(F_k)$. The following predicate is computable:

$prf_T(x, t)$ – "the formula number x appears in (1) as F_t".

Let the formula $PRF_T(x, y)$ express this predicate in PA. The following predicate is computable, too (ref – *refute*):

$ref_T(x, t)$ – "the **negation** of the formula number x appears in (1) as F_t".

Let the formula $REF_T(x, y)$ express this predicate in PA.

Now, let us follow the above-mentioned Rosser's key idea the formula R_T asserting "I can be easier refuted than proved in T". If, for a formula, the "proof complexity measure" would be defined its position number in (1), then Rosser's formula could be obtained from Self Reference Lemma by taking the following formula as C(x):

$$\forall t\,(PRF_T(x,t) \rightarrow \exists z\,(z < t \wedge REF_T(x,z)))\quad .$$

Thus, there is a PA-formula R_T such that

$$\text{PA proves:}\quad R_T \leftrightarrow \forall t\,(PRF_T(\boldsymbol{R_T},t) \rightarrow \exists z\,(z < t \wedge REF_T(\boldsymbol{R_T},z)))\quad . \qquad (2)$$

Indeed, R_T is asserting: "If my proof appears in (1) at the position t, then my refutation appears **before** t".

1. Now, assume that T proves $Tr(R_T)$. Then R_T appears in (1) as, for example, F_k. Hence,

$$\text{PA proves:}\quad PRF_T(\boldsymbol{R_T},\boldsymbol{k})\quad . \qquad (3)$$

If we take t=k in (2), then:

$$\text{PA proves:}\quad R_T \rightarrow (PRF_T(\boldsymbol{R_T},\boldsymbol{k}) \rightarrow \exists z\,(z < \boldsymbol{k} \wedge REF_T(\boldsymbol{R_T},z)))\quad ,$$

and

$$\text{PA proves:}\quad R_T \rightarrow \exists z\,(z < \boldsymbol{k} \wedge REF_T(\boldsymbol{R_T},z))\quad . \qquad (4)$$

If, indeed, $\neg R_T$ appears in (1) as F_m with m<k, then T proves $Tr(\neg R_T)$, and, by Fu_2-right, T proves $\neg Tr(R_T)$, i.e. T is inconsistent. Otherwise,

$$\text{PA proves:}\quad \neg REF_T(\boldsymbol{R_T},\boldsymbol{0}) \wedge \neg REF_T(\boldsymbol{R_T},\boldsymbol{1}) \wedge \ldots \wedge \neg REF_T(\boldsymbol{R_T},\boldsymbol{k-1})\quad .$$

Hence,

$$\text{PA proves:}\quad \forall z\,(z < \boldsymbol{k} \rightarrow \neg REF_T(\boldsymbol{R_T},z))\quad ,$$

and

$$\text{PA proves:} \quad \neg\exists z\left(z<\boldsymbol{k}\wedge REF_T\left(\boldsymbol{R_T},z\right)\right) \quad ,$$

and, by (4), PA proves $\neg R_T$. Then, by Fu_1, T proves $Tr(\neg R_T)$ and by Fu_2-right, T proves $\neg Tr(R_T)$, i.e. T is inconsistent. Q.E.D.

2. Assume now that T proves $\neg Tr(R_T)$, i.e., by Fu_2-left, T proves $Tr(\neg R_T)$. Then $\neg R_T$ appears in (1) as, for example, F_k. Hence,

$$\text{PA proves:} \quad REF_T\left(\boldsymbol{R_T},\boldsymbol{k}\right) \quad ,$$

and

$$\text{PA proves:} \quad \forall t\left(t>\boldsymbol{k}\rightarrow\exists z\left(z<t\wedge REF_T\left(\boldsymbol{R_T},z\right)\right)\right) \qquad (5)$$

(if t>k, we can simply take z=k).

If R_T appears in (1) before $\neg R_T$, then T proves $Tr(R_T)$, and T is inconsistent. If R_T does not appear before $\neg R_T$, then

$$\text{PA proves:}$$
$$\neg PRF_T\left(\boldsymbol{R_T},\boldsymbol{0}\right)\wedge\neg PRF_T\left(\boldsymbol{R_T},\boldsymbol{1}\right)\wedge\ldots\wedge\neg PRF_T\left(\boldsymbol{R_T},\boldsymbol{k-1}\right)\wedge\neg PRF_T\left(\boldsymbol{R_T},\boldsymbol{k}\right)$$

Hence,

$$\text{PA proves:} \quad \forall t\left(t\leq\boldsymbol{k}\rightarrow\neg PRF_T\left(\boldsymbol{R_T},t\right)\right) \quad .$$

Together with (5) this means that

$$\text{PA proves:} \quad \forall t\left(\neg PRF_T\left(\boldsymbol{R_T},t\right)\vee\exists z\left(z<t\wedge REF_T\left(\boldsymbol{R_T},z\right)\right)\right) \quad ,$$

i.e.

$$\text{PA proves:} \quad \forall t\left(PRF_T\left(\boldsymbol{R_T},t\right)\rightarrow\exists z\left(z<t\wedge REF_T\left(\boldsymbol{R_T},z\right)\right)\right) \quad .$$

According to (2), this means that PA proves R_T, and, by Fu_1, T proves $Tr(R_T)$, i.e. T is inconsistent. Q.E.D.

End of proof.

Now we can state the strongest possible form of the Gödel's "imperfectness principle": **a fundamental theory cannot be perfect – either it is inconsistent, or it is insufficient for solving some of the problems in the domain of its competence.**

The fundamentality (the possibility to prove the principal properties of natural numbers) is essential here, because some non-fundamental theories **may** be sufficient for solving all of their problems. As a non-trivial example of non-fundamental theories can serve **Presburger arithmetic** (PA minus multiplication, see Section 3.1). In 1929 M. Presburger proved that this theory is both consistent and complete. After Gödel and Rosser, this means now that

Presburger proved that his arithmetic is not a fundamental theory.

Non-standard Arithmetic

We know that if PA is consistent, then the formula G cannot be proved in PA, hence, the theory PA+{¬G} is consistent, too. Since

PA proves: ¬G ↔ ∃yPRF(**G**, y),

the theory PA+{ ∃yPRF(**G**, y) } is also consistent. On the other hand, since G cannot be proved in PA, for each natural number k:

PA proves: ¬PRF(**G**, **k**).

Let us denote PRF(**G**, y) by C(y). Hence, if PA is consistent, then there is a formula C(y) such that PA+{ ∃yC(y) } is a consistent theory, yet for each natural number k: PA proves ¬C(**k**). Imagine, you wish to investigate the theory PA+{ ∃yC(y) }- why not? It is "as consistent" as PA (and, at the same time, ω-inconsistent!). In this theory the axiom ∃yC(y) says that there is a number y that does possess the property C. On the other hand, for each "standard" natural number k we can prove ¬C(**k**), i.e. that k does not possess the property C. Hence, when working in the theory PA+{ ∃yC(y) }, we are forced to admit the existence of **non-standard natural numbers**.

Exercise 5.7 (for smart students). Prove in PA+{ ∃yC(y) } that there is some minimum number w_0 having the property C. On the other hand, consider a model of PA+{ ∃yC(y) }. Define standard numbers as interpretations of numerals 0, 1, 2, etc. Verify that: a) each standard number is less than any non-standard number, b) there is no **minimum** non-standard number, c) standard numbers cannot be defined by a formula in the language of PA.

Read more: Non-standard arithmetic in Wikipedia.

Exercise 5.8. (inspired by the paper Mostowski [1961]) Return to the paradoxes stated by Albert of Saxony (Section 5.1). Which kind of incompleteness theorems could you derive by modeling these paradoxes in PA? You may find helpful the result of the Exercise 5.4. (Hint: Mostowski defines two closed formulas F, H as T-independent, if and only if none of the following conjunctions can be proved in T: F&H, F&¬H, ¬F&H, ¬F&¬H. Assume, T is ω-consistent, and use the first Albert's paradox to build two T-independent formulas. Could you provide the "Rosserian" version of your proof?)

Exercise 5.8A (for smart students). Which kind of (incompleteness?) theorems could you derive by modeling Curry's paradox?

5.4. Gödel's Second Incompleteness Theorem

Pure mathematical contents of incompleteness theorems (without any attempt of "interpretation") are as follows: there are two algorithms due to Gödel and Rosser.

Algorithm 1. Given the axioms of a fundamental formal theory T this algorithm produces a closed PA-formula R_T. As a closed PA-formula, R_T asserts some property of the natural number system.

Algorithm 2. Given a T-proof of the formula $Tr(R_T)$, or, of the formula $\neg Tr(R_T)$, this algorithm produces a T-proof of a contradiction.

Therefore, if T is a fundamental theory, then either T is inconsistent, or it can neither to prove, nor to refute the hypothesis R_T. A theory that is able neither to prove, nor to refute some closed formula in its language, is called **incomplete**. Hence, Gödel and Rosser have proved that **each fundamental theory is either inconsistent, or incomplete**.

Why is this theorem called **incompleteness** theorem? The two algorithms developed by Gödel and Rosser do not allow deciding whether T is inconsistent or incomplete (verify). Hence, to prove "via Gödel" the incompleteness of some theory T, we must **prove that T is consistent**. Still, as we already know (Section 1.5), in a reliable consistency proof we should not use questionable means of reasoning. The aim of Hilbert's program was to prove consistency of the entire mathematics by means as reliable as the ones contained in first order arithmetic (i.e. PA). Hence, to prove the consistency of PA we must use... PA itself?

Let us formalize the problem. In the previous section, having a fundamental formal theory T we considered some enumeration of all PA-formulas (translations of) which can be proved in T:

$$F_0, F_1, F_2, F_3, \ldots \qquad (1)$$

From a Turing machine program generating (1) we derived a PA-formula $PRF_T(x, y)$ expressing in PA the predicate

$$prf_T(x, y) = \text{"the formula number x appears in (1) as } F_y\text{"}.$$

Then the formula $\exists y PRF_T(x, y)$ asserts, that the formula number x is provable in T. If T is inconsistent, then in T all formulas are provable, i.e. 0=1 is also

provable. And conversely, if we have proved that in T some formula (for example, 0=1) cannot be proved, then we have proved that T is consistent. Hence, the formula $\neg\exists y PRF_T(\mathbf{0=1}, y)$ asserts, in a sense, that T is a consistent theory. Let us denote this formula by Con(T).

Unexpectedly, the properties of Con(T) depend on the choice of the formula $PRF_T(x, y)$. (I got to know about the experiment described below from the Appendix 1 written by A. S. Yessenin-Volpin for the 1957 Russian translation of Kleene [1952], see p.473 of the translation, see also p.37 of Feferman [1960]).

Having the formula $PRF_T(x, y)$ let us introduce another formula $PRF'_T(x, y)$:

$$PRF_T(x, y) \wedge \neg PRF_T(\mathbf{0=1}, y) \quad .$$

If T is consistent, then 0=1 cannot be proved in T, hence, for all k:

$$\text{PA proves: } \neg PRF_T(\mathbf{0=1}, \mathbf{k}).$$

And hence, $PRF'_T(x, y)$ – like as $PRF_T(x, y)$ – expresses in PA the predicate $prf_T(x, y)$. Now let us build the corresponding formula Con'(T) as $\neg\exists y PRF'_T(\mathbf{0=1}, y)$, or:

$$\neg\exists y \left(PRF_T(\mathbf{0=1}, y) \wedge \neg PRF_T(\mathbf{0=1}, y) \right) \quad .$$

This formula Con'(T) can be proved (almost) in the propositional calculus! Does it mean that the propositional calculus can prove the consistency of an arbitrary formal theory T? Yes, and even the consistency of inconsistent theories! Then, where is the trick? The trick is: we assumed that T is consistent **before** we started our "consistency proof". Only this assumption allows to prove that $PRF'_T(x, y)$ expresses only one predicate – $prf_T(x, y)$, and hence – that Con'(T) asserts the consistency of T. If we assume the consistency of T from the very beginning, then we can easily "prove" Con'(T) (an equivalent of our assumption!) by using the most elementary logical rules.

However, the lesson of this experiment is very useful. If we intend to discuss the means that are able (or not) to prove the formula Con(T), then we must **check carefully the means that were used to establish that Con(T) asserts consistency of theory T**.

If Con(T) is built in a "natural" way, i.e. by using a formula $PRF_T(x,y)$ obtained by direct modeling of an appropriate Turing machine program, then the "watched means" do not exceed PA. It would be hard to demonstrate this here directly, yet it is not surprising. Indeed, when proving the Representation

Theorem in Section 3.3, we used only elementary logical and arithmetical means of reasoning.

Now, what means of reasoning are necessary to prove the "natural" formula Con(T) – if theory T is "really" consistent? Let us assume we were successful to prove Con(T) in some way. What kind of consequences could be drawn from this proof? The most powerful means to draw consequences from the consistency proof of some theory would be, perhaps, ... the incompleteness theorem! Gödel's theorem says:

"If T is consistent, then the formula G_T cannot be proved in T".

And G_T says exactly that it cannot be proved in T. Hence, "if Con(T), then G_T". Or, formally:

$$\text{Con(T)} \rightarrow G_T.$$

This is the **formal equivalent of Gödel's incompleteness theorem** (the first part of it). What means of reasoning were used to prove this theorem? Return to the previous section, and you will see that there only (a fantastic combination of) elementary logical and arithmetical means were used. Hence, we can conclude that

$$\text{PA proves: Con(T)} \rightarrow G_T. \qquad (2)$$

It would be hard to prove this here 100% directly, yet it is not surprising – as we know, the axioms of PA cover 100% of elementary logical and arithmetical means of reasoning.

Now, imagine that you were successful in proving Con(T) according to the standards of Hilbert's program, i.e. by using only the means formalized in PA, i.e.

$$\text{PA proves: Con(T).}$$

Add (2) to this, and you will have: PA proves G_T. If T is a fundamental theory, then T proves all theorems of PA, and hence, T also proves G_T. From Gödel's incompleteness theorem we know that, if T proves G_T, then T is inconsistent. Therefore, **if PA proves Con(T), then T is inconsistent!** And, if PA proves Con(PA), then PA is inconsistent!

Kurt Gödel first formulated this conclusion in the same famous 1931 paper, and it is now called **Gödel's Second Incompleteness Theorem**.

Gödel's Second Incompleteness Theorem shows that Hilbert's program cannot

be 100% successful. Let us recall the two stages of this program:

a) Build a formal theory T covering the entire mathematics.

b) Using PA, prove the consistency of T (consistency seems to be simply a "pure combinatorial property" of formal axioms, see Section 1.5).

The first stage was accomplished when the modern axiomatic set theories (such as ZFC) were formulated. Still, the difficulties in advancing the "combinatorial" second stage appeared to be principal ones: using PA, it is impossible to prove even the consistency of PA itself!

Let us recall also the warning by Henri Poincare – his reaction to the first attempts of Russell and Hilbert to initiate rebuilding of the foundations of mathematics (see Poincare [1908], Volume II, Chapter IV, my own re-formulation):

Do not try justifying the induction principle by means of the induction principle. This would mean a kind of vicious circle!

The induction principle builds up 99% of PA, hence, do not try to prove the consistency of PA by means of PA! And Gödel's Second Incompleteness Theorem says: of course, you can try, yet if you will succeed, then you will prove that PA is inconsistent!

Hilbert's reaction to the failure of his program was quite different from that of Frege and Cantor. The following elegant and extremely general version of Gödel's Second Incompleteness Theorem results, in fact, from the analysis of Gödel's proof performed by Hilbert and Paul Bernays in Volume II, Chapter V of:

D. Hilbert, P. Bernays. Grundlagen der Mathematik. Vol. I, 1934, 471 pp. Vol. II, 1939, 498 pp., Berlin (Springer) (Russian translation available)

Recall (Section 3.2), that a formal theory T is called a **fundamental formal theory**, if and only if there is a translation algorithm Tr from PA into T such that, for all closed PA formulas F, G:

Fu_1) if PA proves F, then T proves Tr(F);

Fu_2) T proves Tr(¬F), if and only if T proves ¬Tr(F);

Fu_3) If T proves Tr(F), and T proves Tr(F→G), then T proves Tr(G).

Thus, fundamental formal theories may be based on arbitrary languages and/or logical systems (first order, second order, or any other).

Instead of the formula $PRF_T(x, y)$ expressing the predicate $prf_T(x, y)$, let us

concentrate on the formula $\exists y PRF_T(x, y)$. Let us denote it by $PR_T(x)$. This formula asserts: "T proves the formula number x", or more precisely, "T proves the T-translation of the PA-formula number x".

Now, let us forget about the origin of $PR_T(x)$ – for the rest of this Section, $PR_T(x)$ can be any PA-formula having exactly one free variable x.

As Gödel's formula G_T we can use any formula having the following property (such formulas do exist by the Self-Reference Lemma):

$$\text{PA proves: } G_T \leftrightarrow \neg PR_T(\mathbf{G_T}).$$

Let us define the formula Con(T) as $\neg PR_T(\mathbf{0=1})$.

Let us say that theory T "is aware", that the formula Con(T) asserts the consistency of T, if and only if the following three **Hilbert-Bernays-Löb derivability conditions** hold for each pair of closed PA-formulas B, C:

H_1: If T proves Tr(B), then T proves $Tr(PR_T(\mathbf{B}))$.

H_2: T proves: $Tr[PR_T(\mathbf{B})) \rightarrow PR_T(\mathbf{PR_T(B)})]$.

H_3: T proves: $Tr[PR_T(\mathbf{B}) \rightarrow (PR_T(\mathbf{B \rightarrow C}) \rightarrow PR_T(\mathbf{C}))]$.

Conditions H_1 and H_2 say that T "is aware" that the formula $PR_T(x)$ "expresses" the notion T-provability. The condition H_3 says that T "is aware" that the set of (arithmetical) theorems of T is closed under MODUS PONENS. Hence, if H_1, H_2, H_3 hold, we may, indeed, conclude that T "is aware", that Con(T) (i.e.$\neg PR_T(\mathbf{0=1})$) asserts the consistency of T.

Note. The first version of derivability conditions was introduced in Hilbert, Bernays [1934] (Volume II, Chapter V). The above more elegant version was proposed in 1955 by Martin Hugo Löb (1921-2006):

M. H. Löb. Solution of a problem of Leon Henkin. "J. Symbolic Logic", 1955, vol.20, pp. 115-118.

Gödel's Second Incompleteness Theorem (extended version). If a fundamental formal theory T "is aware" that the formula Con(T) asserts the consistency of T, then either T is inconsistent, or Tr(Con(T)) cannot be proved in T.

Lemma 1 (formalized part-one of the first incompleteness theorem). If a fundamental formal theory T "is aware" that the formula Con(T) asserts the

consistency of T, then T proves $Tr[PR_T(\mathbf{G_T})\rightarrow PR_T(\neg\mathbf{G_T})]$.

Lemma 2. If a fundamental formal theory T "is aware" that the formula Con(T) asserts the consistency of T, then T proves $Tr(Con(T) \rightarrow G_T)$.

Proof of Gödel's Theorem. By Lemma 2, T proves $Tr(Con(T) \rightarrow G_T)$. Let us assume that T proves Tr(Con(T)).

Then, by Fu_3, T proves $Tr(G_T)$, and, by H_1, T proves $Tr(PR_T(\mathbf{G_T}))$.

Since PA proves $PR_T(\mathbf{G_T})\rightarrow\neg G_T$, by Fu_1, T proves $Tr(PR_T(\mathbf{G_T})\rightarrow\neg G_T)$. Then, by Fu_3, T proves $Tr(\neg G_T)$, and, by Fu_2, T proves $\neg Tr(G_T)$, i.e. T is inconsistent. Q.E.D.

Proof of Lemma 1. Let us formalize in T the proof of the (part one of) Gödel's incompleteness theorem: if T proves $Tr(G_T)$, then T proves $Tr(\neg G_T)$.

Since PA proves $PR_T(\mathbf{G_T})\rightarrow\neg G_T$, by Fu_1, T proves $Tr(PR_T(\mathbf{G_T})\rightarrow\neg G_T)$. Then, by H_1, T proves $Tr(PR_T(\mathbf{PR_T(G_T)}\rightarrow\neg\mathbf{G_T}))$. By H_3,

T proves: $Tr[PR_T(\mathbf{PR_T(G_T)})\rightarrow(PR_T(\mathbf{PR_T(G_T)}\rightarrow\neg\mathbf{G_T})\rightarrow PR_T(\neg\mathbf{G_T})]$.

By H_2, T proves $Tr[PR_T(\mathbf{G_T})\rightarrow PR_T(\mathbf{PR_T(G_T)})]$.

Thus, we have the following situation. Let us denote $PR_T(\mathbf{G_T})$ – by A, $PR_T(\mathbf{PR_T(G_T)})$ – by B, $PR_T(\mathbf{PR_T(G_T)}\rightarrow\neg\mathbf{G_T})$ – by C, and $PR_T(\neg\mathbf{G_T})$ – by D. We know that:

T proves: Tr(C),
T proves: Tr(B→(C→D)),
T proves: Tr(A→B).

By Exercise 3.5a, Fu_1 and Fu_3 imply that then T proves Tr(A→D), i.e.

T proves: $Tr[PR_T(\mathbf{G_T})\rightarrow PR_T(\neg\mathbf{G_T})]$.

Q.E.D.

Proof of Lemma 2. We must verify that T proves $Tr(Con(T)\rightarrow G_T)$. We could derive this fact from

T proves: $Tr(PR_T(\mathbf{G_T})\rightarrow PR_T(\mathbf{0=1}))$. (3)

Indeed, by Exercise 3.5a, Fu_1 and Fu_3 imply that if T proves Tr(A→B), then T

proves Tr(¬B→¬A). Hence, from (3) we can derive that T proves Tr(¬PR_T(**0=1**)→¬PR_T($\mathbf{G_T}$)), i.e. T proves Tr(Con(T)→¬PR_T($\mathbf{G_T}$)).

Since PA proves ¬PR_T($\mathbf{G_T}$)→G_T, by Fu_1, T proves Tr(¬PR_T($\mathbf{G_T}$)→G_T). Hence, by Exercise 3.5a, Fu_1 and Fu_3 imply that T proves Tr(Con(T)→G_T).

So, let us prove (3). Since PA proves ¬G_T→(G_T→0=1), by Fu_1, T proves Tr(¬G_T→(G_T→0=1)). Then, by H_1, T proves Tr(PR_T(¬$\mathbf{G_T}$→($\mathbf{G_T}$→**0=1**))). By H_3,

T proves: Tr[PR_T(¬$\mathbf{G_T}$)→(PR_T(¬$\mathbf{G_T}$→($\mathbf{G_T}$→**0=1**))→PR_T($\mathbf{G_T}$→**0=1**))].

By Lemma 1, T proves Tr[PR_T($\mathbf{G_T}$)→PR_T(¬$\mathbf{G_T}$)].

Thus, we have the following situation. Let us denote PR_T($\mathbf{G_T}$) – by A, PR_T(¬$\mathbf{G_T}$) – by B, PR_T(¬$\mathbf{G_T}$→($\mathbf{G_T}$→**0=1**)) – by C, and PR_T($\mathbf{G_T}$→**0=1**) – by D. We know that:

T proves: Tr(C),
T proves: Tr(B→(C→D)),
T proves: Tr(A→B).

By Exercise 3.5a, Fu_1 and Fu_3 imply that then T proves Tr(A→D), i.e. T proves

Tr[PR_T($\mathbf{G_T}$)→PR_T($\mathbf{G_T}$→**0=1**)].

By H_3,

T proves: Tr[PR_T($\mathbf{G_T}$)→(PR_T($\mathbf{G_T}$→**0=1**)→PR_T(**0=1**))].

Thus, we have the following situation. Let us denote PR_T(**0=1**) by E. We know that:

T proves: Tr(A→D),
T proves: Tr(A→(D→E)).

By Exercise 3.5a, Fu_1 and Fu_3 imply that then T proves Tr(A→E), i.e. (3).
Q.E.D.

Let us return to the above "abnormal" formula Con'(T) that could be proved almost in the propositional calculus. If Hilbert-Bernays-Löb conditions were true for the corresponding formula PR'_T(x), then, according to Gödel's Second

Incompleteness Theorem, T would be an inconsistent theory. Hence, if T is consistent, then Hilbert-Bernays-Löb conditions do not hold for $PR'_T(x)$, and we can say that T "is not aware" that Con'(T) asserts its consistency. Proves Con'(T), but "is not aware" that this means proving of its own consistency!

On the other hand, it appears that Hilbert-Bernays-Löb conditions hold for all formulas Con(T) obtained in a "natural" way, i.e. by direct formal modeling of an appropriate Turing machine program. To prove this for a particular formula – it is not a hard work, but nevertheless, an extensive one. Accordingly, for these "natural" formulas Gödel's Second Incompleteness Theorem holds: any fundamental theory T is either inconsistent, or it cannot prove Con(T).

If, in order to justify the axioms of some theory the consistency proof is required, then we can say that a **fundamental theory cannot justify itself**.

Still, how about **non-fundamental theories**? Some of them are not able even to **formulate** their own consistency problem. Either their languages do not allow to write formulas like $PR_T(x)$ and Con(T), or their axioms do not allow to prove Hilbert-Bernays-Löb derivability conditions.

However, it appears that some "stronger" theories are able to prove consistency of some "weaker" theories. For example, in the set theory ZF you can prove consistency of first order arithmetic PA (the set ω appears to be a model where all the axioms of PA are true, see Appendix 1). If PA is consistent, then the formula Con(PA) cannot be proved in PA, yet its translation into the language of set theory can be proved in ZF.

On the other hand, as a closed PA-formula Con(PA) asserts some property of natural numbers. This property can be proved in ZF, but not in PA (if PA is consistent). Thus we have obtained a positive answer to question stated in the Section 3.2: yes, there are statements which involve only the notion of natural numbers (i.e. you can formulate them in the language of first order arithmetic), but which can be proved only by using more powerful concepts, for example, of set theory.

In other words: **the arithmetic contained in set theory is more powerful than first order arithmetic**. And, when Georg Cantor invented his set theory in 1873, **he extended also the human notion of natural numbers**. The arithmetical statement Con(PA) was unprovable before 1873, but it became provable by the end of that year. (If the statement of Con(PA) seems "artificial" to justify the above conclusion, see more striking examples in Section 6.5 and in Appendix 2.) And finally, would you be surprised, if the twin prime conjecture appeared to be provable in ZFC, but not in PA?

Note. For a complete analysis of mathematical problems from around the

incompleteness theorems – see Feferman [1960] and the chapter about incompleteness theorems written by Craig Smorynski in Barwise [1977].

About the version of incompleteness theorem proved by Gregory J.Chaitin see Section 6.8.

6. Around Gödel's Theorem

6.1. Methodological Consequences

From incompleteness theorems, some people derive the thesis about the superiority of the "alive, informal, creative, human thinking" over axiomatic theories. Or, about the impossibility to cover "all the treasures of the informal mathematics" by a stable set of axioms. I could agree with this, when the above-mentioned "superiority" would not be understood as the ability of the "informal thinking" to find unmistakably (i.e. on the first trial) some "true" assertions that cannot be proved in a given axiomatic theory. Some of the enthusiasts of this opinion are painting the following picture.

Let us consider any formal theory T that contains a full-fledged concept of natural numbers (i.e. – in my terms – T is a fundamental theory). Let us build for T Gödel's formula G_T asserting, "I am not provable in T". Gödel proved that, indeed, G_T cannot be proved in T, i.e. Gödel proved that G_T is a true formula (and – as a formula of PA – a true statement about properties of natural numbers). Therefore, if we choose an arbitrary formal theory T, then Kurt Gödel – by using his "informal, creative thinking" – proves immediately some assertion G_T about the properties of natural numbers, which cannot be proved in T. Hence, none of formal theories can express 100% of the "informal, human" notion of natural numbers. If you fix some particular formal theory, my "creative mind" will **unmistakably** find a true assertion G_T overcoming all what can be proved in T.

The analysis of Gödel's proof presented in Section 5.4 forces us to revise this picture. One can prove that G_T is a true formula (i.e. that G_T cannot be proved in T) only by **postulating the consistency** of T. Indeed, if G_T were proved to be true, then also the consistency of T were proved (G_T asserts its own unprovability, and the unprovability of at least one formula means the consistency of T). Hence, if we do not know, whether T is consistent or not, we can say nothing about the truth or falsity of G_T. What could think the enthusiasts of the above picture about the consistency problem?

First of all, they cannot think, that **any** formal theory is consistent. Just add to PA the formula 0=1 as an axiom, and you will obtain an example of an inconsistent theory. Of course, such artificial examples will not be taken

seriously. Still, the following fact has to be taken absolutely seriously: there is no algorithm that could detect, by exploring the axioms and rules of a formal theory, is this theory consistent or not.

Exercise 6.1. Let us assume that PA is consistent. Show (using the techniques of Section 6.3) that there is no algorithm detecting for any given closed formula F, whether the theory PA+F is consistent or not.

Hence, the consistency problem cannot be solved mechanically, by applying some uniform method to all theories. Serious theories are complicated enough to require **individual investigation** of this problem.

And finally, we must return to the history of those mathematical theories which were considered as "absolutely reliable" by their creators, but which were proved inconsistent some time later.

The first of these unhappy theories was the first serious formal system of mathematics developed by Gottlob Frege.

G. Frege. Die Grundlagen der Arithmetik. Eine logisch-mathematische Untersuchung über den Begriff der Zahl. 1884, Breslau, 119 pp.

G. Frege. Grundgesetze der Arithmetik, begriffsschriftlich abgeleitet. Jena, Vol. I, 1893, 254 pp., Vol. II, 1903, 265 pp. (see also online comments by Stanley Burris)

See also the online article Frege's Logic, Theorem, and Foundations for Arithmetic in Stanford Encyclopedia of Philosophy.

In 1902, when the second (final!) volume of Frege's book was ready to print, he received a letter from Bertrand Russell, who established that from Frege's principles a contradiction can be derived (about Russell's paradox see Section 2.2). Frege added Appendix II:

"Hardly anything more unfortunate can befall a scientific writer than to have one of the foundations of his edifice shaken after the work is finished. This was the position I was placed in by a letter of Mr. Bertrand Russell..." (quoted after Heijenoort [1967]).

Soon after this, Frege's wife died in 1904. Frege died in 1925, yet after 1903 he published nothing comparable with his outstanding works of the previous period. Russell's paradox was for him a dreadful blow because of the contrast between the 20 years long impression of absolute reliability of his formal system, and the suddenly following "absolutely trivial" inference of a contradiction. Frege could consider the situation as his personal failure. Was it really? Even today, reading Frege's book without prejudice, you have the impression of absolute reliability of his basic principles. Russell's paradox was not Frege's personal failure, it was failure of the entire old way of mathematical thinking.

Some years before Frege a similar unhappy situation appeared in another

excellent mathematical work of XIX century – in the set theory created by Georg Cantor. Read Cantor's works without prejudice, and you will get again the impression of absolute reliability (if you do not read in German, please, read once more Section 2.2). Cantor developed the principles of the old mathematical thinking up to their natural logical limits – to the concept of static infinite sets. Leider, in 1895 Cantor established himself that from his principles a contradiction can be derived.

Since the lifetime of Frege and Cantor, formal mathematical theories have been improved significantly. No contradictions have been found so far in the improved theories. Still, from the unhappy experience of these extraordinary people we must learn at least the following: our "feeling", our impression of absolute reliability of our premises, no matter how many and how distinguished people share this "feeling", cannot serve as an absolute warranty against contradictions.

Martin Davis: "I'm fond of noting that the list of logicians who have seriously proposed formal systems that turned out to be inconsistent reads like an honor roll: Frege, Church, Curry, Quine, Rosser."

(See FOM Archives, May 30, 2003, http://cs.nyu.edu/pipermail/fom/2003-May/006665.html).

Truth or falsity of the assertions proposed so far as "true statements" unprovable in a particular formal theory depends on the consistency of this theory. Hence, we cannot speak here about a general method that allows obtaining unmistakably "true statements" that overcome a given formal theory. What, if the theory T that we intend to overcome will be proved inconsistent? Then, Gödel's formula G_T will be false. And this must be called a "superior true statement"?

Perhaps, the best way to demonstrate the absurdity of the position I'm trying to criticize may be the following "syllogism":

a) To overcome "a la Gödel" some formal theory T, we must prove the formula G_T.

b) To prove the formula G_T, we must prove consistency of T.

c) To prove consistency of T, we must use postulates from outside of T (Gödel's second theorem).

Hence, to overcome "a la Gödel" some formal theory T, we must use postulates from outside of T. Is this absolutely trivial or not?

If we are not able to prove the consistency of our favorite theory, yet our feeling says that "this is the case", then we may try to adopt the consistency conjecture as an additional axiom, and try to draw consequences from this axiom. This approach is not completely novel for mathematics. For example,

in number theory the consequences of Riemann's hypothesis are studied etc. Note, however, that we are talking here about **hypotheses**. The consistency conjecture of our favorite theory is no more than a hypothesis, and adopting this hypothesis as an axiom is **postulating**, i.e. adoption without sufficient arguments. When drawing consequences from a hypothesis we may come to contradictions, and then we will be forced to reject it.

And once you postulate the consistency of your favorite theory T, then, to prove the truth of the formula G_T we need no more than the (formal!) axioms of PA! Indeed, as we know, PA proves $Con(T) \rightarrow G_T$, hence, after assuming of Con(T), the truth of G_T follows immediately and formally!

“The method of "postulating" what we want has many advantages; they are the same as the advantages of theft over honest toil.” (Bertrand Russell, Introduction to Mathematical Philosophy, 1919, quoted from http://en.wikiquote.org/wiki/Bertrand_Russell)

Our final conclusion may be formulated as follows: incompleteness theorems do not yield a general method allowing to overcome unmistakably (i.e. on the first trial) any given formal theory. It seems that such general methods do not exist at all: serious theories are too complicated, hence, to overcome a particular serious theory we must, perhaps, invent a particular method.

The true methodological significance of incompleteness theorems is completely different: **any fundamental theory is either inconsistent, or it is insufficient to solve some of the problems from its domain of competence.** We know already that the methods developed by Gödel and his followers do not allow deciding is a given theory inconsistent or incomplete. Hence, it would be more exactly to say not "incompleteness theorems", but rather "imperfectness theorems". A fundamental theory cannot be perfect – it is either inconsistent, or it is insufficient to solve some of its problems.

Imperfect theory must be and can be improved. Contradictions can be removed by improving axioms. The problems that were proved (or are suspected) to be undecidable – we can try to solve them by adopting additional powerful (maybe, unreliable!) axioms.

From a methodological point of view formal theories are models of **stable self-contained systems of reasoning**. Hence, we can reformulate our main conclusion as follows: any fundamental stable self-contained system of reasoning is either inconsistent or there are some problems that cannot be solved by using this (stable, self-contained!) system. **The crucial evidence of the inherent imperfectness of any stable self-contained system of reasoning – here is the true methodological significance of Gödel's results.** Mathematical theories cannot be perfect **because** they are stable and self-

contained! Only relatively weak (i.e. non-fundamental) theories can be both consistent and complete. Powerful (i.e. fundamental) theories inevitably are either inconsistent, or incomplete.

Note. Do not conclude from this that mathematics must turn to variable (i.e. unstable or non-self-contained) systems of reasoning – this would be no mathematics! Im mathematics, one is allowed to change the axioms only deliberately.

Note. In the so-called model theory (a branch of mathematical logic, see Appendix 1) theories are defined as arbitrary sets of formulas (sets of theorems). This is a very abstract point of view to be useful in discussions about the foundations of mathematics. A real theory should be defined as a sufficiently definite system of reasoning (and formal theories are models of absolutely definite, i.e. stable, self-contained systems of reasoning). The set of theorems is only a secondary aspect of a real theory: it is the set of assertions that can be proved by using the axioms and rules of theory. If theories are viewed as sets of theorems, then inconsistent theories seem to be "empty" (in these theories all formulas are provable, i.e. they do not make difference between true and false formulas). And, when we manage to remove inconsistencies by improving axioms of our theory, then have we "improved" ... an empty set of theorems? If theories are viewed as systems of reasoning, then inconsistent theories are simply some kind of imperfect systems that should be improved.

Added April 26, 2007

The above argument does not work for people believing in the **natural numbers as a structure that exists** (and is absolutely definite and unique) **independently of any axioms**. For these people, in this structure, the axioms of PA are "obviously true", and, hence, consistent. And hence, Con(PA) and Gödel's formula G_{PA} are "obviously true" arithmetical formulas, while unprovable from the axioms of PA. Of course, not only Con(PA) is a true formula in this structure, so is also Con(PA+Con(PA)) etc. And, in general, if the arithmetical theorems of some formal theory T are true in the natural number structure, then Con(T) is a true arithmetical formula that cannot be proved in T (Gödel's Second Theorem). Thus, for these people, the **natural number structure cannot be described by a fixed system of axioms.**

Some people extend this attitude by believing in the existence of an absolutely definite and unique "true world of sets", that satisfies all the axioms of ZFC set theory (i.e. the Axiom of Choice included). This extended attitude seems to be justified by the developments in the so-called theory of large cardinals. There is a "tower" consisting of about 30 kinds of large cardinal axioms, the next kind essentially stronger than the previous one. The top one of these axioms (postulating the existence of the so-called Reinhardt cardinals), is known to be inconsistent with ZFC. The remaining 29 kinds are believed to be "true" in the "true world of sets", and hence, consistent with ZFC.

However, see:

N. V. Belyakin. One $omega$-inconsistent formalization of set theory. *The 9th Asian Logic Conference*, 16-19 August, 2005, Novosibirsk, Russia (online abstract),

where the following is announced: "From this fact follows, in particular, that the **existence of** strongly inaccessible cardinals **is refutable in ZF**." Thus, contradictions appear already at the **second level** of the large cardinal tower?

Note. The English translation of the abstract contains an error: one should remove [in] from the statement "It is not hard to check that *T* is [in]consistent wrt *ZF*+(*existence of strongly inaccessible cardinals*)".

Will this development lead to the discovery of contradictions in PA? This could be the only kind of argument that could put an end to **all** kinds of platonism... Maybe, the final version of incompleteness theorems will state that **any formal theory proving the basic properties of natural numbers ... leads to contradictions**?

This could be a dead-strong version of my favorite (non-topological) "Poincare's conjecture". Henri Poincare noticed in his book "Science et methode" (Paris, 1908, see Volume II, Chapters III and IV) that (in modern terms) the idea of a "formal theory of natural numbers" is based on *petitio principii*. The abstract notion of formal syntax is based on the same induction principle that is formalized in the "formal theory of natural numbers"...

6.2. Double Incompleteness Theorem

Paul Levy discussed the possibility of the double incompleteness phenomenon in 1926:

P.Lévy. Sur le principe du tiers exclu et sur les théoremes non susceptibles de démonstration. "Revue de Métaphysique et de Morale", 1926, vol. 33, N2, pp. 253-258.

He proposed the following conjecture:

"... il est possible que le theoreme de Fermat soit indemontrable, mais on ne demontrera jamais qu'il est indemontrable. Au contraire, il n'est pas absurde d'imaginer qu'on demontre qu'on ne soura jamais si la constante d'Euler est algebrique ou transcendente."

The undecidability of Rosser's formula R_T in theory T could be derived from the consistency conjecture of T. Otherwise, Rosser's judgment remains within PA (first order arithmetic). Hence, the proof of undecidability of R_T can be formalized in the theory PA+Con(T), i.e. in the theory PA plus the consistency conjecture of T. A theory that is used to discuss properties of some other theory is called a **metatheory**. Hence, the undecidability of R_T can be established in the metatheory PA+Con(T). Perhaps, this metatheory can establish also T-

undecidability of some other formulas. Still, maybe, there are formulas, whose undecidability cannot be established in PA+Con(T), i.e. the consistency conjecture of T may appear insufficient for this purpose?

The answer can be obtained by modeling the Extended Liar's paradox (see Section 5.1):

q: (q is false) or (q is undecidable).

All the three possible alternatives (q is true, q is false, q is undecidable) lead to contradictions. If theory T is discussed in metatheory M, then we can try to obtain a formula H, which will assert that

"H is refutable in T, or M proves T-undecidability of H".

This can be done, indeed, and as a result, we would obtain the first ("Gödelian") version of the double incompleteness theorem: if theories T, M are both w-consistent, then the formula H is undecidable in T, yet this cannot be established in M (see Podnieks [1975]). Hence the term "double incompleteness theorem". We will prove here the extended ("Rosserian") version of this theorem (Podnieks [1976]).

First, we must define the relationship "M is metatheory for T" precisely. Let T and M be two fundamental theories, i.e. theories containing first order arithmetic PA. Let us denote by Tr_T and Tr_M the translations of PA in T and M respectively (see Section 3.2). Let us say that M **is a metatheory of** T, if we have PA-formulas $PR_T(x)$ and $RF_T(x)$ such that for all PA-formulas F:

a) If T proves $Tr_T(F)$, then M proves $Tr_M(PR_T(\mathbf{F}))$.

b) If T proves $Tr_T(\neg F)$, then M proves $Tr_M(RF_T(\mathbf{F}))$.

Thus, the theory M "knows" something about the arithmetical statements that can be proved or refuted in T. For simplicity of notation let us write simply

T proves F, T proves ¬F, M proves $PR_T(\mathbf{F})$, M proves $RF_T(\mathbf{F})$

instead of

T proves $Tr_T(F)$, M proves $Tr_M(PR_T(\mathbf{F}))$ etc.

Double Incompleteness Theorem. Let T and M be two fundamental theories (only conditions Fu_1, Fu_2 are necessary), and M is a metatheory for T. Then there is a closed PA-formula H such that if T and M are both consistent, then H is undecidable in T, yet M cannot prove neither $\neg PR_T(\mathbf{H})$, nor $\neg RF_T(\mathbf{H})$ (i.e. the metatheory M cannot prove neither the T-unprovability, nor the T-unrefutability of the formula H).

Proof. Since the set of all theorems of a formal theory is computably enumerable, let an appropriate Turing machine enumerate all arithmetical theorems of T and M:

$$(T, A_0), (M, A_1), (T, A_2), (M, A_3), \ldots \qquad (1)$$

The appearance of the pair (T, A) means that T proves A, the appearance of (M, A) – that M proves A. Our aim is to obtain a formula H such that none of the following four assertions can hold:

$$T \text{ proves } H,\ T \text{ proves } \neg H,\ M \text{ proves } \neg PR_T(\mathbf{H}),\ M \text{ proves } \neg RF_T(\mathbf{H}). \qquad (2)$$

Therefore, let us call a formula Q **positive**, if in the enumeration (1) one of the pairs (T, Q) or (M, $\neg RF_T(\mathbf{Q})$) appears first, and let us call Q **negative**, if first appears (T, $\neg Q$) or (M, $\neg PR_T(\mathbf{Q})$). Our target formula H must be neither positive, nor negative. The enumeration index of the first pair appeared we call (respectively) the positive or negative index of the formula Q. The following two predicates are computably solvable:

a(x,y) = " y is the positive index of the formula number x",

b(x,y) = " y is the negative index of the formula number x".

Let formulas A(x,y), B(x, y) express these predicates in PA. Now, following the Rosser's proof method, let us take the formula

$$\forall y\,(A(x,y) \rightarrow \exists z{<}y\ B(x,z))$$

and let us apply the self-referential lemma. In this way we obtain a closed PA-formula H such that

$$\text{PA proves: } H \leftrightarrow \forall y\,(A(\mathbf{H}, y) \rightarrow \exists z{<}y\ B(\mathbf{H},z)),$$

i.e. H asserts: "If I am positive, then I am negative, and my negative index is less than my positive index".

Exercise 6.2 (for smart students). Modify Rosser's proof (Section 5.3), and verify that either of the assertions (2) leads a contradiction in T, or in M. (Hint: consider two situations: a) the least negative index of H is less than the least positive index of H (the latter may not exist at all); b) the least positive index of H is less than the least negative index of H (the latter may not exist at all).

This completes the proof of the double incompleteness theorem.

If we take M = PA+Con(T), i.e. if we discuss a theory T by means of PA using only the consistency conjecture of T, then there are T-undecidable formulas, whose undecidability cannot be proved by using this conjecture only. To prove the undecidability of these formulas (obtained from the double incompleteness theorem) the conjecture Con(PA+Con(T)) is needed. This is the answer to the question posed at the beginning of this section.

The incompleteness phenomenon allows a new method of developing mathematical theories. If in some theory T we are not able to prove or disprove an assertion F, then we may try to adopt F (or ¬F) as an additional axiom. However, this approach is somewhat dangerous: maybe, in the **future** the assertion F will be proved (then our attempt to develop the theory T+¬F will cause unwelcome aftereffects) or disproved (then similar aftereffects will cause our attempt to develop T+F). Therefore, it would be nice, before adopting a new axiom F, to obtain some guarantee that this way does not lead to contradictions. I.e. it would be nice to prove the consistency of our intended new theory T+F. From Gödel's second theorem we know that an **absolute** consistency proof is impossible. Such proof must involve assertions from outside of T+F, i.e. assertions that may be even more dangerous than F itself. Hence, we cannot obtain an absolute guarantee. Still, it is possible to obtain a **relative guarantee** – we can try to prove that the adoption of the new axiom F does not generate "new" contradictions (except the "old" ones which – maybe – are already contained in our initial theory T).

The possibility of this approach was realized long before Gödel – at the beginning of XIX century, when the non-Euclidean geometry was invented. Let us denote: A – the so-called absolute geometry, P – Euclid's fifth postulate. Then A+P is the classical Euclidean geometry. In 1820's J. Bolyai and N. Lobachevsky established that developing the theory A+¬P for a long time no contradictions can be obtained. And in 1871 F. Klein proved that

$$\mathrm{Con}(A+P) \rightarrow \mathrm{Con}(A+\neg P),$$

i.e. that we can develop non-Euclidian geometry safely, if the safety of developing A+P (Euclidean geometry) is not questioned. Thus the possibility of developing **alternative** mathematical theories was discovered (or, invented?).

The "normal" way of doing mathematics is deriving consequences from a stable list of axioms. Incompleteness theorems were additional evidence that no stable list of axioms can be sufficient for solving of all problems that can appear in mathematical theories. Since incompleteness is inevitable, one could adopt a more flexible way of doing mathematics: if, doing a theory T we cannot prove the assertion F, let us try to prove that

$$\mathrm{Con}(T) \rightarrow \mathrm{Con}(T+F),$$

then, adopt F as an additional axiom, and continue developing T+F (instead of T) safely. Thus, instead of the old **principle of stable axioms** a new **principle of stable safety** could be adopted.

The double incompleteness theorem shows that the principle of stable safety also is incomplete. Really, by taking M = T+Con(T) we obtain from this theorem a formula H that is undecidable in T, yet in M we cannot prove

neither $\neg PR_T(\mathbf{H})$ (i.e. the consistency of T+¬H), nor $\neg RF_T(\mathbf{H})$ (i.e. the consistency of T+H). Thus, neither of the safety conditions

$$Con(T) \rightarrow Con(T+F),$$

$$Con(T) \rightarrow Con(T+\neg F)$$

can be proved within theory T.

From this point of view, for example, the Axiom of Determinacy (AD) is only a "semi-dangerous" postulate: if ZF is consistent, then

$$Con(ZF) \rightarrow Con(ZF+AD)$$

cannot be proved in ZF. However, one can prove in PA that

$$Con(ZF) \rightarrow Con(ZF+ \neg AD).$$

Open problem? All the well-known powerful set-theoretic hypotheses H are "semi-dangerous" only (in the above sense), all having the following properties:

a) PA proves: Con(ZFC) → Con(ZFC+¬H);

b) Con(ZFC) → Con(ZFC+H) cannot be proved (sometimes, even in ZFC+H).

Or, the same property with ZF instead of ZFC. Is there some interesting set-theoretical hypothesis H such that neither

Con(ZF) → Con(ZF+H) (or Con(ZFC+H)),

nor

Con(ZF) → Con(ZF+¬H) (or Con(ZFC+¬H))

can be proved (in PA, in ZF etc.)?

Added July 10, 2014

The double incompleteness phenomenon was mentioned by Per Lindström in his 1997 book:

P. Lindström. Aspects of Incompleteness. *Lecture Notes in Logic*, Vol. 10, 1997, 132 pp. (available online at Project Euclid)

See Exercise 5 on p. 36:

5. Suppose S extends Q [Robinson's arithmetic]. Show that there is a Π_1 sentence θ such that S does not prove neither θ, nor ¬θ, and T does not prove neither $PR_S(\theta)$, nor $\neg PR_S(\theta)$.

6.3. Is Mathematics "Creative"?

In mathematics all theorems are being proved by using a stable list of axioms (for example, the axioms of ZFC). Sometimes this thesis is put as follows: all

the results you can obtain in mathematics are already contained in axioms. Hence, when doing mathematics, "nothing new" can appear?

Really? If you define as "new" only those principles of reasoning that you cannot justify by referring to commonly acknowledged axioms, then the above thesis becomes a truism (i.e. it contains "nothing new"). And then the only "new" things described in this book, are those that cannot be derived from the axioms of ZFC: Continuum Hypothesis, Axiom of Constructibility and Axiom of Determinacy!

Q.E.D., if you agree that the distinctive character of a mathematical theory is a stable self-contained system of basic principles. All theorems of set theory really are (in a sense) "contained" in the axioms of ZFC. As we know, the set of all theorems of ZFC is computably enumerable. I.e. you can write a computer program that will work printing out the (infinite) sequence of all theorems of ZFC:

$$F_0, F_1, F_2, F_3, F_4, ...$$

Note. According to the official terminology, computably enumerable sets are called "recursively enumerable sets", in some texts – also effectively enumerable sets, or listable sets.

Thus, any theorem of ZFC will be printed out by this program – maybe, this will happen within the next 100 years, maybe, some time later. Still, does it mean that when doing set theory ZFC "nothing new" can appear?

Imagine, you are solving some mathematical problem, and you are arrived at a hypothesis H, and you would like to know, is this hypothesis "true" (i.e. provable in ZFC) or "false" (i.e. disprovable in ZFC)? Could you use the above computer program for this purpose? Having bought enough beer you could stay sitting very long by the paper tape of your computer waiting for the formula H printed out (this would mean that ZFC proves H) or the formula ¬H printed out (this would mean that ZFC disproves H). Still, as we know from incompleteness theorems, formula H may be undecidable for ZFC – in this case neither H, nor ¬H will be printed *ad infinitum*, and we will never be able to decide – let us wait another 100 years or let us drop waiting immediately.

Hence, the obvious enumerating program for ZFC almost does not help doing mathematics. What would really help, is called **decision procedures**. We could say, that mathematics is (in a sense) a purely "mechanical art" (producing "nothing new"), only when we had an algorithm determining for each closed formula H, whether

a) ZFC proves H, or

b) ZFC refutes H, or

c) H is undecidable in ZFC.

Exercise 6.3. Traditionally, **decision procedure** for some theory T is defined as an algorithm determining is an arbitrary closed formula provable in T or not. Verify that a decision procedure exists, if and only if there is an algorithm determining the membership of formulas in classes a), b), c).

If ZFC would be inconsistent, then all formulas would be provable in ZFC, i.e. in this case the classes a) and b) would coincide, and the class c) would be empty. After a contradiction has been found in some theory, it becomes a purely "mechanical art" (in the sense of the above definition).

Thus, we can discuss seriously the existence of an algorithm separating the classes a), b) and c) for some theory T only under the assumption that this theory is consistent, i.e. under the assumption that classes a) and b) do not intersect. Then, by the First (Gödel-Rosser) Incompleteness Theorem, the class c) is non-empty.

So, let T be any consistent fundamental theory (see Section 3.2). We will prove that there is no algorithm determining whether an arbitrary closed formula is provable in T, refutable in T, or undecidable for T.

We will prove this in a somewhat stronger form. Let us say that the class of all T-provable formulas is **computably separable** (another term – "recursively separable") from the class of all T-refutable formulas, if and only if there is an algorithm A transforming each T-formula into 0 or 1 in such a way that:

a) If T proves F, then the algorithm A returns 1.

b) If T refutes F, then the algorithm A returns 0.

c) If F is undecidable for T, then A returns 0 or 1.

Thus, the algorithm A does not recognize exactly neither T-provable, nor T-refutable formulas, yet it knows how to "separate" the first class from the second one. We will prove that even such an algorithm does not exist, if T is a consistent fundamental theory. I.e., we will prove that the class of all T-provable PA formulas (i.e. first order arithmetical formulas) is not computably separable from the class of all T-refutable PA formulas.

Unsolvability Theorem. Let T be a consistent fundamental theory. Then the class of all T-provable PA formulas is not computably separable from the class of all T-refutable PA formulas. Hence, there is no decision procedure for T. And, in particular, there is no decision procedure for PA.

Note. The Unsolvability Theorem was proved in the famous 1936 papers by Church and Turing (see Church [1936] and Turing [1936], and improved by Rosser (see Rosser [1936]).

Proof. Let us assume the opposite – that there is an algorithm separating T-

provable PA formulas from T-refutable PA formulas. Then there is a Turing machine M computing the following function s(x):

1) If n is a Gödel number (see Section 5.2) of (the T-translation of) a T-provable PA formula, then s(n)=1.

2) If n is a Gödel number of (the T-translation of) a T-refutable PA formula, then s(n)=0.

3) Otherwise, s(n)=0 or s(n)=1.

Let the formulas $C_0(x, t)$, $C_1(x, t)$ express in PA the following (computably solvable) predicates:

"the machine M working on the argument value x stops after t steps and issues the result 0",

"the machine M working on the argument value x stops after t steps and issues the result 1".

Following Rosser's idea from Section 5.3 we can obtain from the Self-reference lemma a closed formula E such that

$$\text{PA proves: } E \leftrightarrow \forall t(C_1(\mathbf{E}, t) \rightarrow (\exists z{<}t)C_0(\mathbf{E}, z)).$$

Exercise 6.4. Following Rosser's proof (Section 5.3) show that, if s(**E**)=1, then PA proves ¬E, and if s(**E**)=0, then PA proves E.

Since T proves all theorems of PA, and T is consistent, this means that, if s(**E**)=1, then s(**E**)=0, and if s(**E**)=0, then s(**E**)=1. This is impossible. Hence, no algorithm can separate T-provable PA formulas from T-refutable PA formulas. Q.E.D.

As you know, the class of all T-provable formulas, and the class of all T-refutable formulas both are computably enumerable (or, recursively enumerable). It follows from our theorem that neither of these classes can be computably solvable (i.e. recursive), and that the class of all T-undecidable formulas is not even computably enumerable (and, in particular, non-empty).

Exercise 6.4A. Verify.

Thus, the First **Incompleteness Theorem is an easy consequence of the Unsolvability Theorem.**

The Unsolvability Theorem has important practical consequences. Imagine, you are solving some mathematical problem, and you are arrived at a hypothesis H, and you would like to know, is this hypothesis "true" (i.e. provable in the theory T you are working in) or "false" (i.e. disprovable in T)? If T is a consistent fundamental theory, then there is no decision procedure for T, i.e. there is no **general method** for deciding is H provable in T or not.

Hence, to solve your problem you must find some **specific features** of your hypothesis H that are making it provable, disprovable (or undecidable?) in your theory T. Since there is no general method of doing this, your theory T should be qualified as an "extremely creative environment". If you will succeed in finding the specific features of the hypothesis H that make it true, this will not mean that your ideas will be applicable to your next hypothesis H2 etc.

Note. This part of our "creativity philosophy" is applicable only to consistent theories. Still, maybe, our theory is inconsistent? **Finding a contradiction in a serious mathematical theory should be qualified as a first class creative act!** See, for example, the story of Russell's paradox in Section 2.2. And as we know from the Exercise 6.1, there is no general method for deciding is a given theory consistent or not. Hence, mathematics is creative "on both sides".

Note. The mere existence of a decision procedure does not mean automatically that your theory becomes a purely "mechanical art". Return, for example, to Presburger arithmetic in Section 3.1. Any decision procedure of this theory necessarily takes $2^{2^{Cn}}$ steps to decide about formulas consisting of n characters. Thus, from a practical point of view, we may think as well that Presburger arithmetic "has no decision procedure".

Working mathematicians can view formal theories as mathematical models of the traditional (purely intuitive, semi-axiomatic etc.) mathematical theories. Formal theories, themselves, can be investigated as mathematical objects. The Unsolvability Theorem establishes for formal theories essentially the same phenomenon that is well known from the history of (the traditional) mathematics: **no particular set of ideas and/or methods allows solving of all problems that arise in mathematics** (even when our axioms remain stable and "sufficient"). To solve new problems – as a rule – new ideas and new methods are necessary. Thus, mathematics is a kind of *perpetuum mobile* – a never ending challenge, a never ending source of new ideas.

6.4. On the Length of Proofs

As number theorists have noticed long ago, the famous Riemann's hypothesis (published 1859) allows not only proving of new (stronger) theorems about prime numbers. By assuming this hypothesis we can also obtain **simpler proofs** of some well-known theorems. These theorems can be proved without Riemann's hypothesis, yet these "purist" proofs are much more complicated.

How looks this phenomenon at the level of formal theories? If we add to our theory T a new axiom – some hypothesis H that is undecidable for T, then we obtain a new "stronger" theory T+H. And small wonder, if in T+H not only

new theorems can be proved (that were unprovable in T), yet also some hard theorems of T allow much simpler proofs in T+H?

Kurt Gödel proved in 1935 (published in 1936) that this is really the case:

K.Gödel. Über die Länge von Beweisen. "Ergebnisse eines mathematischen Kolloquiums (herausgegeben von K.Menger)", 1936, Heft 7, pp,23-34.

Let us denote by $|K|_T$ the length of the shortest T-proof of the formula K (the exact definition will follow). For a better understanding of the theorem you may take at first $f(x)=\frac{x}{100}$.

Theorem on the Length of Proofs. If T is a fundamental formal theory, and a closed formula H is not provable in T, then for each computable function f(x), which grows to infinity, there is a theorem K of T such that

$$|K|_{T+H} < f(|K|_T).$$

For example, let us take $f(x)=\frac{x}{100}$. There is a theorem K_1 of the theory T such that its proof in the extended theory T+H is at least 100 times shorter than its shortest proof in T. You may try also $f(x)=\frac{x}{1000}$, or $f(x)=\sqrt{x}$, or $f(x)=\log_2(x)$, etc.

The above theorem holds for any method of measuring the length of proofs that satisfies the following two conditions:

a) The length of a proof is computable from the text of it.

b) For any number t there is only a finite set of proofs having length ≤t. More precisely, there is an algorithm that (given a number t) prints out all proofs having length ≤t, and halts.

The simplest method of measuring the length of proofs (by the number of characters, i.e. the length of the text) satisfies these conditions. Indeed, for a theory T each T-proof is a sequence of formulas in the language of T. If the alphabet of the language is finite, i.e. it consists of some s characters (variable names are generated, for example, as x, xa, xaa, xaaa, etc.), then there are less than $(s+1)^t$ proofs having length ≤t.

Proof of the theorem. Let us assume the opposite: there is a computable function f(x) which grows to infinity such that for all theorems K of the theory T:

$$|K|_{T+H} \geq f(|K|_T). \qquad (1)$$

The main idea – we will derive from this assumption a **decision procedure** for

the theory T+¬H. Since formula H is not provable in T, theory T+¬H is a consistent fundamental theory, hence, such decision procedure cannot exist (see the Unsolvability Theorem in Section 6.3).

So, let use (1) to build a decision procedure for T+¬H. If some formula K is provable in T+¬H, then T proves the formula ¬H→K. Then (1) yields that

$$f(|\neg H \rightarrow K|_T) \leq |\neg H \rightarrow K|_{T+H}. \qquad (1a)$$

The second idea – let us note that the formula ¬H→K always is provable in T+H, moreover, it has a **very short proof** in T+H. Indeed, by means of propositional calculus we can prove the formula H→(¬H→K), and since H is axiom of T+H, we obtain ¬H→K immediately. By (1a), this fact yields an upper bound b for the length of the shortest proof of ¬H→K in T. By scanning all proofs of length ≤b we can determine, is ¬H→K provable in T (i.e. is K provable in T+¬H), or not.

More precisely, let us imagine the mentioned "very short proof" of ¬H→K in full:

...	
H→(¬H→K)	Up to this place – a fixed proof schema in the propositional calculus.
H	Axiom of T+H
¬H→K	By MODUS PONENS.

Thus, the entire proof is a proof schema with "parameters" H, K. Hence, its length is a computable function g(H, K) (see the condition a) above). Thus we have:

$$|\neg H \rightarrow K|_{T+H} \leq g(H, K),$$

and with (1a):

$$f(|\neg H \rightarrow K|_T) \leq g(H, K). \qquad (2)$$

I.e., if K is provable in T+¬H, then T proves ¬H→K and (2) holds. Since f and g are computable functions, and since f is growing to infinity, we can obtain another computable function h(H, K) such that, if K is provable in T+¬H, then

$$|\neg H \rightarrow K|_T \leq h(H, K).$$

Exercise 6.5. Show that this is the case. How would you compute h(H, K)?

Having the function h we can propose the following procedure for solving is

an arbitrary formula K provable in T+¬H, or not. If T+¬H proves K, then T proves ¬H→K, and one of these proofs is of length ≤h(H, K). So, let us compute h(H, K), and let us examine the (finite) list of all proofs of length ≤h(H, K) (see the condition b) above). If one of these proofs is proving ¬H→K in T, then T+¬H proves K. If there is no such proof in the list, then T+¬H cannot prove K. Q.E.D.

Maybe, the above-mentioned method of measuring length of proofs seems "unnatural" to you. Maybe, you would like to have in the alphabet of the language an infinite set of letters for variables, and a finite set of other characters? Then, by replacing variable letters in some proof, you can obtain an infinite number of equivalent proofs having the same length (i.e. the length of text measured in characters). Hence, for your "method", the condition b) does not hold. Still, how would you display your infinite characters set on screens, and how would you print them out? I.e. having an infinite alphabet, you must introduce some method for measuring size ... of characters (in pixels or dots of a fixed size). And the condition: c) for any number t there is only a finite set of characters having size ≤t. And respectively, you must measure length of proofs in pixels or dots, not in characters. And for this elaborate method the condition b) will hold!

Further reading:

Samuel R. Buss. On Gödel's theorems on lengths of proofs I: Number of lines and speedups for arithmetic. *Journal of Symbolic Logic* 39 (1994) 737-756.

Samuel R. Buss. On Gödel's Theorems on Lengths of Proofs II: Lower Bounds for Recognizing k Symbol Provability. In *Feasible Mathematics II,* P. Clote and J. Remmel (eds), Birkhauser, 1995, pp. 57-90.

Short Theorems with Long Proofs

Inspired by reading

D.Zeilberger. THEOREMS FOR A PRICE: Tomorrow's Semi-Rigorous Mathematical Culture. *Notices of the AMS*, Vol. 40, N8 (October 1993), pp.978-981 (online copy available).

Joel H. Spencer. Short Theorems with Long Proofs. *Amer. Math. Monthly*, 1983, vol. 90, pp. 365-366.

John W. Dawson. The Gödel incompleteness theorem from the length of proof perspective. *Amer. Math. Monthly*, 1979, vol. 86, pp. 740-747.

Theorem. Assume, T is a fundamental formal theory, and f(x) is a computable function that grows to infinity. If T is consistent, then there is a theorem K of T such that $|K|_T > f(|K|)$, i.e. the shortest T-proof of K is "f-longer" than the length |K| of the theorem K itself.

For example, let us take f(x) = 1000000·x. There is a theorem K of the theory

T such that its proof is more than million times longer than the formula K itself. You may try also $f(x) = (1000x)^2$, or 2^{1000x} etc.

Exercise 6.6. Prove the above theorem. (Hint: assume the contrary, and derive a contradiction with the Unsolvability Theorem.)

6.5. Diophantine Incompleteness Theorem: Natural Number System Evolving?

How would we prove Gödel's incompleteness theorem knowing that for every computably enumerable set we can build a Diophantine representation (see Section 4.1)? For a precedent of such "Diophantine incompleteness theorems" see Davis, Putnam, Robinson [1961] (Corollary 2a).

Let T be a fundamental theory. The following predicate is computably enumerable:

$pr_T(x)$ = "T proves the T-translation of the PA-formula number x".

Let us denote by

$$\exists z_1 ... \exists z_k \, P_T(x, z_1, ... , z_k)=0$$

a Diophantine representation of $pr_T(x)$. Here P_T is a polynomial with integer coefficients, the numbers k of variables may depend on T (still, we can take for granted that it never exceeds 13, see Matiyasevich, Robinson [1975]). Every PA-formula F is provable in T, if and only if the Diophantine equation $P_T(\mathbf{F}, z_1, ... , z_k)=0$ has solutions in natural numbers (**F** is Gödel number of F). By applying the Self-Referential Lemma we obtain a closed PA-formula D_T such that

$$\text{PA proves: } D_T \leftrightarrow \neg \exists z_1 ... \exists z_k \, P_T(\mathbf{D_T}, z_1, ... , z_k)=0. \qquad (1)$$

Thus D_T is a Diophantine version of the Gödel's formula G_T.

Let us assume that T proves D_T. Then $pr_T(\mathbf{D_T})$ is true, and hence, the equation

$$P_T(\mathbf{D_T}, z_1, ... , z_k)=0 \qquad (2)$$

as solutions in natural numbers. Denote one of these solutions by $(b_1, ... , b_k)$, then

$$\text{PA proves: } P_T(\mathbf{D_T}, b_1, ... , b_k)=0$$

as a numerical equality that does not contain variables (see Exercise 3.4a).

Hence,

$$\text{PA proves: } \exists z_1 ... \exists z_k \, P_T(\mathbf{D_T}, z_1, ... , z_k)=0,$$

and by (1) we have established that PA (and T) proves $\neg D_T$. I.e., if T proves D_T, then T is inconsistent.

On the other hand, if T is consistent, then T cannot prove D_T. Hence, $pr_T(\mathbf{D_T})$ is false, and the equation (2) has no solutions in natural numbers. Nevertheless, the corresponding formula

$$\neg \exists z_1 ... \exists z_k \, P_T(\mathbf{D_T}, z_1, ... , z_k)=0$$

that asserts this unsolvability cannot be proved in T (because it is equivalent to D_T).

Thus we have established the following

Diophantine Incompleteness Theorem. Let T be a fundamental theory. Then there is a Diophantine equation $Q_T(x_1, ... , x_n)=0$ such that: a) If T is inconsistent, then the equation **has** solutions in natural numbers. b) If T is consistent, then the equation **has no** solutions in natural numbers, yet this cannot be proved in T.

Let us consider the Diophantine equation $Q_{PA}=0$. If we will find some its solution in natural numbers, then we will find a contradiction in PA. Still, if $Q_{PA}=0$ has no solutions in natural numbers, then this cannot be proved in PA. I.e. PA cannot solve some problems in the area of Diophantine equations. Since the set theory ZF proves the consistency of PA, then ZF proves also the unsolvability of the equation $Q_{PA}=0$. I.e. in set theory we can solve some problems in the area of Diophantine equations that cannot be solved in first order arithmetic. This contradicts the widely believed thesis about the "primary nature" of natural numbers in mathematics. Some people believe that the notion of natural numbers does not depend on more complicated mathematical notions (for example, on the notion of real numbers, or Cantor's notion of arbitrary infinite sets). A striking expression of this belief is due to Leopold Kronecker:

Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.

(God created the integers, all-else is the work of men.) As we have seen, this cannot be true: there are even some problems in the area of Diophantine equations (i.e. very "intrinsic" problems of "the" natural number system) that can be solved only by using more complicated notions than the initial (first order) notion of natural numbers.

The second conclusion: **the human notion of natural numbers is evolving**. When Georg Cantor invented the set theory in 1873, **he extended also the notion of natural numbers** by adding new features to it. For example, before 1873, the unsolvability of the above equation $Q_{PA}=0$ could not be proved, but now we can prove it. For a much more striking example (the so-called Extended Finite Ramsey's Theorem) see Appendix 2.

Note. The following remarks by Walter Felscher (1931-2000) about Kronecker's famous sentence appeared on the mailing list Historia-Mathematica:

-----Original Message-----
From: Walter Felscher <walter.felscher@uni-tuebingen.de>
To: Bill Everdell <Everdell@aol.com>
Cc: historia-matematica@chasque.apc.org <historia-matematica@chasque.apc.org>
Date: 1999. May 27. 9:36
Subject: [HM] Die ganzen Zahlen hat der liebe Gott gemacht

The earliest reference to Kronecker's dictum, appearing in the subject, seems to be the necrologue

Heinrich Weber: Leopold Kronecker. Jahresberichte D.M.V 2 (1893) 5-31

where Weber writes about Kronecker

Mancher von Ihnen wird sich des Ausspruchs erinnern, den er in einem Vortrag bei der Berliner Naturforscher-Versammlung im Jahre 1886 tat "Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk".

It is important not to omit in this dictum the adjective "liebe" in "liebe Gott".

Because "lieber Gott" is a colloquial phrase usually used only when speaking to children or illiterati. Adressing grownups with it contains a taste of being unserious, if not descending (and not towards the audience, but towards the object of substantive "Gott") ; no priest, pastor, theologian or philosopher would use it when expressing himself seriously. There is the well known joke of Helmut Hasse who, having quoted Kronecker's dictum on page 1 of his yellow "Vorlesungen über Zahlentheorie" 1950, added to the index of names at the book's end under the letter "L" the entry "Lieber Gott ..... p.1 "

As Kronecker's dictum is related, it appears as nothing but a witticism: "About the integers let us not ask, but all the rest came about by men – namely so ... "

Would Kronecker have wanted to make a theologico-philosophical statement, he would have omitted the Children's language: "Die Zahlen kommen von Gott, der Rest ist menschliche Erfindung."

I doubt that Kronecker's dictum can be construed to express a distinction between a Kroneckerian viewpoint of a divine, pre-human origin of the integers, and Dedekind's viewpoint that also the integers are man-made (i.e. man-invented) .

W.F.

6.6. Löb's Theorem

In his proof of the incompleteness theorem K.Gödel used a formula asserting, "I am unprovable in the theory T", i.e. formula G_T such that

$$\text{PA proves: } G_T \leftrightarrow \neg PR_T(\mathbf{G_T}).$$

If T is a consistent theory, then, indeed, G_T is unprovable in T.

Now let us imagine a formula asserting just the opposite – "I am provable in T", i.e. a formula H_T such that

$$\text{PA proves: } H_T \leftrightarrow PR_T(\mathbf{H_T}).$$

Will such a formula really be provable in T – "as it wants to be"? Leon Henkin asked this question in 1952. The answer is "yes" – as Martin Hugo Löb (1921-2006) proved in 1955:

M. H. Löb. Solution of a problem of Leon Henkin. "J. Symbolic Logic", 1955, vol.20, pp. 115-118.

Löb's Theorem. If T is a fundamental theory, and $PR_T(x)$ is a PA-formula satisfying Hilbert-Bernays-Löb derivability conditions (see Section 5.4), then for any closed formula B: if T proves $PR_T(\mathbf{B})\rightarrow B$, then T proves B.

Hence, T proves the above formula H_T.

As put nicely by Marc Geddes on the *extropy-chat mailing list* (February 8, 2006): "...Löb's theorem says that if a löbian machine (PM, PA, or ZF for example) proves Bp → p, for some proposition p, then soon or later the machine will prove p (if it has not been done already)."

Another formulation: if T proves $PR_T(\mathbf{B})\rightarrow B$, then, in a sense, T proves that "T is sound for B". Hence, if T proves its own soundness for B, then T proves B.

"Proof". If T proves $PR_T(\mathbf{B})\rightarrow B$, then T proves $\neg B\rightarrow\neg PR_T(\mathbf{B})$. Hence, T+¬B proves $\neg PR_T(\mathbf{B})$. I.e. T+¬B proves that B is unprovable in T. Hence, T+¬B proves that T+¬B is a consistent theory. By Gödel's second theorem, if T+¬B proves its own consistency, then T+¬B is inconsistent, i.e. T proves B. Q.E.D.

The above "proof" contains essential gaps.

Exercise 6.7 (for smart students). Determine and fill in these gaps. (Hint: a) Show that there is a closed formula L such that PA proves: $L\leftrightarrow\neg PR_T(\neg\mathbf{B}\rightarrow\mathbf{L})$.

Verify that, if T+¬B proves L, then T+¬B is an inconsistent theory. c) Define Con(T+¬B) as $\neg PR_T(\neg \mathbf{B} \rightarrow \mathbf{0=1})$, and verify that if T+¬B proves Con(T+¬B), then T+¬B is inconsistent. d) Next gap?)

Formula $PR_T(\mathbf{B}) \rightarrow B$ asserts: "If B is provable in T, then B is true", i.e. it asserts that T is "sound" for B. Löb's theorem says that if T proves its own "soundness" for B, then T proves B. I.e. if T cannot prove B, then T cannot prove that it is "sound" for B.

Read more about implications of Löb's theorem in the chapter about incompleteness theorems written by Craig Smorynski in Barwise [1977].

Exercise 6.7A (for smart students). An open problem? Formula $B \rightarrow PR_T(\mathbf{B})$ asserts: "If B is true, then B is provable in T", i.e. it asserts that T is "complete" for B. If T proves its own "completeness" for B, then – what?

6.7. Consistent Universal Statements Are Provable

Let us consider the famous Goldbach's Conjecture from 1742 by Christian Goldbach (1690-1764): **every even number greater than 2 can be expressed as a sum of two prime numbers**. For example (the really interesting numbers are shown in bold),

4=2+2, **6=3+3**, 8=5+3, **10=5+5**, 12=7+5, 14=11+3, 16=13+3, 18=13+5, 20=17+3, 22=19+3, 24=19+5, 26=23+3, 28=23+5, **30=23+7**, 32=29+3, 34=31+3, 36=31+5, 38=31+7, 40=37+3, 42=37+5, 44=41+3, 46=43+3, 48=43+5, 50=47+3, 52=47+5, 54=47+7, 56=53+3, 58=53+5, 60=53+7, 62=59+3, 64=61+3, 66=61+5, 68=61+7, 70=67+3, 72=67+5, 74=71+3, 76=73+3, 78=73+5, 80=73+7, 82=79+3, 84=79+5, 86=83+3, 88=83+5, 90=83+5, 92=89+3, 94=89+5, 96=89+7, **98=79+19**, 100=97+3, 102=97+5, 104=97+7, 106=103+3, 108=103+5, 110=107+3, 112=109+3, 114=109+5, 116=113+3, 118=113+5, 120=113+7, **122=109+13**, **124=113+11**, 126=113+13, 128=109+19, 130=127+3, 132=127+5, 134=131+3, ...

See also:

Puzzle 82.- The Goldbach's Comet by www.primepuzzles.net

Goldbach Conjecture Research by Mark Herkommer

Fractal in the statistics of Goldbach partition by Wang Liang, Huang Yan, Dai Zhi-cheng

Assume, you are a platonist believing that Goldbach's Conjecture is, "in fact", true. I.e. if you take any even number n, it can be expressed as a sum of two primes. If it can, you can determine these two primes $p_1 + p_2 = n$ simply by trying n = (n-3)+3, n=(n-5)+5, n=(n-7)+7, n=(n-11)+11, etc. up to n=k+k. Any

particular true equality $p_1 + p_2 = n$, i.e.

$$\underset{p_1 \text{ times}}{(1+1+...+1)} + \underset{p_2 \text{ times}}{(1+1+...+1)} = \underset{n \text{ times}}{(1+1+...+1)}$$

can be proved in PA (see Exercise 3.4a).

Let Go(x) be a formula expressing in PA the following (computable) predicate go(x):

"If x is an even number greater than 2, then x is a sum of two primes",

for example,

$$\exists y(y < x \wedge x = y + y) \wedge 2 < x \rightarrow \exists p_1 \exists p_2 (p_1 < x \wedge p_2 < x \wedge PR(p_1) \wedge PR(p_2) \wedge x = p_1 + p_2) \quad ,$$

where:

a<b is a shortcut for $\exists c(a + c + 1 = b)$, and

PR(z) is a shortcut for $\neg \exists u \exists v(u < z \wedge v < z \wedge z = u * v)$.

Formula Go(x) contains only bounded quantifiers. As we know from Exercise 3.4b, for each natural number n, if Go(**n**) is true, then PA proves Go(**n**) (**n** is the numeral representing the number n).

Now, Goldbach's Conjecture can be represented as the formula ∀x Go(x).

Thus, we have the following situation. If Goldbach's Conjecture is true, then, for each natural number n, PA proves Go(**n**). Could we conclude from this that PA proves ∀x Go(x), i.e. that PA proves Goldbach's Conjecture?

In general, no. Because, "for each n, PA proves Go(**n**)" means that there is an infinite sequence of proofs, a separate proof for each formula Go(**n**). Could we hope to convert this **infinite sequence** into a single **finite proof** of the formula ∀x Go(x)?

In general, no. For example, Gödel's self-referencing formula G, used in the incompleteness proof of PA, asserts "I'm not provable in PA". It is equivalent to the formula ∀y¬PRF(**G**, y), where the formula PRF(x, y) express the predicate "y is a PA-proof of x" (more precisely, "y is Gödel number of a PA-proof of the formula having Gödel number x"). As we know from Section 5.3, if PA is a consistent theory, then G cannot be proved in PA, i.e. the formula ¬PRF(**G**, **n**) is true for each n (**G** is the Gödel number of G). Hence, for each n, PA proves: ¬PRF(**G**, **n**). Could we conclude from this that PA proves ∀y¬PRF(**G**, y), i.e. that PA proves Gödel's formula G? No, because this would mean that PA is inconsistent! Hence, if PA is a consistent theory, then the infinite sequence of PA-proofs of the formulas ¬PRF(**G**, **n**) cannot be converted into a single finite PA-proof of the formula ∀y¬PRF(**G**, y).

On the other hand, let us assume that Goldbach's Conjecture is false. Then

there is an even number n>2, which cannot be expressed as a sum of two primes. Then, as we know from Exercise 3.4b, since the formula ¬Go(x) contains only bounded quantifiers, we can prove in PA the formula ¬Go(**n**). Then, of course, PA proves ∃x¬Go(x), and PA proves ¬∀x Go(x). Hence, if Goldbach's Conjecture is false, then PA "proves this fact".

And thus, if we could prove that PA **cannot** prove that Goldbach's Conjecture is false, then we would have a proof... that Goldbach's Conjecture is true! Since

"PA **cannot** prove that Goldbach's Conjecture is false"

is equivalent to

"PA + Goldbach's Conjecture is a consistent theory".

Hence, **if we could prove that Goldbach's Conjecture is consistent with the axioms of PA, then we would have a proof that Goldbach's Conjecture is true!**

The only specific property used in the above chain of reasoning, is the following: for all n, if Go(**n**) is false, then PA | proves ¬Go(**n**), so, a more general formulation of the above statement should be possible. Let us try to produce it.

Let T be any formal theory in the language of PA, and M – a fundamental theory. We will use M as a meta-theory of T.

F(x) is a formula containing exactly one free variable x.

$PR_T(y)$ is a formula intended to assert that "the formula having the Gödel number y is provable in T".

SUB(x, y, z) is a formula representing in PA the so-called substitution function (see Section 5.2):

sub(x, y) = "Gödel number of the formula obtained from the formula having the Gödel number x by substituting the numeral **y** for all of its free variables" (if x is not a Gödel number of a formula, then let sub(x, y)=0).

Suppose, T and M are powerful enough in the sense that

M proves: "For all natural numbers n, if ¬F(n), then T proves ¬F(**n**)".

More precisely (¬**F** is the Gödel number of the formula ¬F),

M proves: $\forall n(\neg F(n) \rightarrow \forall y(SUB(\neg \mathbf{F}, n, y) \rightarrow PR_T(y)))$.

Hence,

M proves: $\forall n(\neg \forall y(SUB(\neg \mathbf{F}, n, y) \rightarrow PR_T(y)) \rightarrow F(n))$, (*)

i.e. M proves that for all n, if T does not prove ¬F(**n**), then F(n) is true.

(1) Suppose, T, M and PR_T satisfy the following uniform derivability condition:

M proves: "For all n, if T proves: D(**n**), then T proves ∃xD(x)".

More precisely (**D** and **∃xD(x)** are Gödel numbers of the formulas D(x), ∃xD(x)),

M proves: $\forall n[\forall y(SUB(\mathbf{D}, n, y) \rightarrow PR_T(y)) \rightarrow PR_T(\exists \mathbf{xD(x)})]$.

Hence,

M proves: $\forall n[\neg PR_T(\exists \mathbf{xD(x)}) \rightarrow \neg\forall y(SUB(\mathbf{D}, n, y) \rightarrow PR_T(y))]$,

and,

M proves: $\neg PR_T(\exists \mathbf{xD(x)}) \rightarrow \forall n[\neg\forall y(SUB(\mathbf{D}, n, y) \rightarrow PR_T(y))]$, (**)

i.e. M proves that, if T does not prove ∃xD(x), then for all n, T does not prove D(**n**).

(2) Suppose, T, M and PR_T satisfy Hilbert-Bernays-Löb derivability conditions (see Section 5.4).

Now, from (*) and (**) we obtain directly that

M proves: $\neg PR_T(\exists \mathbf{x}\neg\mathbf{F(x)}) \rightarrow \forall n F(n)$.

Since T proves: $\exists x\neg F(x) \rightarrow \neg\forall x F(x)$, then, by (3), we obtain that

M proves: $PR_T(\exists \mathbf{x}\neg\mathbf{F(x)}) \rightarrow PR_T(\neg\forall \mathbf{xF(x)})$,

M proves: $\neg PR_T(\neg\forall \mathbf{xF(x)}) \rightarrow PR_T(\exists \mathbf{x}\neg\mathbf{F(x)})$,

and

M proves: $\neg PR_T(\neg\forall \mathbf{xF(x)}) \rightarrow \forall n F(n)$ (***).

Thus, we have proved the following

Theorem 6.7.1 (Author(s)? Folklore?). Suppose, T is any formal theory in the language of PA, M is a fundamental theory, and they satisfy the above-mentioned derivability conditions (1, 2). If, for the formula F(x) containing exactly one free variable x,

a) M proves: "For all natural numbers n, if ¬F(n), then T proves ¬F(**n**)",

b) M proves that ¬∀xF(x) cannot be proved in T,

then M proves ∀xF(x).

Corollary 6.7.2 (Author(s)? Folklore?). Suppose, T is any formal theory in the language of PA, M is a fundamental theory, and they satisfy the above-mentioned derivability conditions (1, 2). If, for the formula F(x) containing exactly one free variable x,

a) M proves: "For all natural numbers n, if ¬F(n), then T proves ¬F(**n**)",

b) M proves that T+∀xF(x) is a consistent theory,

then M proves ∀xF(x).

Proof. "M proves that T+∀xF(x) is a consistent theory" – what, precisely, does it mean? The formula Con(T+∀xF(x)) can be defined as "T does not prove ∀xF(x)→0=1", i.e. as $\neg PR_T(\forall \mathbf{xF(x)} \rightarrow \mathbf{0=1})$. Since T proves: ¬∀xF(x) → (∀xF(x)→0=1) (Axiom L_{10}), then, by (3), we obtain that

$$\text{M proves: } PR_T(\neg\forall \mathbf{xF(x)}) \rightarrow PR_T(\forall \mathbf{xF(x)} \rightarrow \mathbf{0=1}),$$

$$\text{M proves: } Con(T+\forall xF(x)) \rightarrow \neg PR_T(\neg\forall \mathbf{xF(x)}).$$

By (***),

$$\text{M proves: } Con(T+\forall xF(x)) \rightarrow \forall nF(n).$$

Q.E.D.

Corollary 6.7.3 (Author(s)? Folklore?). Suppose, T is any formal theory in the language of PA, M is a fundamental theory, and they satisfy the above-mentioned derivability conditions (1, 2). If

a) M proves: "For all natural numbers n, if ¬Go(n), then T proves: ¬Go(**n**)",

b) T + Goldbach's Conjecture is a consistent theory,

then M proves Goldbach's Conjecture.

Proof. Immediately, from Corollary 6.7.2.

Corollary 6.7.4 (Author(s)? Folklore?). Suppose, M is a fundamental theory, PA and M satisfy the above-mentioned derivability conditions (1, 2). If M is powerful enough to prove that **PA + Goldbach's Conjecture** is a consistent theory, then M proves **Goldbach's Conjecture**.

Proof. As we established above,

"For all natural numbers n, if ¬Go(**n**), then PA proves: ¬Go(**n**)."

These verifications can be formalized in PA:

$$\text{PA proves: } \forall n(\neg Go(n) \rightarrow \forall y(SUB(\neg\mathbf{Go}, n, y) \rightarrow PR_T(y))).$$

Hence, since M is a fundamental theory, then, by Corollary 6.7.3, Q.E.D.

According to Corollary 6.7.3**,** instead of PA, we could use any weaker axiom system T such that for all natural numbers n, if ¬Go(**n**), then T proves ¬Go(**n**). Thus, if we could prove that Goldbach's Conjecture is consistent with the weakest known of such axiom systems, then we would have proved that Goldbach's Conjecture is true! The weaker the system T, the easier should be the consistency proof of T + Goldbach's Conjecture? Yes, but – the weaker the system T, the more difficult becomes proving of "for all natural numbers n, if ¬Go(**n**), then T proves: ¬Go(**n**)". This proof is very easy for PA, but the consistency proof of PA + Goldbach's Conjecture seems to be very difficult...

Strange and/or crazy situation? A kind of paradox?

Note. The conclusion of Corollary 6.7.4 **does not apply to the Twin Prime Conjecture**:

$$\forall x \exists p(p > x \wedge PR(p) \wedge PR(p+2)) \quad .$$

The negation of it means that there is a number *n* such that

$$\forall p(p \geq \boldsymbol{n} \rightarrow \neg(PR(p) \wedge PR(p+2))) \quad .$$

If one proves that Twin Prime Conjecture (or its negation) does not create contradictions, this does not yield a proof of this conjecture (or its negation).

Exercise 6.8.1 (for smart students). If one proves that **Riemann Hypothesis** (or its negation) does not create contradictions, does this yield a proof of this conjecture (or its negation)?

Further reading:

Online comments by William G.Dubuque at

http://www.math.chalmers.se/~bo/internetguiden/listexempel.html#9

Kemeny, J. G. "Undecidable Problems of Elementary Number Theory." *Math. Ann.* **135**, 160-169, 1958.

Kreisel's Conjecture – see: Eric W. Weisstein. "Kreisel Conjecture." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/KreiselConjecture.html

6.8. Berry's Paradox and Incompleteness. Chaitin's Theorem.

Gödel's Incompleteness Theorem was – in a sense – "inspired" by the Liar's Paradox. The idea that Berry's Paradox could inspire an incompleteness theorem, which could be, in a sense, stronger than Gödel's theorem is due to Gregory J.Chaitin. He tells in his 1993 lecture at the University of New Mexico that in 1974 he tried to check the reaction of Gödel himself to this idea. Unsuccessfully.

In this section, a purely **syntactical version of Chaitin's Theorem** will be

proved. I.e. neither "semantical soundness" of the theories in question, nor even their syntactical consistency will be assumed.

In its classical form, **Berry's Paradox** sounds as follows. Let us consider the following phrase, consisting of **fourteen** English words:

The first natural number, which cannot be defined by using under **fifteen** English words.

Thus, "the first natural number, which cannot be defined by using under fifteen English words" **can** be defined by using **fourteen** English words!

Unfortunately, very little can be found on the web about the author of this paradox. According to Berry paradox: "Bertrand Russell, the first to discuss this paradox in print, attributed it to G. G. Berry, a librarian at Oxford's Bodleian library." And according to Vicious circle[Britannica] the full name of G. G. Berry was **George Godfrey Berry**.

The above-mentioned Russell's 1906 paper:

B. Russell. Les paradoxes de la logique. *"Revue de Metaphysique et de Morale"*, 1906, 14, pp.627-650.

Of course, Berry's Paradox is not the only paradoxical thing that can be expressed "by using English words". Some people try "solving" paradoxes by introducing language rules allowing to avoid them. Still, on the other hand, each paradox contains its specific creative potential. For example, by formalizing the Liar's Paradox one can prove Gödel's Incompleteness Theorem (see Section 5.3). Which kind of incompleteness theorems could be derived from Berry's Paradox?

The proof below was adapted from the paper:

Panu Raatikainen. On Interpreting Chaitin's Incompleteness Theorem. *Journal of Philosophical Logic*, 1998, vol. 27, pp. 569-586 (available online).

Let us consider Turing machines (TMs) that are working without input data, and that, when halting, generate some natural number x. Such a TM can be considered as a "definition" of the number x, and thus, in this way, we can try to obtain a version of Berry's Paradox.

Let us consider an enumeration of the above-mentioned TMs:

$$TM_0, TM_1, TM_2, ..., TM_n, ..., \qquad (1)$$

such that:

a) The following predicate h(x, y, t) is computable (i.e. "recursive"):

$$h(x, y, t) = \text{"}TM_y \text{ halts in t steps and generates the number x"}.$$

b) Kleene's Fixed Point Theorem holds: for any computable (i.e. "recursive")

function f one can construct an index e such that $TM_{f(e)}$ does exactly the same that does TM_e.

According to Representation Theorem, there is a formula H(x, y, t) expressing the predicate h(x, y, t) in PA (i.e. first order arithmetic).

For the number x, if y is the minimum index such that TM_y halts and generates x, then, if you wish, you can think of y as the Kolmogorov complexity of x, and put this as K(x)=y.

The formula

$$C(x, y) = \quad \exists y_0 \exists t\left(y_0 \le y \wedge H\left(x, y_0, t\right)\right)$$

asserts that "x is generated by some TM with an index ≤y". If you wish, you may put this as K(x)≤y.

C(x, y) is a Σ_1-formula, i.e. it "expresses" an computably (i.e. recursively) enumerable predicate.

The formula ¬C(x,y) asserts that "x is not generated neither by TM_0, nor by TM_1, ..., nor by TM_y. If you wish, you may put this as K(x)>y. (¬C(x,y) is a Π_1-formula.)

Of course, for any fixed index c, the formula C(n, c) may be true only for a finite number of n-s (i.e. only for numbers generated by TM_0, TM_1, TM_2, ..., TM_c, if such numbers exist at all). This simple fact can be proved in PA:

$$\text{PA proves:} \quad \forall c \exists n_0 \forall n\left(C\left(n, c\right) \rightarrow n \le n_0\right) \quad \text{, or:}$$

$$\text{PA proves:} \quad \forall c \exists n_0 \forall n\left(n > n_0 \rightarrow \neg C\left(n, c\right)\right) \quad . \qquad (2)$$

Secondly, if for some numbers n, c, the formula C(n, c) is true, then, for any d≥c, C(n, d) is true as well. This simple fact also can be proved in PA:

$$\text{PA proves:} \quad \forall n \forall c \forall d\left(d \ge c \rightarrow \left(C\left(n, c\right) \rightarrow C\left(n, d\right)\right)\right) \quad \text{, or:}$$

$$\text{PA proves:} \quad \forall n \forall c \forall d\left(c \le d \rightarrow \left(\neg C\left(n, d\right) \rightarrow \neg C\left(n, c\right)\right)\right) \quad . \qquad (3)$$

Now, we can try modeling Berry's Paradox. Namely, let us try to define a TM which is trying to generate a number that can't be generated by a TM of this "size". I.e. let us try to define a TM_e which is trying to generate a number that can't be generated neither by TM_0, nor by TM_1, ..., nor by TM_e.

How obtain a TM_e, the definition of which refers to its index e? Of course, by applying Kleene's Fixed Point Theorem. First, we will, having an arbitrary number c, define a TM_d which is trying to generate a number n that can't be

generated neither by TM_0, nor by TM_1, ..., nor by TM_c. Here, by construction, d will be computable from c as some (i.e. recursive) function f(c). Then, by Kleene's Fixed Point Theorem, one will construct an index e such that TM_e does exactly the same that does $TM_{f(e)}$. Hence, TM_e will be trying to generate a number n that can't be generated neither by TM_0, nor by TM_1, ..., nor by TM_e.

Now, to instead of "can't be generated", we will introduce "can't be generated, according to theory T", where T is any fundamental theory (i.e. a formal theory covering first order arithmetic).

Thus, given a number c, we define the following $TM_{f(c)}$: scan, one by one, all the T-proofs, if some of these proofs proves, for some number n, that n can't be generated neither by TM_0, nor by TM_1, ..., nor by TM_c, then output this n as the result.

In other words: given a number c, we define the following $TM_{f(c)}$: scan, one by one, all the T-proofs, if some of them proves the formula $\neg C(\mathbf{n}, \mathbf{c})$ for some number n, then output this n as the result.

Now, by Kleene's Fixed Point Theorem, one can construct an index e such that TM_e does exactly the same that does $TM_{f(e)}$. Hence, TM_e scans, one by one, all the T-proofs, if some of them proves the formula $\neg C(\mathbf{n}, \mathbf{e})$ for some number n, then TM_e outputs this n as the result.

Of course, the index e depends on the theory T: $e = e_T$.

Thus, we have a particular Turing machine TM_e (depending on T). **Does TM_e halt?**

1. TM_e halts in some t steps and outputs some number n, if and only if there is a T-proof of the formula $\neg C(\mathbf{n}, \mathbf{e})$:

$$T \text{ proves: } \neg C(\mathbf{n}, \mathbf{e_T}).$$

But, simultaneously, the fact, that TM_e halts in t steps and outputs the number n, can be proved in PA:

$$PA \text{ proves: } H(\mathbf{e_T}, \mathbf{n}, \mathbf{t}).$$

Hence, also,

$$PA \text{ proves: } \exists y_0 \exists t(y_0 \leq \boldsymbol{e_T} \wedge H(\boldsymbol{n}, y_0, t)) \text{ , i.e.}$$

$$PA \text{ proves: } C(\mathbf{n}, \mathbf{e_T}).$$

Since T covers PA, then also

T proves: C(**n**, $\mathbf{e_T}$).

Thus, if TM_e halts, then T is an inconsistent theory.

2. If, otherwise, TM_e does not halt, then T proves ¬C(**n**, $\mathbf{e_T}$) for NONE of the numbers n. Is this something bad? From (2) we know that

PA proves: $\exists n_0 \forall n (n > n_0 \rightarrow \neg C(n, \boldsymbol{e_T}))$,

i.e. PA (and T) proves that ¬C(**n**, $\mathbf{e_T}$) is true for all n, except for at most a finite number of exceptions. But T cannot prove ¬C(**n**, $\mathbf{e_T}$) for NONE of the numbers n!

Thus, if we denote ¬C(x, y) by K(x, y), then we have proved, in fact, the following

Chaitin's Theorem. In the language of PA, there is a Π_1-formula K(x, y) such that:

a) PA proves: $\forall c \exists n_0 \forall n (n > n_0 \rightarrow K(n, c))$, i.e. that, for any fixed c, K(n,c) is true for all n, except for a finite number of exceptions.

b) For any fundamental formal theory T one can construct a number e_T such that if, for some number n, T proves K(**n**, $\mathbf{e_T}$), then T is inconsistent.

Corollary 1. There is a Π_1-formula K(x,y) such that PA proves $\forall c \exists n_0 \forall n (n > n_0 \rightarrow K(n, c))$, but for any consistent fundamental formal theory T one can construct a number e_T such that T can prove K(**n,** $\mathbf{e_T}$) for none of the numbers n.

Since, for infinitely many numbers i, TM_i does not halt, the formula K(**n**, **n**) must be true for infinitely many numbers n. This simple fact can be proved in PA:

PA proves: $\forall m \exists n (n > m \wedge K(n, n))$.

But, if T is consistent, it can prove K(**n, n**) only for a finite number of n-s. Indeed, T cannot prove K(**n, n**), if $n \geq e_T$. Hence,

Corollary 2. There is a Π_1-formula $K_1(x)$ such that PA proves that $K_1(n)$ is true for infinitely many n-s, but any consistent fundamental theory T can prove $K_1(\mathbf{n})$ only for a finite number of n-s.

Or, if you wish to put ¬C(x, y) as K(x)>y, then you may have a more traditional formulation of

Chaitin's Theorem. In the language of PA, there is a Π_1-formula K(x)>y such that:

a) PA proves: $\forall c \exists n_0 \forall n (n > n_0 \rightarrow K(n) > c)$, i.e. that, for any fixed c, K(n)>c for all n, except for a finite number of exceptions.

b) For any fundamental formal theory T one can construct a number e_T such that if, for some number n, T proves K(**n**)>$\mathbf{e_T}$, then T is inconsistent.

Corollary 1. There is a Π_1-formula K(x)>y such that PA proves $\forall c \exists n_0 \forall n (n > n_0 \rightarrow K(n) > c)$, but for any consistent fundamental formal theory T one can construct a number e_T such that T can prove K(**n**)>$\mathbf{e_T}$ for none of the numbers n.

Corollary 2. There is a Π_1-formula K(x)>x such that PA proves that K(n)>n is true for infinitely many n-s, but any consistent fundamental theory T proves K(n)>n only for a finite number of n-s. If we wish to interpret K(n)>n as "n is a random bit-string", then we can obtain the following beautiful thesis: **PA proves that there are infinitely many random bit-strings, but any consistent fundamental theory T can prove the randomness of only a finite number of concrete bit-strings.**

In (almost?) all the other texts, Chaitin's Theorem is formulated by assuming the so-called **"semantical soundness"** of T, i.e. by assuming (somewhat irresponsibly) that T proves only "true" formulas of the language of PA (whatever it means). Then, first, the formula

$$\forall c \exists n_0 \forall n (n > n_0 \rightarrow K(n) > c)$$

is "obviously, true", and a) can be omitted. Secondly, since T is "obviously, consistent", then b) can be put simply as: T does not prove K(**n**)>$\mathbf{e_T}$ for none of n. In this way we obtain almost one of Chaitin's own formulations of his theorem:

Chaitin's Theorem. For any semantically sound fundamental formal theory T one can construct a number e_T such that, for all numbers n, T does not prove that K(**n**)>$\mathbf{e_T}$ (while this formula is true for all n, except for a finite number of exceptions).

It follows from Chaitin's original proof that we can have: $e_T = A_T+B$, where A_T is the Kolmogorov complexity of the **formulation** of theory T (or, of its axioms, if rules of inference are universally fixed), and B – a universal constant, i.e. B does not depend on T.

I.e., in a sense, **the possibility of proving the complexity of natural**

numbers by using some theory T, is limited by the complexity of the formulation of T itself.

In which sense is Chaitin's Theorem stronger than Gödel's Incompleteness Theorem? Try comparing yourself:

Gödel's Theorem says that, for any fundamental formal theory T, there is a Π_1-formula G_T such that, if some theory T_1 proves the consistency of T, then T_1 proves G_T, but T does not prove G_T.

Chaitin's Theorem says that there is a Π_1-formula C(x) such that PA proves that C(n) is true for infinitely many n-s, but any consistent fundamental formal theory T can prove C(**n**) only for a finite number of n-s.

Gödel's Theorem is used to make a very general prediction: developing any sufficiently strong mathematical theory, we will run either into contradictions, or into unsolvable problems. And this general prediction was confirmed "experimentally" many times since 1963, when Paul Cohen proved that, if set theory is consistent, then it cannot solve the Continuum Problem.

As shown in the paper:

Michiel van Lambalgen. Algorithmic information theory. *Journal of Symbolic Logic*, 1989, 54 (4), pp. 1389-1400 (available online)

(see also the above Raatikainen's paper), the phenomenon discovered in Chaitin's Theorem, **cannot be used for measuring the "mathematical power" of theories**.

One can try to define the "characteristic constant" c_T of theory T as follows:

c_T = "the least e such that, for all numbers n, T does not prove K(**n**)>**e**" =
= 1+ "the maximum e such that, for some number n, T proves K(**n**)>**e**".

By Chaitin's Theorem, if T is a consistent fundamental theory, then $c_T \leq e_T$, i.e. for consistent theories, c_T is always some finite number. We know, as a consequence of Gödel's Second Theorem, that set theory ZF is "mathematically more powerful" than first order arithmetic PA. Namely, ZF proves some arithmetical theorems that PA cannot prove (if PA is consistent). But, as noted in Lambalgen's paper: "**... we do not know, whether $c_{PA}<c_{ZF}$, and, worse, we even have no idea how to establish results of this sort.**" (p. 1395).

If we would define the **complexity of some assertion** as the Kolmogorov complexity of **its formulation** (i.e. of the corresponding formula), then the complexity of theorems provable in some theory T, will NOT be limited by the complexity of the formulation of T. Indeed, for any limit c, there is only a

finite number of formulas having Kolmogorov complexity up to c, but T proves an infinite number of theorems. Hence, the following thesis cannot be true: "... if one has ten pounds of axioms and a twenty-pound theorem, then that theorem cannot be derived from those axioms". But it may become true, if we restrict our assertions to the specific kind of ones used in Chaitin's Theorem, for example, to the assertions of the form K(n)>n. Indeed, while PA proves that K(n)>n is true for infinitely many numbers n, a consistent theory T can prove K(**n**)>**n** only for n-s, limited by the complexity of the formulation of T.

Note. More about other attempts to produce incompleteness theorems by modeling various kinds of paradoxes (P.Vopenka 1966, J.L.Krivine 1972, J.Boolos 1989, M.Kikuchi 1994) see:

Cezary Cieslinski. Heterologicality and Incompleteness. *Mathematical Logic Quaterly*, 2002, vol. 48, N 1, pp. 105-110.

Appendix 1. About Model Theory

Some of the widespread platonist superstitions were derived from other important results of mathematical logic (omitted in the main text of this book): Gödel's completeness theorem for predicate calculus, Löwenheim-Skolem theorem, the categoricity theorem of second order Peano axioms. In this short Appendix 1 I will discuss these results and their methodological consequences (or lack of them).

All these results have been obtained by means of the so-called **model theory**. This is a very specific approach to investigation of formal theories as mathematical objects. Model theory is using the full power of set theory. Its results and proofs can be formalized in the set theory ZFC. **Model theory is investigation of formal theories in the metatheory ZFC.**

Paul Bernays, in 1958: "As Bernays remarks, **syntax is a branch of number theory and semantics the one of set theory."**

See p. 470 of

Hao Wang. EIGHTY YEARS OF FOUNDATIONAL STUDIES. *Dialectica,* Vol. 12, Issue 3-4, pp. 466-497, December 1958 (available online at Blackwell Synergy).

The main structures of model theory are **interpretations**. Let L be the language of some (first order) formal theory containing constant letters c_1, ..., c_k, function letters f_1, ..., f_m, and predicate letters p_1, ..., p_n. An interpretation J of the language L consists of the following objects:

a) a non-empty set D_J – the domain of interpretation (it will serve as the range of variables),

b) a mapping int_J that assigns:

− with each constant letter c_i – a member $int_J(c_i)$ of the domain D_J,

− with each function letter f_i – a function $int_J(f_i)$ from $D_J \times ... \times D_J$ into D_J (of course, $int_J(f_i)$ has the same number of arguments as f_i),

− with each predicate letter p_i – a predicate $int_J(p_i)$ on D_J, i.e. a subset of $D_J \times ... \times D_J$ (of course, $int_J(p_i)$ has the same number of arguments as p_i).

As an example, let us consider the so-called **standard interpretation** S of Peano arithmetic PA:

a) The domain is D_S = {0, 1, 2, ...} (the set w in terms of ZF).

b) The mapping int_S assigns: with the constant 0 – the number 0 (the empty set o), with the constant 1 – the number 1 (the set {o}), with the function letter "+" – the function x+y (addition of natural numbers), with the function letter "*" – the function x·y (multiplication of natural numbers), with the predicate letter "=" – the predicate x=y (equality of natural numbers).

Having an interpretation J of the language L, we can define the notion of **true formula** (more precisely – the notion of formulas that are true under the interpretation J).

As the first step, **terms** of the language L are interpreted as members of D_J or functions over D_J. Terms are defined as constant letters, or variable letters, or their combinations by means of function letters. The term c_i is interpreted as the member $int_J(c_i)$ of D_J. The variable x_i is interpreted as the function $X_i(x_i) = x_i$. And, if $t = f_i(t_1, ..., t_q)$, then $int_J(t)$ is defined as the function obtained by substituting of functions $int_J(t_1)$, ..., $int_J(t_q)$ into the function $int_J(f_i)$. For example, the standard interpretation of the term (x+y+1)*(x+y+1) is the function $(x+y+1)^2$.

As the next step, the notion of **true atomic formulas** is defined. Of course, if a formula contains variables (as, for example, the formula x=1), then its "truth value" must be defined for each combination of values of these variables. Thus, to obtain the truth value of the formula $p_i(t_1, ..., t_q)$ for some fixed values of the variables contained in t_1, .., t_q, we must first "compute" the values of these terms, and then substitute these values into the predicate $int_J(p_i)$.

Note. The equality letter "=" is always interpreted in the standard way – as the equality of members of D_J.

And finally, we can "define" the notion of **true compound formulas** of the language L under the interpretation J (of course, for a fixed combination of values of their free variables):

a) Truth-values of the formulas ¬B, B∧C, B∨C and B→C can be computed from the truth values of B and C.

b) Formula ∀xB(x) is true, if and only if B(c) is true for all members c of the domain D_J.

c) Formula ∃xB(x) is true, if and only if there is a member c of the domain D_J such that B(c) is true.

Note that for an infinite domain D_J this notion of truth is extremely **non-constructive**: to establish, for example, truth-value of the formula $\forall xB(x)$, we must check truth of B(c) for infinitely many values of c. The "degree of constructivity" of the formulas like $\forall x\exists yC(x,y)$, $\forall x\exists y\forall zD(x,y,z)$ etc. is even less... (Compare my "critique" of the notion of true arithmetical formula in Section 3.1).

Let us say that a formula of the language L is true under the interpretation J, if and only if this formula is true for all combinations of values of its free variables.

Some formulas are true for all interpretations, for example:

$$(B\rightarrow C)\rightarrow((C\rightarrow D)\rightarrow(B\rightarrow D)),$$

$$\forall x(C\rightarrow D(x))\rightarrow(C\rightarrow\forall xD(x)),$$

where C does not contain x. Such formulas are called **logically valid** (because they are true independently of the interpretation of their "meaning"). Note that the notion of logically valid formula is **doubly non-constructive** in the sense that the universal quantifier "for all interpretations" is added to the (already) non-constructive definition of (simply) true formula.

See Detlovs, Podnieks [2000], Section 1.3 for one of the possible lists of **axioms and rules of inference of the classical logic** (it is called also “first order logic”).

You could check easily that: a) all the axioms of the classical logic are logically valid, b) the logical rules of inference allow to prove (from logically valid formulas) only logically valid formulas. Hence, in this way only logically valid formulas can be proved in the classical logic. Still, is our list of logical axioms complete in the sense that all logically valid formulas can be proved? The answer is "yes" – as Kurt Gödel established in 1929 (i.e. just a year BEFORE...):

K. Gödel. Die Vollständigkeit der Axiome des logischen Funktionenkalküls. "Monatshefte für Mathematik und Physik", 1930, Vol.37, pp.349-360.

Gödel's Completeness Theorem. A formula (in any first order language) is logically valid, if and only if it can be proved in the classical logic.

Gödel's initial proof was simplified in 1947, when Leon Henkin presented in his Ph.D. thesis a new proof of the so-called Model Existence Theorem (see below). The result was published in 1949:

L. Henkin. The completeness of the first-order functional calculus. "J. Symbolic Logic", 1949, vol.14, pp.159-166.

See also Henkin's later account of his discovery:

L. Henkin. The discovery of my completeness proofs. "The Bulletin of Symbolic Logic",

1996, vol.2, N2, pp.127-158.

An even simpler version Henkin's proof was found independently and almost simultaneously by Gisbert Hasenjäger, however, when publishing, he acknowledged Henkin's priority:

G. Hasenjäger. Eine Bemerkung zu Henkin's Beweis fuer die Vollständigkeit des Prädikatenkalkuels der ersten Stufe. "J. Symbolic Logic", 1953, vol.18, pp.42-48.

If T is a formal theory, and J is an interpretation of its language, then (traditionally) J is called a **model of** T, if and only if J makes true all axioms (and hence, all theorems) of T. The term "model of a theory" may seem somewhat strange: in "normal" branches of science theories serve as basis for building models of natural phenomena, technical devices etc. But only the term is strange ("upside down") here, the process is the same as in "normal" branches of science: formal theories "generate" their models, and these models can be used for modeling natural phenomena, technical devices etc.

Model Existence Theorem. If a (first order) formal theory T is consistent (in the sense that, by using the classical logic, one cannot derive contradictions from the axioms of T), then T has a finite or countable model (i.e. a model in which the domain is finite or countable).

This theorem solved a serious mental problem of anti-formalists. They thought that mere consistency of a theory (in the syntactic sense of the word – as the lack of contradictions) is not sufficient to regard a theory as a "meaningful" one. Model Existence Theorem says that (syntactic!) consistency of a theory **is** sufficient to regard it as "meaningful": if a theory does not contain contradictions, then it describes at least some kind of "mathematical reality". Indeed, even Euclidean geometry is "meaningless" – because it does not describe 100% correctly the spacial properties of the Universe. It's your problem, not Euclid's – use another theory.

See Mendelson [1997] for an elegant proof of the Model Existence Theorem. Or, do the Exercise A.1.1 below.

Proof of the Completeness Theorem. Of course, the only non-trivial part of the work is proving that each logically valid formula in the (first order) language L can be proved by using the logical axioms and inference rules.

Let us assume that some formula F in the language L is logically valid, yet it cannot be proved by using our axioms and rules. Let us consider the theory T in the language L which has (besides the logical axioms) only one specific axiom – the formula ¬F. Since F cannot be derived from logical axioms, T is a consistent theory. Hence, by Model Existence Theorem, T has a model, i.e. an interpretation J that makes all its axioms true. Under this interpretation the formula ¬F (as an axiom of T) is true. On the other hand, since F is logically valid, it is true under all interpretations, i.e. it is true also under the

interpretation J. Hence, formulas F and ¬F both are true under J. This is impossible; hence, F must be provable from logical axioms. Q.E.D.

Such a simple proof seems almost impossible! We are proving that the logical axioms and rules of inference are strong enough, but where come these axioms in? They do come in – in the proof of Model Existence Theorem: this theorem says that if some formal theory T does not have models, then the logical axioms and rules of inference are strong enough to derive a contradiction from the axioms of T.

Corollary. In any first order language the set of all logically valid formulas is computably (recursively) enumerable. I.e. given a language L, we can write a computer program that (working *ad infinitum*) prints out all the logically valid formulas of L.

This makes Gödel's completeness theorem very significant: it shows that the "doubly non-constructive" notion of logically valid formula is at least 50% constructive!

Still, unfortunately, this notion is not 100% constructive. In 1936, Alonzo Church proved that at least some first order languages do not allow an algorithm determining, is a given formula logically valid or not (i.e. an algorithm solving the famous Entscheidungsproblem – decision problem):

A. Church. A note on the Entscheidungsproblem. "Journal of Symb. Logic", 1936, vol.1, pp.40-41.

After this, Laszlo Kalmar proved that, if a first order language contains at least one binary predicate letter, then it does not allow an algorithm determining, is a given formula logically valid or not. Thus, none of the serious first order languages allows such an algorithm (languages of PA and ZF included):

L. Kalmar. Die Zurückführung des Entscheidungsproblems auf den Fall von Formeln mit einer einzigen, binären Funktionsvariablen. "Compositio Math.", 1936, Vol.4, pp.137-144.

For details, see Mendelson [1997]. Sometimes, this fact (the 50% constructiveness of the notion of the logical validity) is expressed a follows: the logical validity of first order formulas is **semi-decidable**.

Initially, Model Existence theorem was proved in a weaker form in 1915 (by Leopold Löwenheim) and 1919 (by Thoralf Skolem): if a first order theory has a model, then it has a finite or countable model (the famous **Löwenheim-Skolem theorem**). Proof (1929): if T has a model, then T is consistent, i.e. T has a finite or countable model.

L. Löwenheim. Über Möglichkeiten im Relativkalkül. "Mathematische Annalen", 1915, Vol.76, pp.447-470.

T. Skolem. Logisch-kombinatorische Untersuchungen über Erfüllbarkeit oder Beweisbarkeit mathematischer Sätze nebst einem Theoreme über dichte Mengen. "Skrifter utgit av Videnskapsselskapet in Kristiania, I, Mat.-Nat. Kl.", 1919, N4, pp.1-36.

Model Existence theorem is steadily provoking the so-called **Skolem's paradox**. Indeed, in ZF we can prove existence of uncountable sets. Still, according to Model Existence theorem, if ZF is consistent, then there is a countable model of ZF. I.e. ZF proves existence of uncountable sets, yet it has a countable model! Is this possible? Does it mean that ZF is inconsistent? Platonists could say even more: any consistent axiomatic set theory has countable models, hence, no axiom system can represent the "intended" set theory (i.e. "the" platonist "true world of sets") adequately.

For a formalist, Skolem's paradox is not a paradox at all. I would rather call it Skolem's effect – like as photo-effect, it is simply a **striking phenomenon**. Indeed, let J be a countable model of ZF. In ZF we can prove that the set r of all real numbers is uncountable, i.e.

$$\neg\exists f \text{ (f is 1-1 function from r into w)}, \qquad (1)$$

where w is the set of all natural numbers. What is the meaning of this theorem in the countable model J? Interpretations of r and w are subsets of the domain D_J, i.e. they both are countable sets, i.e.

$$\exists f \text{ (f is 1-1 function from } r_J \text{ into } w_J). \qquad (2)$$

Interpretation of (1) in J is

$$\neg\exists f(\ f \in D_J \ \text{ and f is 1-1 function from } r_J \text{ into } w_J).$$

Hence, the mapping f of (2) does exist, yet it exists **outside the model** J! Do you think that f of (2) "must" be located in the model? Why? If you are living (as an "internal observer") within the model J, the set r_J seems uncountable to you (because you cannot find a 1-1 function from r_J into w_J in your world J). Still, for me (an an "external observer") your uncountable r_J is countable – in my world I have a 1-1 function from r_J into w_J!

Hence, indeed, Skolem's paradox represents simply a striking phenomenon. It is worth of knowing, yet there is no danger in it.

Another platonist superstition is connected with the so-called **categoricity theorem** of second order Peano axioms. By second order Peano axioms I mean the initial variant of axioms of arithmetic proposed by R. Dedekind. Modern version of this system is represented in the axioms P1, P2 and P3 of Section 3.1. The notion of models for these axioms can be discussed comfortably within ZF as a metatheory. Namely, any such model (according to our general definition above in this Appendix) is a triple (v, q, s), where v is a set (its members represent "natural numbers" of the model), q is a member of v (it represents the number 0), and s(x) is a function from v into v (it represents the function x+1). A triple (v, q, s) is a model of Peano axioms P1, P2, P3, if

and only if:

P1: ¬(s(x)=q) for all $x \in v$.

P2: If ¬(x=y), then ¬(s(x)=s(y)) for all $x, y \in v$.

P3: If $u \subseteq v$, $q \in u$, and $\forall y(y \in u \rightarrow s(y) \in u)$, then u=v.

Of course, the set w of all "set-theoretical" natural numbers (see Section 2.3), together with the empty set (representing the number 0) and the function $x \cup \{x\}$ (representing s(x)) is a model of Peano axioms. This model is called traditionally the **standard model of arithmetic**. Let us say, that some other model (v, q, s) is isomorphic with the standard model, if and only if there is a 1-1 function f from w onto v ("onto v" means that range(f)=v) such that:

a) $f(o)=q$;

b) $f(n \cup \{n\}) = s(f(n))$ for all $n \in \omega$.

The following theorem can be proved in ZF:

Categoricity Theorem. Any model of second order Peano axioms is isomorphic with the standard model.

This theorem has been first proved by R.Dedekind (the author of Peano axioms, see Section 3.1) in his remarkable book:

R. Dedekind. Was sind und was sollen die Zahlen. Braunschweig, 1888.

Proof. Assuming that the axioms P_1, P_2, P_3 are true in the model (v, q, s), let us define by recursion the following function from w into v:

f(o) = q, f({o}) = s(q), f({o,{o}}) = s(s(q)), ..., f(n∪{n}) = s(f(n)), ...

Let us prove that f is the required isomorphism.

a) $f(o)=q$ by definition.

b) $f(n \cup \{n\}) = s(f(n))$ for all $n \in w$ – also by definition.

c) Let us show that range(f)=v. Of course, $q \in range(f)$, and if some $x \in range(f)$ (i.e. x=f(n) for some n), then $s(x)=s(f(n))=f(n \cup \{n\})$, i.e. s(x) also is in range(f). Hence, by P_3 (this axiom is true in the model (v, q, s)) we obtain that range(f)=v.

d) Let us show that f is 1-1 function, i.e. let us prove that, if f(m)=f(n), then m=n. We must consider three cases:

d1) m=n=o. Q.E.D.

d2) m=o, n>o. Then f(m)=q, but f(n)=s(f(n−1)), i.e. f(n) is not q by the axiom P_1. Q.E.D.

d3) m>o, n>o. Then f(m)=s(f(m−1))=f(n)=s(f(n−1)), and by the axiom P_2 we

obtain that f(m−1)=f(n−1). Let us repeat this argument enough times, and we will have the case d1) or d2 at the end. Q.E.D.

Q.E.D.

Thus, it seems that the second order Peano axioms contain an "unambiguous definition" of the structure of their models. For this reason, sometimes, the Categoricity Theorem is considered as an additional evidence in favor of the platonist opinion that natural numbers exist as a unique specific "world" where each definite assertion "must be" either true or false. Still, note that Categoricity Theorem is a theorem of ZF. How could a theorem of ZF have "super-natural" consequences?

Exercise A.1.1. (for smart students). Prove Model Existence theorem by using the following smart ideas (see Mendelson [1997]). Let T be a consistent theory. We must build a model of T, what kind of "bricks" should we use for this "building"? **Idea #1:** let us use language constant letters! So, let us add to the language of T an infinite set of new constant letters b_1, b_2, b_3, ... (and modify the logical axioms accordingly). Prove that this extended theory T_0 is consistent. The model we are building must contain all "objects" whose existence can be proved in T_0. **Idea #2:** for each formula F of T_0 having exactly one free variable (for example, x) let us add to the theory T_0 an axiom $\exists xF(x)\rightarrow F(b_i)$, where the constant b_i is unique for each F. If T_0 proves $\exists xF(x)$, then this b_i will represent in our model the "object" x having the property F. Prove that this extended theory T_1 is consistent. **Idea #3:** prove the (non-constructive) Lindenbaum's lemma: any consistent theory has a consistent complete extension (the axiom set of the extension may not be computably solvable). After this, extend T_1 to a consistent complete theory T_2. **Idea #4:** let us take as the domain of the interpretation M the set of all those terms of T_0 that do not contain variables. And let us interpret a function letter f as the "syntactic constructor function" f', i.e. let define the value $f'(t_1, ..., t_n)$ simply as the character string "$f(t_1, ..., t_n)$". Finally, let us interpret a predicate letter p as the relation p' such that $p'(t_1, ..., t_n)$ is true in M, if and only if T_2 proves $p'(t_1, ..., t_n)$. To complete the proof, prove that an arbitrary formula G is true in M, if and only if T_2 proves G. Hence; all theorems of the initial theory T are true in M.

Adolf Lindenbaum (1904-1941). His wife Janina Hosiasson-Lindenbaum (1899-1942), some more details in EiGENSiNN philosophiestudentische Zeitung, Juli 2006.

Appendix 2. Around Ramsey's Theorem

The attitude of many working mathematicians to Gödel's Incompleteness Theorem is generally indifferent. Some methodological basis for such a position is given in the following quote from Parikh [1971]:

"... Thus exponentiation is not only a means for denoting "large numbers" but also the means for introducing "nonmathematical" questions into number theory. Why do we say "nonmathematical"? Because consider Gödel's formula A which says "I am not provable". Now this formula does express properties of N, since it can be written with quantifiers and connectives. However to see that A is true but not provable, we do not use properties of N, but properties of the intuitive notion "provable". Thus to say that A is a statement about numbers is like arguing that human behaviour is a problem of physics since human beings are physical entities. Even if such an assertion is true, it is very theoretical and not very useful."

Since human beings are physical entities, I do not believe that there are ghosts, I think that astrology is nonsense, etc. Hence, for me, the above assertion is very practical and very useful.

So is Gödel's Incompleteness Theorem. For me, this theorem predicts that a fundamental mathematical theory cannot be perfect: while developing any such theory we will inevitably come either into contradictions, or into unsolvable problems. Is such a prediction practical? Some 30 years after Gödel's proof, in 1963 P.Cohen proved that if the set theory ZFC is consistent, then this theory is not able to solve Cantor's Continuum Problem. If you prefer calling Gödel's Theorem "very theoretical", then Cohen's result must be acknowledged as its "empirical confirmation". Since 1963 many classical problems of set theory were proved to be unsolvable, so we can speak about "massive empirical confirmation" of Gödel's theoretical prediction. Can we exclude that also some classical problems of number theory (for example, the twin prime conjecture) will be proved unsolvable?

Perhaps, Laurence Kirby, Jeff Paris and Leo Harrington made the first steps in this direction shortly before 1977. They proved that an extension of the so-called Finite Ramsey's theorem (a statement of discrete combinatorics that can be proved in set theory) cannot be proved in first order arithmetic (PA). Thus, for the first time, it was established that a relatively interesting assertion about natural numbers is unprovable when we are using the elementary (i.e. first

order) notion of natural numbers. Still, using the extended "post-Cantor" (i.e. second order) notion of natural numbers we can prove this assertion.

In the 1982 paper

L. Kirby and J. Paris. Accessible independence results for Peano arithmetic. *Bulletin London Mathematical Society*, 4:285-293, 1982

two similar and even more impressing results were proved:

a) About the so-called Goodstein's Sequences (from 1944) $G_k(n)$ (n is the index of the sequence, k – the index of its member). Despite the apparent extremely fast growth of $G_k(n)$ as a function of k, one can prove in ZF for all n that $G_k(n)$ will stop growing, moreover, $G_k(n)= 0$ for all sufficiently large k. But this can't be proved in PA.

Reuben Louis Goodstein

R. Goodstein. On the restricted ordinal theorem. *Journal of Symbolic Logic*, Vol. 9 (1944), pp. 33-41.

b) About the so-called "Battle of Hydra and Hercules" – read the above original paper, or:

Nachum Dershowitz and Georg Moser. The hydra battle revisited. In: *Rewriting Computation and Proof, Lecture Notes in Computer Science*, Vol. 4600, Springer-Verlag, 2007, pp.1-27.

The Infinite Ramsey's Theorem

Frank P. Ramsey published this theorem in 1930:

F. P. Ramsey. On a problem of formal logic. "Proc. London Math. Soc.", 1930, vol.30, pp.264-285.

In a sense, Ramsey's Theorem is a generalization of the well known and very simple the so-called **Pigeon Hole Principle** which states that, if M is an infinite set, and each member of it is marked by one of r colors, then at least one of the colors is assigned to an infinite subset of members.

As the next step, let us consider an **infinite complete graph**, i.e. a graph, where each pair of nodes is connected by an edge. Imagine, each edge of this graph is marked by one of r colors. Then, by Ramsey's Theorem, there is an i**nfinite "monochrome" complete subgraph**, i.e. a subgraph, all the edges of which are marked by the same color.

Infinite Ramsey's theorem. Suppose, M is an **infinite** set, and e, r are positive integers. Imagine that each e-member subset of M is marked by one of r colors. Then there is an **infinite** subset of M such that all its e-member subsets are marked by the same color.

Proof (in ZFC, i.e. by using the Axiom of Choice). See

R. L. Graham. Rudiments of Ramsey theory. AMS, Providence, 1981 (Russian translation available).

1. For **e=1** the proof is obvious. Indeed, if M is an infinite set, and each member of it is marked by one of r colors, then at least one of the colors is assigned to an infinite subset of members. Q.E.D.

2. For **e=2** the proof is straightforward. Here, M is an infinite set, and each pair of its members {a, b} is marked by one of r colors. Let us select a member b_0 of M, and consider all pairs $\{b_0, b\}$ where $b \in M - \{b_0\}$. There is a color c_0 such that the set

$$M_1 = \{ \ b \in M \ | \{b_0, b\} \text{ is marked by } c_0\}$$

is infinite. As the next step, let us a select member b_1 of M_1, and consider all pairs $\{b_1, b\}$ where $b \in M_1 - \{b_1\}$. There is a color c_1 such that the set

$$M_2 = \{ \ b \in M_1 - \{b_1\} \ | \{b_1, b\} \text{ is marked by } c_1\}$$

is infinite. Etc.

As the result, we obtain three infinite sequences:

− the sequence of members of M: $b_0, b_1, b_2, ...$,

− the sequence of colors: $c_0, c_1, c_2, \ldots$,

− the sequence of subsets: $M = M_0 \supset M_1 \supset M_2 \supset ...$,

where each $b_i \in M_i - M_{i+1}$, and all pairs $\{b_i, b\}$ with $b \in M_{i+1}$ are marked by the color c_i.

One of the colors (let us denote it by c) occurs an infinite number of times in this sequence: $c = c_i$ for $i = i_0, i_1, i_2, ...$ The set of corresponding members:

$$H = \{ b_i \mid i = i_0, i_1, i_2, ...\}$$

is an infinite subset of M, and all pairs {a, b} with $a, b \in H$ are marked by the same color c. Indeed, if $a = b_i$ and $b = b_j$, where $i = i_k$, $j = i_m$, and $k<m$, then $a \in M_i - M_{i+1}$, and $b \in M_{i+1}$, hence, {a, b} is marked by the color c_i, i.e. by c. Q.E.D.

3) For **e≥3** the proof is by induction, i.e. by using the following

Lemma. Suppose, M is an infinite set, and e, r are positive integers. Imagine that each e-member subset of M is marked by one of r colors. If the Infinite Ramsey's theorem is true for e−1, then for each infinite subset M' of M and

each member b' of M' there is an infinite subset H' of M'−{b'} such that all e-member sets consisting of b' and e−1 members of H' are marked by the same color.

Proof of the Lemma. Let us derive from the "r-coloring" of e-member subsets of M the following "r-coloring" of (e−1)-member subsets of M' − {b'}:

Mark $\{x_1, ..., x_{e-1}\}$ by the color c, if and only if $\{b', x_1, ..., x_{e-1}\}$ is marked by the color c.

From the Infinite Ramsey's theorem for e−1 we obtain an infinite subset H' of M' − {b'} such that all its (e−1)-member subsets are marked by the same color. Now add b' to each of these subsets. Q.E.D.

Having this Lemma we can derive Ramsey's theorem for e from Ramsey's theorem for e−1 by repeating the argument we used for e=2. Indeed, our Lemma allows obtaining an infinite subset M_{i+1} of $M_i - \{b_i\}$ such that all e-member subsets of $M_{i+1} \cup \{b_i\}$ containing b_i are marked by the same color (denoted by c_i). Q.E.D.

Our formulation and proof of the Infinite Ramsey's theorem belong to the set theory ZFC. The language of first order arithmetic (PA) does not allow discussing arbitrary infinite sets, i.e. in PA we cannot even formulate this version of Ramsey's theorem.

The Finite Ramsey's Theorem

The following finite version of Ramsey's theorem can be both formulated and proved in PA. Having an **infinite** set M we were searching for an infinite "single color" subset H. Now, dealing with a **finite** set M we are interested in the following question: **how large** must be the set M to have "single color" subsets with at least k members?

Let us denote by |M| the cardinality (i.e. the number of members) of M.

Finite Ramsey's theorem. There is a computable function R(e, r, k) such that for all positive integers e, r, k and each finite set M the following holds: if $|M| \geq R(e, r, k)$, and each e-member subset of M is marked by one of r colors, then there is a subset H of M such that |H|=k, and all e-member subsets of H are marked by the same color.

Proof (in PA). 1) For **r=1** the proof is obvious: we can take R(e, 1, k) = k.

2) Now let us consider the case **r=2**, when e-member subsets of M are marked by two colors. Surprisingly, the following generalization of the theorem is easier to prove: there is a computable function $R'(e, r, k_1, k_2)$ such that if |M|

$\geq R'(e, 2, k_1, k_2)$, then there is either a subset H_1 of M such that $|H_1|=k_1$, and all e-member subsets of H_1 are marked by the **first** color, or a subset H_2 such that $|H_2|=k_2$, and all e-member subsets of H_2 are marked by the **second** color.

The proof is by induction from e−1, (e, k_1-1, k_2), and (e, k_1, k_2-1) to (e, k_1, k_2).

Induction base. For e=1 we can take $R'(1, 2, k_1, k_2) = k_1+k_2$. Indeed, in this case members of M themselves are marked by using two colors.

For the minimum k_1, i.e. $k_1=e$ we can take $R'(e, 2, e, k_2) = k_2$ (where $k_2 \geq e$). Indeed, if $|M| \geq k_2$, and there is an e-member subset x marked by the first color, then we can take $H_1 = x$. If there are no such subsets, then all e-member subsets of M are marked by the second color, and we can take $H_2 = M$.

For the minimum k_2, i.e. $k_2=e$ we can take $R'(e, 2, k_1, e) = k_1$. The proof is identical.

Induction step. Let $k_1, k_2 \geq e$. Let us show that we can take

$$R'(e, 2, k_1, k_2) = 1+R'(e-1, 2, R'(e, 2, k_1-1, k_2), R'(e, 2, k_1, k_2-1)).$$

Indeed, suppose $|M| \geq R'(e, 2, k_1, k_2)$, select a member b of M, and consider all e-member subsets of M that contain b: $\{b, x_1, ..., x_{e-1}\}$. Each of these subsets is marked either by the first, or by the second color. Let us define the following "2-coloring" of (e−1)-member subsets of $M-\{b\}$ (i = 1, 2):

$\{x_1, ..., x_{e-1}\}$ is marked by i-th color,
if and only if $\{b, x_1, ..., x_{e-1}\}$ is marked by i-th color.

Since $|M - \{b\}| \geq R'(e-1, 2, T_1, T_2)$, where $T_1 = R'(e, 2, k_1-1, k_2)$, and $T_2 = R'(e, 2, k_1, k_2-1)$, then by our modified theorem for e−1 we obtain a subset M' of $M - \{b\}$ such that:

a) Either $|M'| = T_1$ and all (e−1)-member subsets of M' are marked by the first color.

b) Or $|M'| = T_2$ and all (e−1)-member subsets of M' are marked by the second color.

In the case a), for all subsets $\{x_1, ..., x_{e-1}\}$ of M' the e-member set $\{b, x_1, ..., x_{e-1}\}$ is marked by the first color. Since $|M'| = T1 = R'(e, 2, k_1-1, k_2)$, by our modified theorem for (e, k_1-1, k_2) we obtain a subset H' of M' such that:

a1) Either $|H'| = k_1 - 1$ and all e-member subsets of H' are marked by the first color. Then for the case (e, k_1, k_2) we can take $H = H' \cup \{b\}$.

a2) Or $|H'| = k_2$ and all e-member subsets of H' are marked by the second color. Then for the case (e, k_1, k_2) we can take $H = H'$.

The proof for the case b) is similar.

To complete the case r=2 of the Finite Ramsey's theorem we can take

$$R(e, 2, k) = R'(e, 2, k, k).$$

Q.E.D. for r=2.

3) The case **r>2** we will prove by induction, namely by showing that we can take

$$R(e, r, k) = R(e, 2, R(e, r-1, k)).$$

Indeed, assume that $|M| \geq R(e, r, k)$ and all e-member subsets of M are marked by using r colors. To reduce the situation to the case r=2 let us "merge" the second and all the following colors (i.e. except the first one). Then, by the case r=2 we obtain a subset M' of M such that $|M'| = R(e, r-1, k)$ and:

a) Either all e-member subsets of M' are marked by the first color.

b) Or all e-member subsets of M' are marked by the second (i.e. "merged") color.

In the case a), since $R(e, r-1, k) \geq k$, we obtain immediately a subset H of M' such that $|H| = k$ and all e-member subsets of H are marked by the first color. Q.E.D.

In the case b) we have an "(r−1)-coloring" of all e-member subsets of M'. Since $|M'| = R(e, r-1, k)$, we have the case r−1 of the Finite Ramsey's theorem that is supposed to be true, i.e. there is a subset H of M' such that $|H| = k$ and all e-member subsets of H are marked by the same color. Q.E.D.

Q.E.D. for the entire Finite Ramsey's theorem.

It may seem that the Finite Ramsey's theorem is discussing arbitrary finite sets, not natural numbers. Still, since this theorem does not involve properties of members of finite sets, we can simply replace these members by natural numbers. Each finite set of natural numbers $\{n_1, ..., n_k\}$ we can represent by two numbers (b, c) (we could use, for example, Gödel's β-function, see Section 3.3):

$$\beta(b, c, 0) = k, \beta(b, c, 1) = n_1, ..., \beta(b, c, k) = n_k.$$

In this way the Finite Ramsey's theorem can be formulated in the language of

PA, and our very elementary proof of it can be converted into a formal proof in PA.

The Extended Finite Ramsey's Theorem

Now we have two extreme versions of Ramsey's theorem:

a) The infinite version that can be neither formulated, nor proved in PA, yet it can be both formulated and proved in ZFC.

b) The finite version that can be both formulated and proved in PA.

In 1977 an intermediate version of Ramsey's theorem was discovered (= invented) that can be formulated in PA, and can be proved in ZFC, yet not in PA (if PA is consistent).

L. Kirby, J. Paris. Initial segments of models of Peano's axioms. "Proceedings of the Bierutowice Conference 1976", Springer, Berlin, 1979.

J. Paris. Independence results for Peano arithmetic. "J. Symbolic Logic", 1978, vol. 43, N4, pp.725-731.

J. Paris, L. Harrington. A mathematical incompleteness in Peano arithmetic. In Barwise [1977].

The authors are telling their story in the third of these papers:

"The first examples of strictly mathematical statements about natural numbers which are true but not provable in PA (Peano arithmetic) were due to the first author (see Paris [to appear], and grew out of the work in Paris and Kirby [to appear]. The second author's contribution was to show that Paris's proof could be carried through with the particularly simple extension of the Finite Ramsey Theorem..."

If the finite sets discussed in the Finite Ramsey's theorem would come from some fixed countable "universe" (for example, if we decided to consider only sets of natural numbers), then we could not restrict ourselves to counting of members of these sets. And we could consider also some other properties of them.

For example, let us call a property g of finite sets of some "universe" U a **dense property**, if and only if:

a) If a finite set H_1 possess the property g, and H_1 is a subset of a finite set H_2, then H_2 also possess the property g.

b) For each infinite set H_2 there is a finite subset H_1 that possess the property g (this is the "density" of g).

A simple example of a dense property of sets of natural numbers is the so-

called property of being "relatively large": a set H of natural numbers is called **relatively large**, if and only if $\min(H) \le |H|$.

Indeed:

a) If $\min(H_1) \le |H_1|$, and H_1 is a subset of H_2, then $\min(H_2) \le \min(H_1) \le |H_1| \le |H_2|$, i.e. $\min(H_2) \le |H_2|$.

b) If H_2 is an infinite set of natural numbers, take as H_1 the set of $\min(H_2)+1$ least members of H_2. Then $\min(H_1)=\min(H_2)<|H_1|$, i.e. H_1 is relatively large.

This is an example of a **computable** dense property: having all members of some finite set, we can computably decide, possess this set the property or not.

Extended Finite Ramsey's theorem. Let us consider only sets of natural numbers. For **each computable dense property** g there is a computable function $R_g(e, r, k)$ such that for all positive integers e, r, k and each finite set M the following holds: if $|M| \ge R_g(e, r, k)$, and each e-member subset of M is marked by one of r colors, then there is a subset H of M such that $|H| \ge k$, H **possess the property** g, and all e-member subsets of H are marked by the same color.

This theorem differs from the Finite Ramsey's theorem only "a little" – additionally, the set H possess the property g.

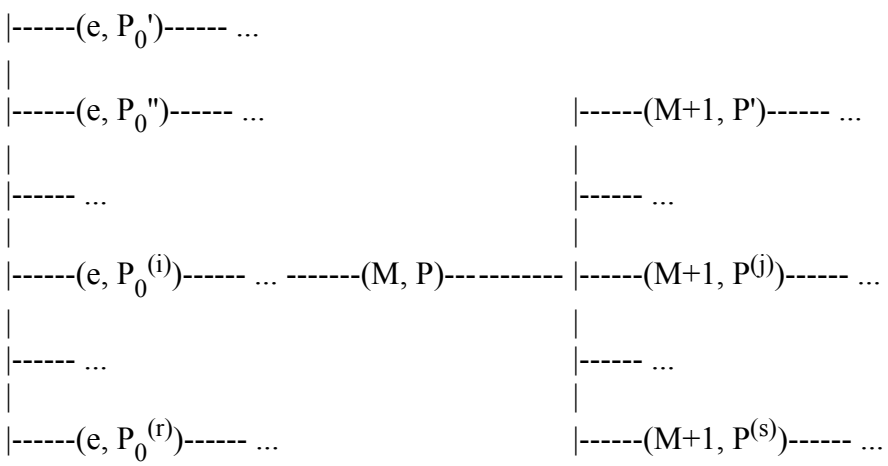
Proof – part 1 (in PA). Since properties of members of the set M do not affect the problem to be solved, we can replace M, for example, by the set of natural numbers $\{0, 1, ..., |M|-1\}$, i.e. in terms of Section 2.3 we can say that M **is** a natural number.

For M=e there is only one e-member subset $\{0, 1, ..., e-1\}$. The number of possible "r-colorings" of this subset is r.

Suppose, we have a pair (M, C), where C is some r-coloring of e-member subsets of M. Of course, for each triple (e, r, M) there is only a finite number of different r-colorings of e-member subsets of M. Hence, if we proceed from M to M+1, where

$$M+1 = \{0, 1, ..., M-1, M\} = M \cup \{M\},$$

then from the r-coloring C we can obtain only a finite number of r-colorings (of e-member subsets) of M+1 that are **extensions** of C. (Some coloring C' of M+1 is called an extension of C, if and only if each e-member subset of M is marked in C' by the same color as it is marked in C.)



If we proceed in this way from e to e+1, after this – to e+2, e+3 etc., then we obtain an **infinite tree** of pairs (M, C) having at each of its nodes only a **finite** number of branches. Indeed, let us start from a fictive empty node O. At the next level (M=e) we have r branches to r different r-colorings of the only e-member subset of e. Etc., from each node (M, C), where C is an r-coloring of e-member subsets of M, a finite number of branches is starting to all the possible nodes (M+1. C') such that C' is an r-coloring of e-member subsets of M+1 that extends C.

Of course, (for fixed e and r) this tree contains all the possible pairs (M, C), where C is an r-coloring of e-member subsets of M, and it defines some natural ordering of them.

Let us say that (M, C) is a "good" node, if there is a subset H of M such that $|H| \geq k$, H possess the property g, and all e-member subsets of H are marked (in the coloring C) by the same color.

Exercise A.2.1. Verify that if (M, C) is "good", and there is a branch from (M, C) to (M+1, P'), then (M+1, P') also is "good". I.e. if some node is "good", then the entire subtree of it is "good".

Since each level of the tree contains only a finite number of nodes, the Extended Finite Ramsay's theorem would be proved, if we could prove that there is only a finite number of "bad" nodes. Indeed, then we could produce the following algorithm computing the function $R_g(e, r, k)$. Let us scan all levels of the tree one by one, determining for each node, is it "good" or "bad". If there are only a finite number of "bad" nodes, then at some level all nodes will be "good". Let us take the level number M for the value of $R_g(e, r, k)$.

Exercise A.2.2. Describe an algorithm determining, is a given tree node "good" or "bad". How much time is required to solve this task?

Of course, we do not need set theory to define the above algorithm. Indeed, let us repeat its definition once more:

Input: numbers e, r, k. Build the corresponding (M, C)-tree. Scan all levels of this tree one by one, determining for each node, is it "good" or "bad". If at some level all nodes are "good", take the level number M and output it as the value $R_g(e, r, k)$.

Hence, no problem to write a computer program that takes numbers e, r, k as input, and either calculates the number $R_g(e, r, k)$ as output, or ... does not halt (if there are no tree levels with "good" nodes only).

Surprisingly, we need set theory to prove that this program halts for all triples (e, r, k).

Proof – part 2 (in ZFC). Let us assume the opposite – that there is an infinite number of "bad" nodes. If there is a branch from (M, C) to (M+1, C'), and the node (M+1, C') is "bad", then (M, C) also is "bad". Hence, the substructure of "bad" nodes in our tree is itself a tree – a finitely branching infinite tree.

Exercise A.2.3. Prove the following version of the so-called König's lemma: if a finitely branching tree has infinite set of nodes, then this tree contains an infinite branch.

Hence, our tree contains an infinite branch B consisting of "bad" nodes only. This branch defines a single r-coloring C" of **all e-member** sets of natural numbers. Indeed, if $\{x_1, ..., x_e\}$ is a set of natural numbers, then take $M = \max\{x_1, ..., x_e\}$, consider the node (M, C_M) of the branch B, and mark the set $\{x_1, ..., x_e\}$ (in the coloring C") by the color it is marked in the coloring C_M. This definition of C" is "stable" in the sense that on the branch B the coloring C_M is the first one that assigns a color to the set $\{x_1, ..., x_e\}$, and all the following colorings C_{M+1}, C_{M+2}, ... cannot change this color, since they all are extensions of C_M. I.e. C" is an extension of C_M for all M.

Let us apply the Infinite Ramsey's theorem to the set N of all natural numbers and the r-coloring C". I.e. there is an infinite subset H" of N such that all e-member subsets of H" are marked by the same color. Since g is a dense property, there is a finite subset H of H" that possess the property g. Let us add to H enough members of H" to ensure that $|H| \geq k$. This extended set also possess the property g. If we take $M = \max(H)+1$, then H appears to be a subset of M such that: $|H| \geq k$, H possess the property g, and all e-member subsets of H are marked by the same color in the coloring C_M. Hence, (M, P_M) is a "good" node – on the branch B consisting of "bad" nodes only!

I.e. our tree always contains only a finite number of "bad" nodes. And hence,

our algorithm computing the function $R_g(e, r, k)$ halts for all triples (e, r, k). Q.E.D.

The Extended Finite Ramsey's theorem cannot be proved in PA

For any computable dense property g the Extended Finite Ramsey's theorem can be formulated in PA. We have proved this theorem in ZFC, yet:

Kirby-Paris-Harrington Theorem. For the property g of being **relatively large** (i.e., if g(H) means $\min(H) \leq |H|$) the Extended Ramsey Theorem cannot be proved in PA (if PA is consistent).

Proof. See the above paper by Paris and Harrington.

Thus, since 1977 we know an example of a "strictly mathematical statement about natural numbers" that cannot be proved in first order arithmetic. And since 1977, some similar results were established (see above).

All this means that Greeks having only their first order notion of natural numbers could not prove the Extended Finite Ramsey's theorem and some other "strictly mathematical statements about natural numbers". These proofs became possible only in 1870s when Georg Cantor invented set theory. **By introducing the notion of arbitrary infinite sets Cantor added new features also to the 2400 years old notion of natural numbers.** Q.E.D.

Now let us return to the beginning of this Appendix where the problem of introducing "nonmathematical" questions into number theory was discussed. If you believe that formulas of first order arithmetic (PA) used in Gödel's proofs are not normal mathematical statements about natural numbers, then what would you say about the following theorem from the same famous paper by Paris and Harrington?

Traditionally, the so-called Σ_1-formulas are defined as formulas of PA having the form $\exists x_1 ... \exists x_n F(...)$, where F belongs to the class of the so-called "primitive recursive" formulas, and all quantifiers before F are existential. Still, as we have proved in Section 4, any such formula has a Diophantine representation

$$\exists x_1 .. \exists x_n \exists y_1 ... \exists y_k \; P = 0,$$

where P=0 is a Diophantine equation. Since our proof can be formalized in PA, we can define Σ_1-formulas simply as Diophantine representations, i.e. as Diophantine equations preceded by existential quantifiers.

The following statement can be formulated in the language of PA:

"For all Σ_1-formulas F(x) having exactly one free variable x,

if for each n, PA proves F(**n**), then ∀xF(x)"

This statement is called the **uniform Σ_1 reflection principle** for PA. This principle says that if PA proves all cases of some Σ_1-formula F(x), then F(x) is true for all x. Of course, this principle can be proved in ZF by using the standard model of PA (see Appendix 1). Still, it cannot be proved in PA, moreover, it cannot be proved even in PA + Con(PA) (if this extended theory is consistent, see the chapter about incompleteness theorems in Barwise [1977]). Hence, the uniform Σ_1 reflection principle for PA is a stronger hypothesis than the hypothesis "PA is consistent".

Is the uniform Σ_1 reflection principle for PA (as a formula of first order arithmetic) an example of introducing "nonmathematical" questions into number theory? Of course, it is. Is the Extended Finite Ramsey's theorem an example of a "strictly mathematical statement about natural numbers"? Of course, it is. Still, one can prove the following

Theorem. It can be proved in PA, that, for property g of being relatively large, the Extended Finite Ramsey's theorem is equivalent to the uniform Σ_1 reflection principle for PA.

Proof. See the above paper by Paris and Harrington.

A deadlock? Not for me. I find more interesting the conclusion that Extended Finite Ramsey's theorem cannot be proved not only in PA, but it cannot be proved also in PA+Con(PA).

The function R(e, r, k) from the Finite Ramsey's theorem is known as a very fast growing function (see Graham [1981]). Still, for min(H)≤|H| as g, the function $R_g(e, r, k)$ exceeds in this area any possible expectations. Namely, for this specific property g the "diagonal" function $R_g(k, k, k+1)$ is growing faster than any function f(k) such that

PA proves: ∀x∃y F(x, y),

where the formula F(x, y) represents f in PA (see Section 3.3). I.e. if you can prove in PA, that your algorithm for computing f(k) halts for all k, then f(k) as a function of k is growing slower than $R_g(k, k, k+1)$.

Proof. See the above paper by Paris and Harrington.

Appendix 3. Elements of Category Theory (under construction)

History of Mathematics as Invention of New Structures

Around 6th century BC: the invention of an infinite sequence of natural numbers (starting with 1). Theorem. There are infinitely many prime numbers (the old formulation...)

The "atomic" geometry and the paradox of $\sqrt{2}$. Proportion theory as the first theory of real numbers.

Euclidean geometry.

Inventiong of zero, the arabic notation.

Solving of cubic equations. Invention of *i* and of complex numbers.

Development of algebraic notation in 16th – 17th centuries.

Negative numbers.

Is the 5th postulate derivable? Non-euclidean geometries.

Modular arithmetic ($a \equiv b \, mod \, p$). Quadratic fields ($a + b\sqrt{p}$).

Quadratic forms.

Solving of quintic equations. Permutations as the first kind of non-commutative transformations (almost pure "group structure" with no other admixtures)

Cyclotomic fields, ideal numbers.

Groups

See also Group theory in Wikipedia.

What is a group? This notion represents an important type of mathematical structures (examples below). That is the reason why such a notion is considered.

Fields and rings arise naturally when considering various number systems. *Fields* represent the essential properties of the "most natural" numbers systems such as rational numbers, real numbers, complex numbers, where division is

always possible (except division by zero). *Rings* represent properties of number systems (such as integers), where division is not always possible. If , over some field K, we consider single variable polynomials, or *n* x *n* matrices , we obtain another two important examples of rings, i.e systems, where division is not always possible.

Groups arise in more advanced contexts – they represent the essential properties of systems of **invertible transformations**.

To create the abstract notion of group, we must identify the essential common features of all systems consisting of invertible transformations. Each such system includes a particular set *Ob* of *objects* (that can be *transformed* one into another somehow) and a particular set *Tr* of *invertible transformations*. Thus, each element $f \in Tr$ is a function $f : Ob \rightarrow Ob$.

The first (somewhat strange) step of abstraction: let us ignore the inner structure of objects in *Ob*, i.e. let *Ob* consist of "indivisibles", let us "transform indivisibles", and let us concentrate on the properties of *Tr* alone.

The set *Tr* must possess some specific properties.

First, *Tr* must be *closed under composition*: let us apply some $f \in Tr$ to any object $x \in Ob$ (obtaining the object $f(x)$), and, after this, let us apply some $g \in Tr$ to $f(x)$ (obtaining the object $g(f(x))$, then the resulting transformation (denoted usually by $g \circ f$) must belong to *Tr*.

[The reverse denotation is somewhat frustrating here. It is caused by the widely used prefix notation *f(x)*. The postfix notation *(x)f* would be, in fact, justified better: first, we must select arguments, and only after that we can apply the transformation. In this case we could denote the compositon of *f* and *g* more naturally – as ((x)f)g and $f \circ g$.]

Secondly, transformations in *Tr* are *invertible*. For each $f \in Tr$, there is an *inverse* transformation $f^{-1} \in Tr$. What does it mean? It means that if we apply *f* to any object $x \in Ob$ (obtaining the object $f(x)$), and if, after this, we apply f^{-1} to $f(x)$, then we re-obtain *x*: $f^{-1}(f(x)) = x$. In other words, the composition $f^{-1} \circ f$ is the *identity* transformation. And, of course, the relation "is inverse of" is symmetrical: if f^{-1} is inverse to f, then f must be inverse to f^{-1} : $f(f^{-1}(x)) = x$.

Thus, thirdly, the set *Tr* must include the *identity* transformation $e = f^{-1} \circ f$, that "does not transform at all", i.e. the one with the property $\forall x \in Ob(e(x) = x)$.

Now, the second (equally strange?) step of abstraction: let us drop the objects (the set *Ob*) at all. Let us formulate the essential properties of *Tr* without referring to *Ob*.

A group is a **set** G (of **group elements** – the former invertible tranformations) and a two argument **function** o: $G \times G \rightarrow G$ (called the **group operation** – the

former transformation composition) satisfying the **group axioms** (trying to capture the essential features of *Tr*, see below). Hence, one needs set theory (ZFC or other) before to start working with arbitrary groups (infinite ones included). If one wished to work with finite groups only, this could be done within the first order arithmetic (PA) as well.

Now, more precisely. Let us work in ZFC. And let us call the pair (G, o) a **group**, if and only if:

G is a set (the informal meaning: a set of *transformations*, the objects to be transformed are ignored here completely);

o is a function $G\times G\to G$ (the informal meaning: *composition* of transformations, we will write $x\circ y$ instead of $o(x,y)$);

the following group axioms are satisfied:

$\forall x,y,z\in G((x\circ y)\circ z=x\circ(y\circ z))$ (*associativity*, informally: a natural property of transformation composition);

[The commutativity property $x\circ y=y\circ x$ is not included here. Some of the transformation groups are not commutative. See Exercise 2.33 c), d).]

there is $e\in G$ such that $\forall x\in G(x\circ e=e\circ x=x)$ (e is a *unit element*, the informal meaning: *identity* tranformation).

[How to formulate "leaving untransformed" without mentioning the objects to be transformed? Here we see the idea: $\forall x\in G(x\circ e=e\circ x=x)$, i.e. we formulate the intended property of *e* by referring not to objects, but to other transformations. Does this formulatio capture the "true" property of being identity transformation? Of course, the "true" identity transformation *e* possess the property $\forall x\in G(x\circ e=e\circ x=x)$. And, as you will prove in Exercise 2.33, in a group, there is a *unique* element with this property. Q.E.D.]

$\forall a,b\in G\,\exists x,y\in G(a\circ x=b\wedge y\circ a=b)$ (invertibility, formulated in terms of solvability of equations).

[In some other texts, the invertibility property is formulated by using the inverse element: for each element x there is an element x^{-1} having the property $x^{-1}\circ x=x\circ x^{-1}=e$. However, before using "the" symbol e, we must prove that the unit element is unique. It is not cool to involve theorems to formulate the basic axioms. Our formulation of the invertibility axiom implies the traditional one (and conversely), as you will prove in Exercise 2.33.]

Exercise A.3.1 (optional). Prove that, in a group: a) there is only one unit element (so, we can denote it by *e*); b) for each element x , there is exactly one element x^{-1} , such that $x\circ x^{-1}=x^{-1}\circ x=e$ (the inverse element). Thus, $(x^{-1})^{-1}=x$. c) the equations $a\circ x=b;\ y\circ a=b$ possess exactly one solution each, namely, $x=a^{-1}\circ b$ (the "left-side division") and $y=b\circ a^{-1}$ (the "right-side division"); d) $(x\circ y)^{-1}=y^{-1}\circ x^{-1}$.

The above properties c) and d) express strikingly the "smell" of the possible non-commutativity.

Is the above formal definition of groups **complete**, i.e. is each group (in the sense of the definition), indeed, "a kind of" transformation group? More precisely, is is each group (in the sense of the definition) *isomorphic* to some tranformation group? Yes, it is. This fact follows from Cayley's theorem. Arthur Cayley published it in 1854.

Exercise A.3.2 (optional, for smart students). Prove Cayley's theorem. Hint: for a group *(G, o)* and each $a \in G$, consider the transformation $f_a(x) = a \circ x$, and verify that it is a *permutation* (i.e. a specific kind of transformation) of G. After this, verify, that (G, o) is isomorphic to the transformation group $\{f_a | a \in G\}$.

Transformation groups are not the only possible interpretations of groups (in the sense the above formal definition).

Take any *ring* (for example, integer numbers) and consider its *addition* operation. In this way we obtain a *commutative group* (with zero element in the role of the unit element). Commutative groups are called abelian groups.

Take any *field* (for example, rational numbers, real, or complex numbers) and consider its *multiplication* operation, but with zero element excluded. In this way we obtain, again, a commutative group.

Take any non-trivial field *K*, and consider $n \times n$ *matrices* over *K* (n>1) with non-zero determinants. In this way we obtain a *non-commutative* group.

Take any prime number *p*, and consider the numbers $0, 1, \ldots, p-1$ with addition and multiplication *modulo p*. In this way we obtain a *finite field* denoted usually by Z_p , and thus – two examples of finite groups.

In **group theory**, we investigate "abstract groups", i.e. the consequences of group axioms. Why should we? These consequences are applicable to any "concrete groups", i.e. to any structures satisfying the group axioms. See Normal subgroup and Quotient group in Wikipedia for the first important examples of such consequences.

Why should we? Discovering new structures? Finite groups and their classification. Lie groups etc.

Topological spaces

See also Topological spaces in Wikipedia.

In the notion of topological spaces, mathematicians are trying to capture the most general properties of mathematical spaces – the ones allowing to consider **continuous** transformations (of 2-dimensional surfaces in a 3-dimensional space, for example) without introduction of distances between points.

(A modern "distilled" definition.) A **topological space** *T=(S, Op)* consists of

1) A set S of objects of any kind. These objects are called *points*, to emphasize the idea that, in the general theory, their inner structure will be ignored.

2) A set $Op \subseteq P(S)$, i.e. a collection of subsets of S. Members of *Op* are called **open sets** of T. The set Op is called "a topology on S", to emphasize the idea that one can consider different topologies on the same set of objects.

3) The following **topology axioms** must be satisfied:

3a) The empty set 0 and the set S is open (i.e. $0 \in Op \wedge S \in Op$).

3b) Any (even *infinite*) union of open sets is an open set.

3c) Any *finite* intersection of open sets is an open set.

Hence, one needs set theory (ZFC or other) before to start working with arbitrary topological spaces.

Complements of open sets are called **closed sets**.

The central notion of topology:

A set *A* is called a **neighbourhood** of a point *x*, if and only if there is an *open* set *B* such that $x \in B \wedge B \subseteq A$.

The intuition behind the notion of open set is revealed in the following

Exercise A.3.X. a) Assume, the set A contains each of its points together with some neighbourhood of it. More precisely: $\forall x \in A \, \exists B \in Op (x \in B \wedge B \subseteq A)$. Show than then, A is an open set.

b) Verify that any neighbourhood A of a point x contains a ("smaller") neighbourhood B of x such that A is a neighbourhood of *each point of* B.

Continuous functions. Consider two topological spaces $T_1 = (S_1, Op_1); T_2 = (S_2, Op_2)$, two open sets $R_1 \subseteq S_1; R_2 \subseteq S_2$ and a function $f: R_1 \to R_2$. We will say that f is continuous, if and only if for each $x \in R_1$ and each neighbourhood B of f(x) there is a neighbourhood A of x such that $f'' A \subseteq B$.

Exercise A.3.X. Verify that f is continous, if and only if for all open sets $B \in Op_2$, $f^{-1}(B)$ is an open set (in Op_1). More precisely: ???????

Homeomorphisms ("topological isomorphisms"). A continuous function $f: R_1 \to R_2$ is called a homeomorphism, if and only if it is invertible (i.e. an injection) and f^{-1} is a continuous function as well. And then, the sets R_1 and $f'' R_1$ are called homeomorphic.

Examples.

?????

In a 3-dimensional space, the surface an elipsoid (or a cube) is homeomorphic to sphere.

Categories

See also Category theory in Wikipedia.

What is a category? It represents the next level of abstraction: an abstract type of important types (**type of types!**) of mathematical structures.

Groups and topological spaces represent two important types of mathematical structures. How could we create an abstract notion of such types - "type of types", in particular, covering these two structures – as different as they are? What are the common features of groups and topological spaces?

It seems, we will not be able to find such common features by looking at the inner organizations of groups and topological spaces – the properties of group operations and open sets.

But let us remember the abstraction by means of which we created the notion of group from the notion of systems of invertible transformations: we dropped the set *Ob* of objects (to be transformed) and tried considering only the necessary properties of the transformation set *Tr*. I.e. we started to consider tranformations as **indivisible objects** without any inner structure, and tried to describe how transformations are **related to each other**.

Couldn't we try a similar abstraction at the next level? For example, by trying to consider *groups* as indivisible objects and trying to describe how are they related to each other? And, similarly, by trying to consider *topological spaces* as indivisible objects and trying to describe how are they related to each other?

Indeed, how are "they" related to each other? Let us consider the case of groups.

Group category

One can try mapping the structure of a group into the structure of another group by means of "structure preserving" mappings called *group homomorphisms*. In this way we are trying to find "how many" of one group's structure can be found in another group.

Consider two groups $(G_1, o_1), (G_2, o_2)$ and a mapping (function) $h: G_1 \to G_2$ having the following "structure preserving" properties: $h(e_1) = e_2$, and, for all $x, y \in G_1$,

$$h(x \circ_1 y) = h(x) \circ_2 h(y) \ .$$

Such functions are called group *homomorphisms*.

Exercise A.3.3. Verify that $h(e_1)=e_2$, and $h(x^{-1})=(h(x))^{-1}$ for all $x\in G_1$, and that the image $h''G_1$ is a *subgroup* of G_2 .

There is always a *trivial* homomorphism from (G_1,o) to *any* group (G_2,o) , defined as $h(x)=e_2$ for all $x\in G_1$. Of course, calling such a homomorphism "structure preserving" is an exaggeration. Truly structure preserving are only *injective* homomorhisms, i.e. the ones having the property: $x\neq y\rightarrow h(x)\neq h(y)$. For an injective homomorphism $h:G_1\rightarrow G_2$, the inverse function $h^{-1}:h''(G_1)\rightarrow G_1$ is a homomorphism as well (verify). In this situation we say that groups G_1 and $h''G_1$ (a subgroup of G_2) are *isomorphic*, and that $h:G_1\rightarrow h''G_1$ is an *isomorphism*.

In a sense, the set of all the possible homomorphisms $h:G_1\rightarrow G_2$ represents **all the substructures of** $(G_{1,}o_1)$ **that can be found in** $(G_{2,}o_2)$. So, let us try to characterize the inner structure of the group $(G_{1,}o_1)$ by its homomorphisms to all the possible other groups $(G_{2,}o_2)$, and by homomorphisms from all the possible other groups $(G_{2,}o_2)$ into $(G_{1,}o_1)$. In this way we arrive at the notion of *group category*, consisting of all the possible groups (now, indivisible objects) and all the possible homomorphisms (now, indivisible "arrows") between them.

Now,

The general notion of category

First of all, in general, a category is based on two **classes** – the class of **objects** (groups, topological spaces, etc.) and the class of **morphisms** (group homomorphisms, homeomorhisms, etc.) satisfying the **category axioms**. Hence, again, one needs set theory before to start working with categories.

Objects and morphisms may form, indeed, even *proper classes*. For example, the formula asserting that $(G_{1,}o_1)$ is a group, defines the class of all groups. One can easily verify that this is, indeed, a proper class. If objects and morphisms of a category form sets only, such a category is called *small category*.

Now, more precisely. To start, let us work in ZFC. And let us call the quadruple C=(*Ob, Mor, o, id*) a category, if and only if:

1) *O* is a class (its elements are called *objects*).

2) *Mor* is a function $Ob\times Ob\rightarrow V$. For any objects $x,y\in Ob$ the value $Mor(x,y)$ is a set, whose elements are called *morphisms* from x to y. Instead of $f\in Mor(x,y)$ we will write simply $f:x\rightarrow y$, and we will call x the

domain of *f*, and y – the *codomain* of f. [The term "range", so usual in set theory, is not used in category theory, because here, objects "do not consist of elements".]

Informal meaning: a morphism $f: x \to y$ maps the "structure" of the object *x* into the "structure" of the object *y*. However, elements of structures and "values" of mappings ($f(a)=b; a \in x; b \in y$) do not appear in category theory (like as objects to be transformed do not appear in group theory). This makes necessary the axiom 5a below.

Let us denote by M the class of all morphisms of the category C, i.e. the union of all sets $Mor(x, y)$.

3) o is a partial function $M \times M \to M$ (*composition* of morphisms, we will write $f \circ g$ instead of $o(f, g)$).

Informal meaning: first, the mapping g is applied, after it – the mapping f. Of course, $f \circ g$ is defined for compatible morphisms only (see the axiom 5a below).

4) *id* is a function $O \to M$ such that $id(x): x \to x$, the morphism id(x) (or $id_{x)}$ is called the *identity* morphism of the object x.

Informal meaning: an identity morhism maps "x onto x literally" (see the axiom 5d below).

5) The following **category axioms** are satisfied:

5a) For different pairs *(x, y)*, the sets of morphisms $Mor(x, y)$ do not intersect.

5b) $f \circ g$ is defined for compatible morphisms only. Namely, $f \circ g$ is defined, if and only if $g: x \to y; f: y \to z$ for some *x, y, z*, and, in this case, $f \circ g: x \to z$.

5c) Associativity: if $f \circ g$ and $g \circ h$ are both defined, then

$$f \circ (g \circ h) = (f \circ g) \circ h \ .$$

Informal meaning: associativity is a natural property of mappings. [If $f \circ g$ and $g \circ h$ are both defined, then $f \circ (g \circ h); (f \circ g) \circ h$ are both defined as well.]

5d) For each $f: x \to y$, $f \circ id_x = id_y \circ f = f$.

The meaning of being an identity mapping looks somewhat different from what is said in the axiom 5d. We know this phenomenon from group theory above. Of course, a "real: identity mapping must possess the property expressed in the axiom. And, we will prove in Proposition C1 that for each object, there is only one identity morphism.

The end of definition.

The simplest theorems of category theory

are proved similarly to the ones of group theory.

Let us first prove the simplest possible theorem of category theory:

Proposition C1. If $i: x \to x$, and, for each $f: x \to x$, $f \circ i = f \vee i \circ f = f$, then $i = id_x$. Hence, for each object, there is only one identity morphism.

Proof. If $id_x \circ i = id_x$ is given as a property of *i*, then $id_x \circ i = i$ as a property of id_x, hence, $i = id_x$. And, if $i \circ id_x = id_x$ is given as a property of *i*, then $i \circ id_x = i$ as a property of id_x, hence, $i = id_x$. Q.E.D.

Let say that $g: y \to x$ is an *inverse morphism* to $f: x \to y$, if and only if $f \circ g = id_y \wedge g \circ f = id_x$.

Proposition C2. Each morphism *f* possess zero or one inverse morphism, and thus, we can denote the inverse of f (if it exists) by f^{-1} .

Proof. Indeed, if $g_1, g_2: y \to x$ both are inverse to $f: x \to y$, then, on one hand, $g_1 \circ f \circ g_2 = g_1 \circ id_y = g_1$, on the other hand, $g_1 \circ f \circ g_2 = id_x \circ g_2 = g_2$, hence, $g_1 = g_2$. . Q.E.D.

Exercise A.3.4. a) Verify that $id_x^{-1} = id_x$. b) Verify that, if *f, g* are invertible morphisms, and $f \circ g$ exists, then it is invertible as well, and $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

If a morphism $f: x \to y$ possess an inverse morphism $f^{-1}: y \to x$, then let us call *f* and f^{-1} *isomorphisms*, and let us say that the objects x, y are *isomorphic*.

Category of sets

Let us introduce a category of objects that possess only a minimum of "structure" – the category of sets **Set** = (*Ob, Mor, o, id*). As objects, let us consider arbitrary sets (of ZFC), thus, *Ob=V.* As morphisms $f: x \to y$ let us consider arbitrary mappings, i.e. functions with $domain(f) = x$ and $range(f) \subseteq y$, marked, additionally, by *x* and *y* (thus, speaking very precisely, set morphisms are tripples *(f, x, y)*). Hence, for different pairs *(x, y),* the sets *Mor(x, y)* do not intersect, and the axiom 5a is satisfied.

The composition *o* of morphisms is defined here as the usual composition of mappings: if $f: y \to z$ and $g: x \to y$, then, for any $a \in x$, $(f \circ g)(a) = f(g(a))$, and we mark this function by *x* and *z*. Thus, the axioms 5b and 5c are satisfied.

The identity morphism $id_x: x \to x$ is defined here as the identity function: for

any $a \in x$, $id_x(a) = a$. We mark this function by x and x.

However, for the empty set 0, the identity function $id_0 : 0 \to 0$ is an empty set of pairs (a somewhat unusual, but necessary assumption). And if so, to satisfy the axiom 5d, we must admit the *empty morphism* $0 : 0 \to x$ for any set x as well (marking it by *0* and *x*).

For an overview of other important categories, see Category-theoretic categories in Wikipedia.

"Categorical Reasoning"

Now, the first example of a non-trivial "categorical reasoning". If our objects are indivisible, i.e. if they do not possess elements, how can we apply to them such notions as, for example, *surjective* and *injective* morphisms?

A surjective mapping $f : x \to y$ must exhaust all the elements of y as its target values. But now, we do not have elements in y! So, we must define the surjectivity property of f somehow **with respect to other morphisms**. A surjective mapping f possess the following property: if $g_1, g_2 : y \to z$, then $g_1 \circ f = g_2 \circ f \to g_1 = g_2$. Indeed, in the category of sets, if f is *not* a surjective mapping, i.e. it leaves some element of y unused, then we can build two mappings $g_1 \neq g_2$ such that $g_1 \circ f = g_2 \circ f$.

So, let us call $f : x \to y$ an *epimorphism*, if and only if for all $g_1, g_2 : y \to z$:

$$g_1 \circ f = g_2 \circ f \to g_1 = g_2 \ .$$

Is this definition not only "necessary", but also "sufficient"? How could we verify that? We could consider concrete categories and verify that all of their epimorhisms are surjective mappings. [The term "surjective morphism" is not used in category theory, because objects do not possess elements here.]

Now, how about injective mappings? Let us try out the dual definition:

Let us call $f : x \to y$ a *monomorphism*, if and only if for all $g_1, g_2 : z \to x$:

$$f \circ g_1 = f \circ g_2 \to g_1 = g_2 \ .$$

Is this property injectivity? Yes, it is, indeed, in the category of sets: if f is *not* an injective mapping, i.e. if it glues some elements of y together, then we can find two mappings $g_1 \neq g_2$ such that $f \circ g_1 = f \circ g_2$.

Is this definition not only "necessary", but also "sufficient"? How could we verify that? We could consider concrete categories and verify that all of their monomorhisms are injective

mappings. [The term "injective morphism" is not used in category theory, because objects do not possess elements here.]

Exercise A.3.5. Verify that any isomorphism is monomorphism and epimorphism as well. [The converse is not true: build an artificial finite category as a counter-example.??????]

Trivial, Initial and Terminal Objects

In some category, which of the objects are the simplest ones? How to define such a notion without referencing the inner structure of objects, i.e. by referencing only morphisms between objects?

The idea: let us say that x is a **trivial object**, if and only if the only morphism $f: x \to x$ is the identical morphism id_x. Indeed, if an object would possess some "inner structure", it would allow some non-trivial "morphing" on it.

In the category of sets, there are two kinds of trivial objects: a) the empty set 0; b) singletons $x=\{a\}$.

Proposition C3. If two trivial objects possess a two-way connection via morphisms, then they are isomorphic.

Proof. Let x and y be trivial objects connected by some morphisms $f: x \to y; g: y \to x$. Then, inevitably, $g \circ f = id_x; f \circ g = id_y$. Q.E.D.

In the category of sets, the empty set 0 possess only a one-way connection to a singleton: $0: 0 \to \{a\}$, this is why there are two kinds of trivial objects in this category.

The above idea "there is exactly one morphism..." can be exploited further. If there is exactly one morphism $f: x \to y$, what can be said about the "inner structures" of *x, y*? It seems, either x, or y, or both must be trivial????

And, what, if I is an object such that for any x, there is exactly one morphism $f: I \to x$? Then I is called the **initial object** of the category.

The dual notion is the one of a **terminal object** T: for any x, there is exactly one morphism $f: x \to T$.

Exercise A.3.6. Verify that: a) all initial objects of a category are isomorphic and trivial; b) all terminal objects of a category are isomorphic and trivial.

In the category of sets, the only initial object is the empty set, and the only terminal objects are singletons *{a}* (verify).

Products and Co-products

Another experiment: let us try to define, for an arbitrary category, **the notion**

of product. For sets, it is the cartesian product, for groups – the direct product of groups, for topological spaces – the product (Tychonoff) topology. But how to define such a notion without referencing the inner structure of objects (sets, groups, spaces), i.e. by taking into account only their relations to other objects via morphisms?

Let us try solving a seemingly completely different task. Having two objects of a category, x and y, how could we "join them together" obtaining a new object XY that could replace both of them? Of course, XY must be connected somehow to x, y via morphisms. There are two possibilities:

a) there must exist two morphisms: $\varphi_x : XY \to x ; \varphi_y : XY \to y$;

b) there must exist two morphisms: $\varphi_x : x \to XY ; \varphi_y : y \to XY$.

What should our "join and replace" mean? There is only one kind of "activities" in a category – morphisms. Thus, XY must replace x, y in morphisms.

For example, could we replace two "incoming" morphisms $f_x : Z \to x ; f_y : Z \to y$ by a single morphism $f : Z \to XY$ and the two fixed "universal" morphisms $\varphi_x : XY \to x ; \varphi_y : XY \to y$ in the following way:

$$f_x = \varphi_x \circ f ; f_y = \varphi_y \circ f \ ?$$

We are interested to obtain the "minimum" XY providing this property, i.e. XY must possess the "properties" of x and y without a minimum of "admixtures". This can be assured by requiring, for any two morphisms f_x, f_y , the **uniqueness** of the "joint" morphism *f*.

Thus we could call an object XY and two "outgoing" morphisms $\varphi_x : XY \to x ; \varphi_y : XY \to y$ the "**incoming join**" of *x, y*, if and only if, for any two "incoming" morphisms $f_x : Z \to x ; f_y : Z \to y$, there is exactly one morphism $f : Z \to XY$ such that $f_x = \varphi_x \circ f ; f_y = \varphi_y \circ f$.

In a similar way, we could call an object XY and two "incoming" morphisms $\varphi_x : x \to XY ; \varphi_y : y \to XY$ the "**outgoing join**" of x, y, if and only if, for any two "outgoing" morphisms $f_x : x \to Z ; f_y : y \to Z$, there is exactly one morphism $f : XY \to Z$ such that $f_x = f \circ \varphi_x ; f_y = f \circ \varphi_y$.

Do such "joins" exist in all categories and for all object pairs x, y? No. (You could try verifying this by building some artificial finite categories.)

But let us consider the *category of sets*. It appears that, in this category, the "incoming join" of *x, y* is provided by the *cartesian product* $x \times y$, and the "outgoing join" of *x, y* is provided by the *disjoint union* of *x, y.*

Indeed, let us consider $x \times y$ together with the projection mappings

$\varphi_x(a,b)=a;\varphi_y(a,b)=b$. Then, for any two "incoming" mappings $f_x:Z\to x;f_y:Z\to y$, there is exactly one mapping $f:Z\to x\times y$ such that $f_x=\varphi_x\circ f;f_y=\varphi_y\circ f$, namely, $f(c)=(f_x(c),f_y(c))$.

And, let us consider the *disjoint union* of *x, y*, namely, the set $x+y=(\{1\}\times x)\cup(\{2\}\times y)$ together with the mappings $\varphi_x(a)=(1,a)$; $\varphi_y(b)=(2,b)$. Then, for any two "outgoing" mappings $f_x:x\to Z;f_y:y\to Z$, there is exactly one mapping $f:x+y\to Z$ such that $f_x=f\circ\varphi_x;f_y=f\circ\varphi_y$, namely, $f(1,a)=f_x(a);f(2,b)=f_y(b)$.

This why, in category theory, the "incoming join" is called the **product** of *x, y*, and the "outgoing join" – the **coproduct** of *x, y.*

Thus, in the category of sets, products and coproducts always exist, and are represented by cartesian products and disjoint unions.

In the category of groups, products and coproducts always exist as well, and are represented by the so-called direct products of groups and free products of groups.

In the category of topological spaces, products and coproducts always exist as well, and are represented by product (Tychonoff) topologies and disjoint unions of spaces.

Proposition C4. In any category, any two products of the objects *x, y* (if such exist) are isomorphic.

Proof. Let us denote by $(XY,\varphi_x,\varphi_y);(XY',\varphi_x',\varphi_y')$ two products of *x, y.*

Lemma. $(\forall f:XY\to XY)[\varphi_x=\varphi_x\circ f\wedge\varphi_y=\varphi_y\circ f\to f=id_{XY}]$. And, similarly, for XY'.

Indeed, let us take, in the definition of the "incoming join": $Z=XY;f_x=\varphi_x;f_y=\varphi_y$. Then there is exactly one morphism $f:XY\to XY$ such that $\varphi_x=\varphi_x\circ f\wedge\varphi_y=\varphi_y\circ f$. Hence, $f=id_{XY}$. Q.E.D.

Now, let us take, in the definition of the "incoming join" XY: $Z=XY';f_x=\varphi_x';f_y=\varphi_y'$. Then there is a morphism $f:XY'\to XY$ such that $\varphi_x'=\varphi_x\circ f\wedge\varphi_y'=\varphi_y\circ f$. Similarly, there is a morphism $f':XY\to XY'$ such that $\varphi_x=\varphi_x'\circ f'\wedge\varphi_y'=\varphi_y'\circ f'$. Hence,

$$\varphi_x'=\varphi_x\circ f=(\varphi_x'\circ f')\circ f=\varphi_x'\circ(f'\circ f)\ ;$$

$$\varphi_y'=\varphi_y\circ f=(\varphi_y'\circ f')\circ f=\varphi_y'\circ(f'\circ f)\ .$$

By Lemma, $f'\circ f=id_{XY'}$. In a similar way, $f\circ f'=id_{XY}$. Thus, f and f' are isomorphisms, and XY and XY' are isomorphic. Q.E.D.

Proposition C4 (dual). In any category, any two coproducts of the objects *x, y*

(if such exist) are isomorphic.

Proof. Dual.

See also Product and Coproduct in Wikipedia.

Functors

See also Functor in Wikipedia.

Universal Property

For a general treatment, see Universal property in Wikipedia.

As we will see later, ZFC is too weak, to support a natural development of category theory. The extended set theory ZFC+"there is a proper class of strongly inaccessible cardinals" is more suitable.

Yoneda lemma, an analogue of Cayley's theorem in category theory

...

To be continued.

Not quite a categorical reasoning...

Grothendieck Group

See also Grothendieck group in Wikipedia.

Monoids (another term: *semigroups*) represent an abstract algebraic structure more general than groups. If, in the definition of groups, we drop the axiom guaranteeing the existence of inverse elements, then we obtain the definition of monoids. Thus, a monoid is a set with an associative binary operation and an (in fact, "the") identity element. In a **commutative monoid** (another term: *abelian semigroup*), the operation is commutative. When working with commutative monoids, usually, the additive notation is used: the operation is denoted by "+", and the identity element – by 0.

Example: the set of all natural numbers 0, 1, 2, ... with the addition operation.

Some time ago, people extended this monoid by introducing negative numbers, and obtained in this way the *abelian* (i.e. commutative) *group* of integers. Negative numbers play here the role of elements inverse to the positive numbers.

Could this fundamental construction be extended to *all* commutative monoids? Could *any* commutative monoid be extended to (or, embedded into) an abelian group in some unique and natural way? How to make this desire *precise*? Perhaps, one could extend a monoid into a group in many ways, but which one of these ways would be the most natural one?

Category theory offers the answer. Having a commutative monoid M, we may consider many abelian groups G and monoid homomorhisms $f: M \to G$ embedding M into G. Which one of these groups would be the most natural one for M? Let us denote it by K, and by $k: M \to K$ – the corresponding monoid homomorphism.

According to category theory, K and k will represent the most natural abelian group for M, if, for each abelian group G and monoid homomorhism $f: M \to G$ there will exist **exactly one** *group* homomorphism such that $f = g \circ k$.

BILDE!!!

Thus, any embedding of M into an abelian group G can be reconstructed *in a unique way* via a *universal* embedding k of M into K.

K is called a **Grothendieck group** of the monoid M. It represents the simplest case of a very general and powerful construction introduced by Alexander Grothendieck in 1950s.

Exercise. Verify that if M is an abelian group, then all Grothendieck groups of M are isomorphic to M.

Theorem. For each commutative monoid M there exists a Grothendieck group.

Proof. Let us start with the cartesian product $M \times M$, and let us define the natural (commutative) addition operation on it:

$$(a, b) + (c, d) = (a+c, b+d),$$

where the first "+" is new, but the remaining two represent the addition in M. And let us introduce a kind of inversion on $M \times M$ as follows:

$$-(a, b) = (b, a).$$

Now, $(a, b) + [-(a, b)] = (a, b) + (b, a) = (a+b, a+b)$, and not (0, 0). Thus, the construction is not yet completed: some of the pairs must be defined as *equivalent*. For example, (a+b, a+b) must become equivalent somehow to (0, 0).

If we would work with natural numbers, we would wish (m, n) to be equivalent to (0, n–m), when m<n, and to (m–n, 0), otherwise.

In an arbitrary monoid, there may be no subtraction. So, let us define that

$(x_1,y_1)\equiv(x_2,y_2)$, if and only if, there are $a,b\in M$ such that

$$(x_1+a,y_1+a)=(x_2+b,y_2+b)\ .$$

In particular, $(x,x)\equiv(0,0)$.

This relationship is reflexive (take a=b=0), symmetric (obviously), and transitive well:

if $(x_1+a,y_1+a)=(x_2+b,y_2+b)$ $(x_2+c,y_2+c)=(x_3+d,y_3+d)$ and, then

$$x_1+a+c=x_2+b+c=x_3+b+d;\ y_1+a+c=y_2+b+c=y_3+b+d$$, i.e.
$$(x_1+a+c,y_1+a+c)=(x_3+b+d,y_3+b+d)\ .$$

Secondly, if $(x_1,y_1)\equiv(x_2,y_2)$, then, obviously, $-(x_1,y_1)\equiv-(x_2,y_2)$.

Thirdly, if $(x_1,y_1)\equiv(x_2,y_2)$ and $(a_1,b_1)\equiv(a_2,b_2)$, then, obviously,

$$(x_1+a_1,y_1+b_1)\equiv(x_2+a_2,y_2+b_2)\ .$$

Thus, these equivalence classes of $M\times M$ form an abelian group, let us denote it by $K_0(M)$.

The natural monoid homomorphism $k_0:M\to K_0(M)$ we define as $k_0(x)=|(0,x)|$ (i.e. as the equivalence class containing $(0,x)$).

Now, if we have an abelian group G and a monoid homomorphism $f:M\to G$, then there is only one way to reconstruct f as $f=g\circ k_0$ via k_0, K_0 and a *group* homomorphism $g:K_0(M)\to G$.

Indeed, we must pass from $x\in M$ to $f(x)\in G$. Since $k_0(x)=|(0,x)|$, we must set: $g|(0,x)|=f(x)$. Since g must be a group homomorphism, we are forced to set:

$$g|(a,b)|=g|(0,b)|+g|(a,0)|=g|(0,b)|-g|(0,a)|=f(b)-f(a)\ .$$

Thus, g is determined by f uniquely. Let us verify that g is a group homomorphism, indeed:

$$g|(a,b)+(c,d)|=g|(a+c,b+d)|=f(b+d)-f(a+c)=f(b)+f(d)-f(a)-f(c)$$
$$g|(a,b)+(c,d)|=g|(a,b)|+g|(c,d)|\ .$$

Q.E.D

Theorem. All Grothendieck groups of the same M are *isomorphic*.

Proof. Let us consider a Grothendieck group K of M (and the corresponding univeral morphism $k:M\to K$). Let us show that K is isomorphic to $K_0(M)$.

First, there is a [unique] group homomorphism $g:K\to K_0(M)$ such that $k_0=g\circ k$. Since, for any $x\in M$, $k_0(x)=|(0,x)|$, we obtain that $g(k(x))=|(0,x)|$. Then, since g is a group homomorphism, for any

$x, y \in M$:

$$g(k(x)-k(y))=|(0,x)|-|(0,y)|=|(y,x)| \ .$$

Thus, *g* is a *surjection* $K \to K_0(M)$.

Secondly, there is a [unique] group homomorphism $g_0 : K_0(M) \to K$ such that $k = g_0 \circ k_0$. Since, for any $x \in M$, $k_0(x)=|(0,x)|$, we obtain that $g_0(|(0,x)|)=k(x)$. Then, since g_0 is a group homomorphism, for any $x, y \in M$:

$$g_0(|(y,x)|)=g_0(|(0,x)|-|(0,y)|)=k(x)-k(y) \ .$$

Thus, g_0 is *inverse* to the surjection g , hence, both are group isomorphisms.

(By the way: the above shows that any Grothendieck group K is "minimal" , i.e. that

$$K=\{x \in K | (\exists y, z \in M) x=k(y)-k(z)\} \ ).$$

Q.E.D.

One might ask: must the universal monoid homomorphism $k : M \to K$ from M into its Grothendieck group K always be *injective*? It must not:

Theorem. If M supports the *cancellation law* ($x+z=y+z \to x=y$), then the universal monoid homomorphism $k : M \to K$ from M into its Grothendieck group K is *injective*.

Proof. Suppose, M supports the cancellation law.

First, let us consider the above group $K_0(M)$ and the universal monoid homomorphism $k_0 : M \to K_0(M)$ that was defined as $k_0(x)=|(0,x)|$. Let us show that k_0 is injective.

If $k_0(x)=k_0(y)$, then $(0,x) \equiv (0,y)$, i.e. $(0+a, x+a)=(0+b, y+b)$ for some a, b. Hence, $x+b=y+b$ and $x=y$. Thus, k_0 is injective, indeed.

Now, consider any Grothendieck group K of M, and the universal monoid homomorhism $k : M \to K$. Then there is a group homomorphism $g : K \to K_0$ such that $k_0 = g \circ k$. Thus, if k would be non-injective, then so would be k_0 that is impossible.

Q.E.D.

Ex. Uzbuvejiet pretpiemeru.

Exercise. Verify that the Grothendieck group of the additive monoid of natural numbers is isomorphic to the additive group of integers.

Groupoids

Introduced by Heinrich Brandt.

The main idea: let us allow the group operation $x \circ y$ be undefined for some x, y.

To be continued.

Voevodsky about groupoids

http://en.wikipedia.org/wiki/Vladimir_Voevodsky

http://www.math.ias.edu/~vladimir/Site3/Univalent_Foundations_files/2014_IAS.pdf

"The successes of category theory inspired the idea that categories are "sets in the next dimension" and that the foundation of mathematics should be based on category theory or on its higher dimensional analogs.

It is the idea that categories are "sets in the next dimension" that was the most difficult roadblock for me. I clearly recall the feeling of a breakthrough, which I experienced when I understood that this idea is wrong. Categories are not "sets in the next dimension". They are "partially ordered sets in the next dimension," and "sets in the next dimension" are groupoids.

One of the things that made the "categories" versus "groupoids" choice so difficult for me is that I remember it being emphasized by people I learned mathematics from that the great Grothendieck in his wisdom broke with the old-schoolers and insisted on the importance of considering all morphisms and not only isomorphisms and that this was one of the things that made his approach to algebraic geometry so successful."