FERMAT'S LAST THEOREM PROVED BY INDUCTION

Vasil Penchev, vasildinev@gmail.com
Bulgarian Academy of Sciences: Institute of Philosophy and Sociology:
Dept. of Logical Systems and Models

Abstract. *A proof of Fermat's last theorem is demonstrated. It is very brief, simple, elementary, and absolutely arithmetical. The necessary premises for the proof are only: the property of identity of the relation of equality,* modus tollens*, axiom of induction, the proof of Fermat's last theorem in the case of "*n = 3*" as well as the premises necessary for the formulation of the theorem itself. It involves a modification of Fermat's approach of infinite descent. The infinite descent is linked to induction starting from "*n = 3*" by* modus tollens*. An inductive series of* modus tollens *is constructed. The proof of the series by induction is equivalent to Fermat's last theorem. As far as Fermat had been proved the theorem for "n = 4", one can suggest that the proof at least for "n ≥ 4" had been accessible to him.*

The theorem known as "Fermat's last theorem" (FLT) was formulated by the French mathematician in 1637 and proved by Andrew Wiles (1995). Fermat remained both its statement and his claim for the proof too long for the margin. So, the challenge of a simple proof accessible to Fermat has been alive for centuries.

Andrew Wiles's proof is too complicated. It is not only beyond arithmetic, but even the question whether it is within set theory can be asked (whatever the answer might be).

What follows is a simple and elementary proof by the axiom of induction applied to an enumerated series of uniform recurrent arithmetical statements sharing the logical form of *modus tollens*.

The necessary premises are only: the identity of equality in mathematics; *modus tollens*; the axiom of induction, the proof of FLT for $n = 3$. All premises necessary for the theorem itself to be formulated should be added as well as propositional logic for the proof itself. Thus, all Peano axioms of arithmetic and those of propositional logic are included.

The set of all natural numbers, designated as "N", is the only set meant anywhere bellow. All variables (x, y, z, n, a, b) and the constant "c" are defined only on it: their values are its elements. However, the set "N" (as an actual infinite set in the sense of set theory) is not used. It is utilized only for simplifying the notations.

The idea of proof is a modification of Fermat's infinite descent, consisting in the following: The modification is not directed to construct a false statement included in any proof by *reductio ad absurdum*. Furthermore, it starts as if "from infinity" rather than from any finite natural number. Anyway, the modification is able to be restricted only to arithmetic and the axiom of induction (i.e. without the set-theory "actual infinity") by means of an enumerated series of *modus tollens*. Thus, Fermat's infinite descent is seen and utilized as "reversed": as an ascent by induction.

If one decomposes FLT to an enumerated series of statements, namely, FLT (3), FLT (4), FLT (5), …, FLT (n), FLT (n+1) , ..., each of one referring to a certain natural number, 3, 4, 5, n, n=1, … , which is the exponent in FLT, the idea of the proof is:

$$\forall(x,y,z,n)\,\epsilon\,N\colon[(a=x^{n+1})\rightarrow(b=x^{n})]\leftrightarrow\ [FLT(n)\ \rightarrow\ FLT(n+1)]$$

According to FLT, all FLT (n) are negative statements. If one considers the corresponding positive statements, FLT*(n) = ¬FLT (n), the link to the series of *modus tollens* is obvious:

$$\forall(x,y,z,n)\epsilon\,N\colon[(a=x^{n+1})\rightarrow(b=x^{n})\leftrightarrow[\neg\text{FLT*(n)}\rightarrow\neg\ \text{FLT*(n+1)}]$$

This is the core of proof. It needs a reflection even philosophical.

Two triple equalities ("$a=x^{n+1}=y^{n+1}+z^{n+1}$", and "$b=x^{n}=y^{n}+z^{n}$") are linked to each other by *modus tollens*. What is valid for the left parts, $(a=x^{n+1})\rightarrow(b=x^{n})$, is transferred to the right parts, $\neg(x^{n}=y^{n}+z^{n})\ \rightarrow\neg(x^{n+1}=y^{n+1}+z^{n+1})$, as an equivalence. The mediation of each middle member in both triple equalities is crucial: it allows for the transition. An extended description of "$\forall(x,y,z,n)\epsilon\,N\colon[(a=x^{n+1})\rightarrow(b=x^{n})\leftrightarrow\ [\neg$FLT*(n) $\rightarrow\neg$ FLT*(n+1)]" is:

$$\forall(x,y,z,n)\epsilon\,N\colon[(a=x^{n+1}=y^{n+1}+z^{n+1})\rightarrow(b=x^{n}=y^{n}+z^{n})]\leftrightarrow$$
$$\leftrightarrow[\neg(b=x^{n}=y^{n}+z^{n})\rightarrow\neg(a=x^{n+1}=y^{n+1}+z^{n+1})]$$

In fact, the arithmetical equality ("=") and logical equality "↔" are divided disjunctively. Their equivalence is not necessary or used.

Anyway, their equivalence is valid as a mathematical isomorphism. Even more, the law of identity in logic, "$\forall a\colon a\leftrightarrow a$", referring to the propositional logic, and the axiom of identity, "$\forall a\colon a=a$", referring to any set of objects in a (first-order, second-order, ..., n-order, ...) logic are isomorphic mathematically. The identity is a special kind of relation, in which all those orders are merged, and thus, indistinguishable from each other within it.

Nonetheless, any exemplification of that indistinguishability of identity due to mathematical isomorphism is not used in the proof. Furthermore, the auxiliary variables "*a*" and "*b*" (involved only for the explanation of the idea) will not be utilized.

The proof in detail:

$$\text{FLT}\colon\forall(x,y,z,n\geq3)\,\epsilon\,N\colon\neg\text{"}x^{n}=y^{n}+z^{n}\text{"}$$

"FLT(c)" means: ¬"$x^{c}=y^{c}+z^{c}$" where "c" is a constant: $c\geq3,\ c\,\epsilon\,N$. FLT will be proved as FLT(c) will be proved for each "c" ($\forall c$) by induction. The equivalence of "FLT" and "∀c: FLT(c)" is granted as obvious. The set of all "FLT(c)" is neither used nor involved in any way.

The relation of equality can be defined by its three properties: identity, symmetry, and transitivity. Only "identity" will be used to be proved a corollary from *modus tollens*, which is necessary to be linked Fermat's infinite descent to an inductive ascent.

Law (axiom) of identity [LI]: $\forall A\colon A = A$

For the present utilization, it will be modified equivalently to:

(A) "$\forall x\colon x \leftrightarrow x = x$", and then to

(B) "$(\forall x\colon x = y) \leftrightarrow (\forall x\colon x \leftrightarrow x = y)$".

Proof:

A: (1) $x \rightarrow (x = x)$. Indeed, let $\neg\,(x \rightarrow x = x) \rightarrow \exists x\colon x \neq x \rightarrow \neg\,(\forall x\colon x = x)$: contradiction.

(2) $(x = x) \rightarrow x$. Indeed: if not, the term "x" of the proposition "$x = x$" would be absent sometimes: contradiction.

B: $\forall x\colon x \leftrightarrow (x{=}x) \leftrightarrow [x = (x = y)] \leftrightarrow (x = x = y) \leftrightarrow [(x = x) = y] \leftrightarrow (\mathrm{x} = \mathrm{y})$.

Consequently, $\forall x\colon x \leftrightarrow (x{=}y)$

"$A" \wedge "B" \rightarrow "(x = x) \leftrightarrow (x = y)$" which is necessary for *modus tollens* to be equivalently modified.

Modus tollens [MT]: $(A \rightarrow B) \leftrightarrow (\neg B \rightarrow \neg A)$, and it modified for the case [MMT]:

$$[("x^{n+1} = x^{n+1}" \rightarrow "x^n = x^n") \leftrightarrow (\neg "x^n = x^n" \rightarrow \neg "x^{n+1} = x^{n+1}")] \leftrightarrow$$
$$\leftrightarrow [("\boldsymbol{x^{n+1} = x^{n+1}}" \rightarrow "\boldsymbol{x^n = x^n}") \leftrightarrow (\neg "\boldsymbol{x^n = y^n + z^n}" \rightarrow \neg "\boldsymbol{x^{n+1} = y^{n+1} + z^{n+1}}")]$$

Axiom of induction [AI]: $"\forall p, n\colon p(1) \wedge [p(n) \rightarrow p(n+1)] \rightarrow p"$ where "$p(n)$" is an arithmetical proposition referring to the natural number "n", and "p" is the same proposition referring to all natural numbers. "Arithmetical proposition" means a proposition in a first-order logic applied to arithmetic. The axiom of induction is modified starting from $n = 3$ rather than from $n = 1$:

$$\{\forall p, n\colon p(1) \wedge [p(n) \rightarrow p(n+1)] \rightarrow p\} \rightarrow \{\forall p, n \geq 3\colon p(3) \wedge [p(n) \rightarrow p(n+1)] \rightarrow p\}$$

A modification of Fermat's infinite descent [MFID]: MT modified as above is applied as starting from $n = 3$ as follows:

$$\ldots n, n-1, \ldots 5, 4, 3$$

The same descent is interpreted as a series of enumerated propositions:

$$\ldots (n), (n-1), \ldots (5), (4), (3)$$

A reverse chain of negations is implied:

$$\neg(3), \neg(4), \neg(5), \ldots, \neg(n-1), \neg(n), \ldots$$

Both ascent of "negations" and infinite descent are constructed step by step following the increasing number of the negative propositions (rather than the decreasing number of the positive propositions):

$$[(4) \to (3)] \leftrightarrow [\neg(3) \to \neg(4)], [(5) \to (4)] \leftrightarrow$$
$$[\neg(4) \to \neg(5)], [(6) \to (5)] \leftrightarrow [\neg(5) \to \neg(6)], \quad \dots$$
$$\dots [(n+1) \to (n)] \leftrightarrow [\neg(n) \to \neg(n+1)], [(n+2) \to (n+1)] \leftrightarrow$$
$$\leftrightarrow [\neg(n+1) \to \neg(n+2)], \dots \dots$$

So, one builds a series of *modus tollens* starting from $n = 3$.

FLT (3): x, y, z *are natural numbers. There do no exist any* x, y, z:

$$x^3 + y^3 = z^3$$

Many mathematicians beginning with Euler claimed its proof. Ernst Kummer's proof (1847) will be cited here for its absolute rigor. It refers to all cases of "regular prime numbers" defined by Kummer, among which the case "$n = 3$" is.

Furthermore, the "n^{th}" member of the series of *modus tollens*, namely:

"[(n+1)→(n)]↔[¬(n)→¬(n+1)]" is valid as far as "(n+1)→(n)" is valid.

@One interprets that "(n+1)→(n)" in the case of FLT:

$$\forall x, n: (x^{n+1} = x^{n+1}) \to (x^n = x^n)$$

This is true for "$x^{n+1} = x^{n+1} = x^n . x^1$". Thus, "$x^n = x^n$" is a necessary condition for "$x^{n+1} = x^{n+1}$" and the former is implied by the latter.

One uses [MMT] "modified *modus tollens*" further:

The series of modified *modus tollens* is interpreted in terms of FLT as the following series of implications:

["$x^4 \to x^3$" ∧ "FLT (3)"] → "FLT (4)"
["$x^5 \to x^4$" ∧ "FLT (4)"] → "FLT (5)"
["$x^6 \to x^5$" ∧ "FLT (5)"] → "FLT (6)"
... → ...
["$x^{n+1} \to x^n$" ∧ "FLT (n)"] → "FLT (n+1)"
["$x^{n+2} \to x^{n+1}$" ∧ "FLT (n+1)"] → "FLT (n+2)"
... → ...

The member of the series of implications is true for "n=3", the validity for "n" implies the validity for "n+1". Thus, it is valid for "any member enumerated by a natural number greater than two" in virtue of the axiom of induction.

FLT is proved.

If one accepts that Fermat (1670) had proved FLT (4) and as far as the above proof seems to be accessible to him, he might prove FLT at least for $n \geq 4$.

The answer of a frequent objection:

The objection is: the "modified *modus tollens*" needs "$x^n = y^n + z^n$" to be proved. Fermat's infinite descent modified as in the claimed proof uses the substitution "$\neg(x^n = y^n + z^n)$". So, this contradiction, involved in the proof, makes it false.

The answer is: "$x^n = y^n + z^n$" is a necessary condition for the "modified *modus tollens*". Thus, the latter implies the former. "$\neg(x^n = y^n + z^n)$" is a substitution in the "modified *modus tollens*". Thus, the latter implies the former.

Consequently, the "modified *modus tollens*" implies both "$x^n = y^n + z^n$" and "$\neg(x^n = y^n + z^n)$", but **separately**, i.e. by disjunction rather than by conjunction. This is not a contradiction as:

$$[(a \to b) \vee (a \to \neg b)] \leftrightarrow "True"$$
$$\forall x: ("True" \to x) \leftrightarrow x$$

This means only that the proof involves a tautology redundant to the syllogism.

This is quite different from the alleged "$[a \to (b \wedge \neg b)] \to "False$", which is absent in the proof.

References:

Fermat, P. (1670) "Diophanti Alexandrini Arithmeticorum libri sex, et De numeris multangulis liber unus. Cum commentariis C.G. Bacheti v.c. & obseruationibus D.P. de Fermat .senatoris Tolosani," in *Acessit Doctrinae analyticae inuentum nouum, collectum ex varijs eiusdem D. de Fermat epistolis.* Tolosae: Excudebat Bernardus Bosc, è regione Collegii Societatis lesu, M. DC. LXX, pp. 338-339 (Source: http://books.google.com/books?id=yx9VIgeaCEYC&hl=&source=gbs_api 1670.)

Wiles, A. (1995) "Modular Elliptic Curves and Fermat's Last Theorem," *Annals of Mathematics* Second Series **141** (3): 443-551 (DOI 10.2307/2118550. MR1333035. Zbl 0823.11029)

Kummer, E. (1847) "Beweis des Fermat'schen Satzes der Unmöglichkeit von $x^\lambda + y^\lambda = z^\lambda$ für eine unendliche Anzahl Primzahlen λ," in Kummer, Ernst Eduard. *Collected papers* (ed. Andre Weil) Volume 1. *Contributions to number theory*. Berlin, Heidelberg, New York: Springer, 1975, pp. 274-297. (ISBN 978-3662-48832-4. DOI N/A. MR0465760. Zbl 1331.01037.)

A comment. *The original proof of Fermat's las theorem: a philosophical reflection*

Prehistory and background:

Fermat remained a statement (supposedly, in 1637) in the margin of his exemplar of Diophantus's works as well as the claim he had proved it, but the proof was too long to be recorded in the margin. The statement is known as Fermat's last theorem (FLT): *the equation* $x^n + y^n = z^n$ *where x, y, z, n are natural numbers does not have any solution for* $n \geq 3$.

Fermat himself remained a proof for the case $n = 4$. Euler proved it for $n = 3$ in two different ways, but both proofs met criticism. Gauss's proof of the same particular case met criticism as well. Ernst Kummer's one (1847) refers to all "regular prime numbers" define by him, among which the case $n = 3$ is. His proof is mathematically rigorous enough. The theorem has been proved for many particular cases since then.

The statement in general was proved only in 1995 by Andrew Wiles as a corollary from the Taniyama-Shimura-Weil conjecture known as the modularity theorem after his proof. It links the continuous (even smooth) elliptic curves with the discrete modular forms. The proof is not arithmetical or accessible to Fermat. It is even so complicated that the question whether it is within set theory rather than only within arithmetic can be asked.

Anyway, Fermat's challenge for an elementary arithmetical proof remains.

An idea for the inductive proof of FLT:

An idea for proving FLT might be the following. The statement is proved for $n = 3$. If one proves that its validity for n implies its validity for $n + 1$, the statement will be proved by virtue of the axiom of induction in arithmetic, and thus: absolutely arithmetically.

Fermat's "infinite descent" involving *modus tollens* might be modified for the purpose. The modification would consists in the following. The infinite descent would not include in a *reductio ad absurdum* proof. It would starts as if "from infinity" rather than from any finite natural number. The descent might be transformed into a corresponding ascent, to which the axiom of induction would be applicable, by means of *modus tollens*.

The inspiration of the inductive proof might be the mathematical isomorphism of the law of identity in logic and the axiom of identity in the definition of the relation of equality axiomatically. It implies the isomorphism of logical equivalence referring to propositions and the relation of equality referring to objects or terms. Thus, identity in virtue of its definition is a special "singularity" where propositional logic and any logic of an arbitrary order merge to each other.

The inspiration for merging can originate from a few philosophical doctrines such as Pythagoreanism, Hegel's panlogism, Husserl's phenomenology, Heidegger's doctrine(s). Furthermore, it can originate from an experimental science such as quantum mechanics and its mathematical formalism grounded on the separable complex Hilbert space.

However, it can originate from the absence or instability of Descartes's dualism during Fermat's life (as far as he is almost Descartes's contemporary). This together with some kind of naïve Pythagoreanism admissible or even probable for a mathematician in number theory might inspire Fermat for a simple arithmetical proof of FLT.

Fermat's accessibility to that kind of inductive proof:

The idea of inductive proof is relative to Fermat's infinite descent. He himself had been prove FLT

for $n = 4$. So, the conjecture that Fermat meant the proof for $n \geq 4$ is probable.
Furthermore, the one of Euler's proof (the more correct one though containing gaps) was admissible to Fermat at least in principle. So, the option for Fermat meant the case $n \geq 3$ might not be excluded absolutely.

The meaning of identity in an eventual inductive proof:

The identity is able to inspire an elementary, simple, very brief, and absolutely arithmetical proof of FLT by the method of mathematical induction. The philosophical essence of that identity is the identity of anything (i.e. an object in any n-order logic) and the "word" designating the same thing (i.e. the corresponding term in the (n-1)-order logic). In other words, this means the identity of any mathematical structure and its interpretation of any kind. For example, meaning that identity, one should erase the distinction between mathematical models and their material interpretation in physics. The identity refers only to its scope: it does not imply mathematical models and their interpretations to be identified at all. It states only the existence of a mathematical model identical to a given physical system or vice versa: a given physical system identical to a given physical model.
This seems to be a philosophical postulate. On the contrary, Western philosophy (and particularly, philosophy of science) as far as originates from Descartes's dualism postulates the opposite statement: no mathematical model can be identical to the physical system interpreting it. Only a few, though the most important, properties and relations of the system can be captured by the model, but there exist always others, which are not, regardless of whether there exist property or relation of the system which cannot be reflected in the model ever at all, in principle.
Thus, a difference whether absolute or historically relative justifies the distinction of "things" and "words" in Western philosophy and philosophy of science. Its "blind spot" is all knowledge within the opposite postulate allowing the identity of a mathematical model and a physical system. Thus, the necessary inspiration for an elementary proof of FLT by induction turns out to be within the same 'blind spot". The proof out of it, e.g. that of Andrew Wiles, is incredibly complicated, indirect, and mediated by many, many chain links way to be seen the invisible being situated in the area corresponding to the "blind spot". If one manages to reflect the existence of "blind spot", the change of position is much simple as to observing what is located in the "blind spot" area. Abandoning the metaphor, this means to be accepted the opposite postulate: mathematical model and reality can coincide and thus, be identical. Once, that postulate is the case, the identity necessary for an elementary inductive proof of FLT is admissible and the pathway to it is open. However, one can suggest that the actual pathway as a "Wittgenstein ladder" might be removed in the final analysis. That is: the identity is necessary for the inspiration to an elementary proof, but not within it actually, not within its text literally.
In facts, quantum mechanics was forced almost violently by the experimental results to see the area corresponding to the "blind spot" of Western philosophy and science. The shocking theorems of the "absence of hidden variables" in quantum mechanics were proved. They implied the absolute coincidence of model and reality at least as to quantum mechanics, and thus, their identity. Consequently, quantum mechanics might serve as an "inspiration" for an elementary, inductive proof of FLT.

Identity in terms of Descartes's dualism:

However, Fermat's contemporary Descartes, his "older brother" by age, born, lived, and died about ten years ago, ten years before Fermat, postulated the non-identity at issue by his doctrine of dualism.

Perhaps only God and belief might be the "key" to identity, otherwise inaccessible to human beings. Thus, the direct pathway for an elementary inductive proof of FLT would turn out to be closed for centuries, and a very, very round and indirect road would be walked exceptionally hard only at the end of millennium by Andrew Wiles.

One can admit easily, that the direct pathway had not been closed ultimately in Fermat's age. So, Fermat might prove his last theorem really, relying on that identity still possible and admissible in science and mathematics.

Descartes remained his "analytic geometry" together with the "dualism": what is gapped in the latter is linked in the former. Measuring the earth (i.e. "geometry") is identical to algebra generating mathematical models only. Thus, a Foucault "episteme" of identities and distinctions has been determined for centuries:

An identity (that of analytic geometry) has linked geometry to algebra and arithmetic, therefore constituting mathematics. A distinction (that of dualism) has gapped mathematics from physics, therefore constituting experimental science.

So, a plot about the “bystander – victim” Fermat, a "younger brother" of the “villain” Descartes can be outlined. The original proof of FLT would be the symbol and title of that scenario.

Identity in terms of the modern western philosophy:

Descartes’s dualism underlay all Western philosophy after him. One of its main problems was how the dualism might be overcome without God’s help. Kant’s transcendentalism and Hegel’s dialectic panlogism can be considered as ones of the most successful solutions.

The fundamentally different is only Husserl’s phenomenology (as well as Heidegger’s doctrine(s) influenced by it crucially). They considered the dualism as an axiom, and postulated its negation in their doctrines.

Conclusion:

A counterfactual course of time in history of philosophy and in history of mathematics can be allowed. The real branch of Descartes’s dualism and a lost original proof of FLT is ours. The counterfactual one would suggest an elementary arithmetical proof and perhaps the absence of Descartes’s dualism and the originating Western philosophy following it. The bifurcation happened in Descartes and Fermat’s age.

One might attempt to write down those counterfactual histories of mathematics and philosophy.