Is Euclid's proof of the infinitude of prime numbers tautological?

ZeeshanMahmud

January 31, 2011

Abstract

Euclid's classic proof about the infinitude of prime numbers has been a standard model of reasoning in student textbooks and books of elementary number theory. It has withstood scrutiny for over 2000 years but we shall prove that despite the deceptive appearance of its analytical reasoning it is tautological in nature. We shall argue that the proof is more of an observation about the general property of a prime numbers than an expository style of natural deduction of the proof of their infinitude.

"A mathematical theory is not to be considered complete until you have made it so clear that you can explain it to the first man whom you meet on the street."

David Hilbert

1 Introduction

There exist many versions of the proof and we will inspect three such instances of them.

1.1 Ribenboim's statement of Euclid's proof

Theorem. *There are infinitely many primes.*

Proof. *Suppose that p1=2 < p2 = 3 < ... < pr are all of the primes. Let P = p1p2...pr+1 and let p be a prime dividing P; then p can not be any of p1, p2, ..., pr, otherwise p would divide the difference P-p1p2...pr=1, which is impossible. So this prime p is still another prime, and p1, p2, ..., pr would not be all of the primes.*

1.2 David Joyce's English translation of Euclid's theorem

Theorem. *Prime numbers are more than any assigned multitude of prime numbers.*

Proof.

Let A, B, and C be the assigned prime numbers.

I say that there are more prime numbers than A, B, and C.

Take the least number DE measured by A, B, and C. Add the unit DF to DE.

Then EF is either prime or not.

First, let it be prime. Then the prime numbers A, B, C, and EF have been found which are more than A, B, and C.Next, let EF not be prime. Therefore it is measured by some prime number. Let it be measured by the prime number G. I say that G is not the same with any of the numbers A, B, and C.

If possible, let it be so.

Now A, B, and C measure DE, therefore G also measures DE. But it also measures EF. Therefore G, being a number, measures the remainder, the unit DF, which is absurd.

Therefore G is not the same with any one of the numbers A, B, and C. And by hypothesis it is prime. Therefore the prime numbers A, B, C, and G have been found which are more than the assigned multitude of A, B, and C. Therefore, prime numbers are more than any assigned multitude of prime numbers.

and,

1.3 Reformulation in modern terms

Theorem. *There are more primes than found in any finite list of primes.*

Proof. *Call the primes in our finite list p1, p2, ..., pr. Let P be any common multiple of these primes plus one (for example, P = p1p2...pr+1). Now P is either prime or it is not. If it is prime, then P is a prime that was not in our list. If P is not prime, then it is divisible by some prime, call it p. Notice p can not be any of p1, p2, ..., pr, otherwise p would divide 1, which is impossible. So this prime p is some prime that was not in our original list. Either way, the original list was incomplete.*

1.4 Formal statement of Euclid's theorem

Theorem(Euclid). *There exists an infinite set of prime numbers for any set of natural numbers.*

$$\vdash (N \in \mathbb{N} \to \exists j \in \mathbb{N}(N < j \bigwedge \forall k \in \mathbb{N}((j/k) \in \mathbb{N} \to (k = 1 \bigvee k = j))))$$

In words:

There exist infinitely many prime numbers: for any natural number N, there exists a prime number j greater than N.

2 Where Euclid erred

We take note of Euclid's definition of *prime* from Book VII, Definition 11:

> **Definition 2.1.** *A prime number is that which is measured by a unit alone.*

It is understood that Euclid had a very different notion of *infinite* in terms of *measure* and thus he wrote the theorem in an informal language. It was not until Cantor that the theory of infinite was made into a science and for sake of lucidity we shall examine Theorem 1.2 first.

Euclid begins the proof by stating: *Call the primes in our finite list p1, p2, ..., pr.* The moment we start off with a *finite* list of primes, we are assuming that there is a finite list to begin with! Intuitively suppose we live in an universe where time moved in super-slow motion where our thinking took place at snail pace giving us miniscule intelligence. Let us then take a set of first two primes {2,3}. How do we know that the next prime in the series is 5? The reason is we have at our disposal two already 'created' numbers less than 5 with which we can *test* to see if the next number is prime. What if we lived in another 'low-dimensional' universe *per se* where we could not even determine if 3 is a prime? Or what if we truncate the set to include 2 only? Now if we have reached a cul-de-sac as we have defined 2 as the first prime. And therein lies the problem. For there to exist infinitely many primes there must exist at least one prime. For that prime to exist we must define it. Thus if we define it we are proving a property of something that we already defined. The moment one defines a prime one pollutes the 'pure' set of numerals with a structure like a droplet of ink in a clear liquid. One causes a 'dent' so to speak. It is almost analoguous to 'Don't think of an elephant!' dilemma as it requires you to think of a structure with an assumption that a structure of that object exist.

Euclid then proceeds with his proof which we shall enumerate for sake of reference:

1. *Let A, B, and C be the assigned prime numbers.*
2. *I say that there are more prime numbers than A, B, and C.*
3. *Take the least number DE measured by A, B, and C. Add the unit DF to DE.*
4. *Then EF is either prime or not.*
5. *First, let it be prime. Then the prime numbers A, B, C, and EF have been found which are more than A, B, and C.Next, let EF not be prime. Therefore it is measured by some prime number. Let it be measured by the*

prime number G. I say that G is not the same with any of the numbers A, B, and C.

6. *If possible, let it be so.*

7. *Now A, B, and C measure DE, therefore G also measures DE. But it also measures EF. Therefore G, being a number, measures the remainder, the unit DF, which is absurd.*

8. *Therefore G is not the same with any one of the numbers A, B, and C. And by hypothesis it is prime. Therefore the prime numbers A, B, C, and G have been found which are more than the assigned multitude of A, B, and C. Therefore, prime numbers are more than any assigned multitude of prime numbers.*

Although Euclid's classical proof is mistakenly identified as using *reductio ad absurdum,* it is actually constructive in nature. With a finite list of primes in arsenal Euclid then constructs a case such that there would be *more* beasts of the same essence. By multiplying the primes and adding 1 to the resultant Euclid is surreptiously creating a constraint for the prime. Assuming a list of finite well-ordered primes, multiply them 2 X 3 X 5 X 7 X 11... and add 1 to get EF as in Steps 1-3, proceed to test for primality. *But the Steps 1-3 themselves constitute a test for primality!* If we lived in our hypothetical universe where time was slowed down then we would not be privy to access the list of initial finite list of primes. There are infinitely many primes implies existence of at least one prime. But how do we know that the prime exists? Simple because we invent it! In order to bootstrap our way out of the recurisveness we **define** the first prime - such as the number 2- which invariantly dilutes our number system, as mentioned above, and thus just by creating *a* prime, we are creating *infinite* primes!

3 Field of natural number embeds prime number

Note we are obviously not denying the existence of infinitude of primes.

Definition 3.1. A countable set is a set with the same cardinality (number of elements) as some subset of the set of natural numbers. A set that is not countable is called uncountable.

Theorem 3.1. *The set of prime numbers is countable.*

Proof. *Let X be the inductive set of natural numbers. By axiom of infinity, X is infinite. Let Y be the set of prime numbers where by prime we mean a number y such that it is divisible by y or 1 only. Does it follow that if X is infinite then Y is infinite? Assume no. But what if the elements of Y "builds up" X or rather, Y encodes the* genes *of X.*

Hence,

X: 1 2 3 4 5 6 7 8 9...

Y: 2 3 5 7 11 13 17...

Every subset of a countable set is countable. In particular, every infinite subset of a countably infinite set is countably infinite. For example, the set of prime numbers is countable, by mapping the n-th prime number to n:

2 maps to 1
3 maps to 2
5 maps to 3
7 maps to 4
11 maps to 5
13 maps to 6
17 maps to 7
19 maps to 8
23 maps to 9
and so on...

Either the set of the prime numbers can be put in one-to-one correspondence with set of natural numbers or not. Assume that it cannot be. Since, the cardinality of the natural numbers is $\aleph_0$ *if the prime numbers "dry out" then it has a finite cardinality C where* $C < \aleph_0$. *However, when* $C < \aleph_0$ *by mathematical induction it is possible to construct a number such that it is greater than C. This new number* $(C + \Delta)$.

For example, assume that in the set S of {2,3,5,7,11,13,17...} the primes "stop" at 17. This finite list has a cardinality 7 which is obviously smaller than $\aleph_0$. *But it is possible to conceive of a number* $7 + \Delta$, *where* Δ*could be, say 4, and thus we get the new cardinal 11 which means that 4 is the cardinality of the successive non-primes. But if we extend this notion assuming that primes "dried out" then we can divide the set of natural numbers into two sets the first one being the set of primes and the last one being that of non primes. The set of nonprimes must be infinite with cardinality* $\aleph_0$. *Thus we get* $C + \aleph_0 < \aleph_0$ *which is a contradiction proving our assumption wrong. Thus the set of primes must be infinite or countable.*

4 Prime numbers are infinite by virtue of their definition

Theorem 4.1. S is tautological where S:'There are infinitely many primes'.

Informally, can we create infinite number of cars without creating infinite number of chasis when the very basic core of a car is the chasis? Or for the same matter the reason why it is impossible to create infinite amount of cars without any color. Infinite list of *such* implies infinite list of *suchness ipso facto*.

The preceeding proof in Section 3 of the infinitude of prime numbers highlights that prime number verification requires the set Y to be infinite. If it follows that if X is infinite then Y must be infinite. But X encodes Y and X is infinite. So by stating that X is infinite we automatically have to assume certain characteristics of X. Primeness is a virtue of that characteristic. And by

assuming *primeness* we are stating in circular tongue that : If X is infinite then a subset of X must be infinite when we know that the definition of finiteness or measure depends upon the function acting upon itself. Therefore it is redundant and tautological to 'prove' the infinitude of prime numbers.

Consider the statement S: There are infintely many primes.

S is equivalent to S' : There are infinitely many prime numbers in a set of natural numbers.

S' is equivalent to S": There are infinitely many prime numbers in an infinite set of natural numbers.

S" is equivalent to S"': There are infinitely many prime numbers in an infinite set of natural numbers containing prime numbers (finite or infinite).

Or, if there exist a set N such that N is infinite and contains set P such that every element of N can be expressed in terms of elements of P, then P must be infinite.

5 Implications to Riemann Hypothesis

I invite the reader to venture a journey with the rigor of an atheist reading text of Bible. When confronted with the question: "Does God exist?" it immediately begs the question the definition of God but then by doing so we are concocting a predefined image in mind. Similarly when we begin a proof by assuming that there are primes to begin with we have certain mental construct of *primeness*. *We* have a taste for particular pattern. *We* prefer that particular pattern and because of our best interest we begin a search to look for them. We define *prime* with the characteristic of *primeness*. If we define them we create them and once they are "created" with as minimum as one ur-element then it is enough to guarantee infinitude of it. A number system cannot exist without primes just like *nouns* cannot exist without *adjectives*.

As stated by Don Zagier the following:

> "There are two facts about the distribution of prime numbers of which I hope to convince you so overwhelmingly that they will be permanently engraved in your hearts. The first is that, despite their simple definitions and role as the building blocks of the natural numbers, the prime numbers belong to the most arbitrary and ornery objects studied by mathematicians: they grow like weeds among the natural numbers, seeming to obey no other law than that of chance, and nobody can predict where the next one will sprout. The second fact is even more astonishing, for it states just the opposite: that the prime numbers exhibit stunning regularity, that there are laws governing their behavior, and that they obey these laws with almost military precision."
>
> The First 50 Million Prime Numbers

If we acknowledge the tautological nature of Euclid's proof than it immediately becomes obvious to us that the reason for the exhibition of the strange behavior

is simply because we designed it to be that way! Or rather a non-technical answer would be: "Duh!" Not only we define the prime number but we set it forth like Prime Mover a collection of sinusoidal strings each with unique wavelength where a set begins rather 'awkwardly' with 2,3,5,7 where 2 is the only even prime number.

When confronted with the question if Riemann Hypothesis is true, the catch-all, silver bullet response would be: "Depends!" with the understanding in mind that it must be either true, false or formally undecidable. Whatever frame of reference we use the answer would vary accordingly. If an 'observer' designs a set of numbers explicitly with a framework of design in mind and asks if it extends indefinitely even with such specific questions as the Montgomery Pair Correlation conjecture then it necessiates that we start off with a solid foundation of what we is it that we are explicitly seeking.

6 Conclusion

The above informal proof has been a *process*. By actively participating in the process we came to find out about the conclusion hence it is empirical in nature. Thus proof of infinitude of prime numbers can only be found from empiricism which itself is based on reason and opens up many avenues for philosophical implications of the nature of proof theory or the psychology of the matter as there is no independent "form" out there contrary to what Erdos would have us believe with the idealistic existence of "The Book".