ON THE FUNDAMENTAL THEOREM OF ARITHMETIC AND EUCLID'S THEOREM

HENDRA GUNAWAN

Abstract. We encounter a circular argument in the proofs of Euclid's theorem on the infinitude of primes that rely on the Fundamental Theorem of Arithmetic. We discover this by carefully observing the set of primes involved in the statement.

Introduction. We know what a **circular argument** or a **circular reasoning** is. To recall, an argument is circular if its conclusion is contained in its premises, or if it assumes — either explicitly or not — what it is trying to prove (see, for instance, [4]). An example of a circular argument can be found in the context of first year Calculus when one **proves** that $\lim_{x\to 0} \frac{\sin x}{x} = 1$ via L'Hôpital rule as follows:

$$\lim_{x\to 0} \frac{\sin x}{x} = \lim_{x\to 0} \frac{\cos x}{1} = 1.$$

The reason why this argument is circular is that the knowledge that the derivative of $\sin x$ is $\cos x$ is obtained by using the fact that $\lim_{x\to 0} \frac{\sin x}{x} = 1$, as is done in [5], Chapter 8. Thus, the above argument is like saying that $\lim_{x\to 0} \frac{\sin x}{x} = 1$ because $\lim_{x\to 0} \frac{\sin x}{x} = 1$, which is clearly circular.

In this short article, we shall discuss the logical relation between Euclid's Theorem (ET) on the infinitude of primes and the Fundamental Theorem of Arithmetic (FTA) for natural numbers. We know that Euclid has proved the infinitude of primes in his celebrated work *Elements*, precisely in Book IX, Proposition 20, by using only the definition of prime and composite numbers. Meanwhile, we have the FTA which states that *every natural number greater than 1 can be written as the product of primes, and that such a product is unique, up to the order of the factors*. In Book VII and IX of *Elements*, Euclid wrote some propositions related to the FTA, but the above statement of the FTA was formulated by C.F. Gauss in his work *Disquisitiones Arithmaticae* [2].

Although ET is already proved without the FTA (meaning that we already know that the infinitude of primes is a fact, without the aid of the FTA), we see that the FTA is stronger than ET. Thus, in some modern textbooks (from the 20th Century on) the authors prove the FTA first, then present ET as a corollary, as in [3]. Moreover, we can also find many proofs of ET that uses not only the FTA but also some other known facts. For example, L. Euler and P. Erdös proved ET by using the FTA and the knowledge about the series $\sum \frac{1}{n}$ and square free numbers, respectively. By considering carefully the primes involved in the FTA, we discover that proving ET by using the FTA, with or without other facts, is a circular reasoning.

Date: May 21, 2016.

I would like to thank Djoko Suprijanto, Oki Neswan, Aleams Barra, and Fajar Yuliawan for their useful comments.

1. ET as a necessary condition for the FTA

Let us begin with the statement of ET and the FTA for natural numbers, and their proofs. (We assume that the reader is familiar with natural numbers, primes, and composites. Here we are talking only about the natural numbers, not an arbitrary integral domain.)

Theorem 1. (ET) *There exist infinitely many primes among natural numbers.*

Proof. Suppose that we have a finite list of primes, say $p_1, p_2, \ldots, p_k$. Then we can show that there must be a prime number which is not in the list. Let $P := \prod_{i=1}^{k} p_i$ and $q := P + 1$. Then q is either prime or composite. If q is a prime, then we have found a prime which is not in the list. If q is a composite, then some prime p divides q. Since none of $p_i,\ i = 1, \ldots, k$ divides q, we have found a prime which is not in the list. Therefore, there must be infinitely many primes among natural numbers. □

Theorem 2. (FTA) *Every natural number greater than 1 can be written as the product of primes, and that such a product is unique, up to the order of the factors.*

Proof. We shall prove the first part by induction, and leave the uniqueness to the reader. The statement is true for 2, and assume that the statement is true for all numbers from 2 to $n-1$, where n is greater than 2. If n is prime, then there is nothing to prove. Otherwise, n is a composite, that is, $n = ab$ where $1 < a \leq b < n$. By the induction hypothesis, a and b are products of primes, so is n then. □

The following theorem tells us that the FTA is stronger than ET. The proof is similar to, but not the same as, that of ET.

Theorem 3. *If the* FTA *holds, then so does* ET.

Proof. Suppose that ET is false, that is, there is only a finite number of primes, say $p_1, \ldots, p_k$. Let $q = 1 + \prod_{i=1}^{k} p_i$. Since none of p_i's is a factor of q, the number q cannot be expressed as the product of p_i's. Hence the FTA is false. □

From the above theorem, we see that for the FTA to hold, it is necessary that the collection of primes must be infinite. Using a finite number of primes, we can only factorize **some** natural number greater than 1, but not **all**. Knowing that the infinitude of primes is a necessary condition for the FTA, we would like to find out next what is the sufficient condition for the FTA to hold (for natural numbers).

2. The FTA reconstructed

To understand the FTA better, let S be a set of primes, not necessarily containing all primes, and consider the following statement:

Every natural number greater than 1 can be written as the product of primes in S (in a unique way, up to the order of factors).

We shall refer to this statement as the *Unique Prime Factorization over S*, abbreviated by UPF-S. From the previous theorem, we know that the set of primes involved in the FTA is infinite. We restate this fact in the following theorem.

Theorem 4. *If* UPF-S *holds, then* S *is infinite. Equivalently, if* S *is finite, then* UPF-S *is false.*

The infinitude of S is a necessary condition, but clearly not a sufficient condition for UPF-S. For instance, the set $S := \{3, 5, \dots\}$ of primes other than 2 is infinite but UPF-S fails to hold. In general, we have the following theorem.

Theorem 5. *If* UPF-S *holds, then* S *contains all primes. Equivalently, if* S *does not contain all primes (that is, there is a prime which does not belong to* S*), then* UPF-S *is false.*

Proof. Just take a prime q which is not in S. Then q cannot be expressed as a product of primes in S. □

`Remark`. For our purpose, we deliberately avoid denoting the set of all primes by any letter.

Now we come to the important question: what is a sufficient condition on the set S for UPF-S to hold? From Theorems 4 and 5, we have two necessary conditions for UPF-S to hold: (C1) S is infinite and (C2) S contains all primes. By ET, we know that the condition (C2) is stronger than (C1). But let us pretend that we do not know that the set of all primes is infinite. Knowing the two necessary conditions, any sufficient condition for UPF-S cannot be weaker than these two conditions put together. The following theorem states that (C1) and (C2) together are not only necessary but sufficient conditions for UPF-S to hold.

Theorem 6. UPF-S *holds if and only if* S *is infinite and contains all the primes.*

Proof. We only need to prove the "if" part, and it is basically the same as that of the FTA. Suppose that S is infinite and contains all the primes. Noticing that the statement is true for 2, we assume that it is true for all numbers from 2 to $n-1$ for n greater than 2. The two assumptions on S assure that either $n \in S$ or n is composite. If $n \in S$, there is nothing to prove; otherwise $n = ab$ where $1 < a \leq b < n$, so that by induction hypothesis, a and b can be written as a product of primes in S, and so is n. We leave the proof of uniqueness to the reader. □

Concluding remarks. What we have obtained is as follows. Identifying the FTA as UPF-S for some set S of primes, we see that the FTA (for natural numbers) holds if and only if the associated set S is infinite and contains all primes. With this result, we now know that proving ET by using the FTA as follows

$$\begin{array}{l} \text{FTA} \Rightarrow \text{ET} \\ \text{FTA} \\ -\,-\,-\,-\,- \\ \qquad \therefore\ \text{ET} \end{array}$$

is actually a circular reasoning, since behind the FTA there is a hidden premise about the infinitude of primes involved. The same situation occurs in several existing proofs of ET that rely on the FTA. If we know that the FTA (for natural numbers) holds, we actually know that there are infinitely many primes involved in it.

Comparing to the original proof of the FTA for natural numbers, one might ask: where does the induction go wrong if we try to prove UPF-S for a finite set S of primes? First, we do not even know whether the statement is true for 2. Anyway, suppose $2 \in S$, so the statement is true for $n = 2$, and now we continue the induction process. As in the proof of ET, we know there must be a prime q which is not in S. Thus, when the induction arrives at this number, we have $q \notin S$ but q is not composite either. Hence the induction stops! In the proof of the FTA by induction, there is actually a hidden assumption that the number of primes involved is infinite, which makes the induction runs well.

References

[1] M. Aigner and G.M. Ziegler, *Proofs from THE BOOK*, Springer (2014)

[2] C.F. Gauss, *Disquisitiones Arithmaticae*, Leipzig (1801) [English translation by A.C. Clarke, Yale Univ. Press (1966)]

[3] S. Mac Lane and G. Birkhoff, *Algebra*, American Mathematical Society (1999)

[4] L.J. Rips, "Circular reasoning", *Cognitive Science* **26** (2002), 767–795

[5] D. Varberg, E. Purcell, and S. Rigdon, *Calculus*, 9th ed., Pearson International Edition (2006)

*H. Gunawan, Department of Mathematics, Institut Teknologi Bandung, Bandung 40132, Indonesia