# The History of the Fundamental Theorem of Arithmetic

Claire

December 2 2021

A long time ago, 2,321 years to be exact, lived a wise man named Euclid. Inspired by Theudius, Euclid spent long days and long nights discovering elements of geometry and unlocking universal facts about math [2]. Euclid's work led to many developments thousands of years later. One of which is the Fundamental Theorem of Arithmetic.

## 1 The Fundamental Theorem of Arithmetic

What is the Fundamental Theorem of Arithmetic?

**Fundamental Theorem of Arithmetic.** *Every integer greater than 1 can be factored as a product of primes in a unique way. [9]*

First off, there are prime numbers and composite numbers. **Prime numbers** are numbers which do not have any divisors except for one and the number itself. **Composite numbers** are positive integers which are not one and are not prime [7]. This is one of the important discoveries made by Euclid in 300 BC. To find a composite number, one can multiply several prime numbers a specific amount of times to get the final product:

Let $N$ represent a composite number. Let $a$, $b$, and $c$ represent prime numbers. Let $m$, $n$, and $y$ represent the exponents which the prime numbers are being multiplied to. One can suppose (because of what Legendre stated)

$$N = a^m * b^n * c^y$$

will always result in the unique make-up of a composite number [3]. For example, 3840 can be shown as:

$$3840 = 2^8 * 3^1 * 5^1$$

Taking from this it is shown that each number has one, and only one prime factorization (aside from the order), or the Fundamental Theorem of Arithmetic.

## 2 Euclid's Discoveries

Euclid wrote 13 books which made up a treatise called *The Elements*. Euclid's *Elements* were revolutionary, progressing math to a whole new level [2]. While Euclid didn't state the Fundamental Theorem of Arithmetic, VII.30 and VII.31 presented the basis to create it [3]. In Euclid's *Elements* Book VII it states:

**Proposition 30.** *If two numbers, multiplied by one another make some number, and any prime number measures the product, then it also measures one of the original numbers.*

**Proposition 31.** *Any composite number is measured by some prime number.*

Proposition 30 explains that when a prime number, $p$, divides a product of two numbers it will divide at least one of them. No composite number can have this property because if $c$ is a composite number, $c = ab$, so $c$ divides the product $ab$ but it doesn't divide either factor $a$ or $b$ [11].

Proposition 31 talks about how a prime number makes up composition numbers as it will be apart of the total sum of the number. This uses the unstated principle, "that any decreasing sequence of numbers is finite" [12].

Looking at the two propositions, one is able to find some similarities with the Fundamental Theorem of Arithmetic. Proposition 30 talks about how prime numbers are the make-up of composite numbers, and Proposition 31 builds off of that discussing how composite numbers are made up only prime numbers (and one). Proposition 30 actually is used to support IX.14 in *The Elements* Book IX:

**Proposition 14.** *If a number is the least that is measured by prime numbers, then it is not measured by any other prime number except those originally measuring it.*

Proposition 14 talks about how the "least common multiple of a set of prime numbers is not divisible by any other prime" [10]. This means that if a number is the least common multiple of the set of prime numbers, there is no other prime number outside that set that can divide it. Taking this

information, one can see how it translates to the Fundamental Theorem of Arithmetic. But there is a couple of problems. The Fundamental Theorem of Arithmetic starts with a positive integer greater than one. In these propositions it does not mention anything about positive integers. Also, Proposition 14 doesn't cover numbers in a square factor [3].

Nothing more came from Euclid on the subject of the Fundamental Theorem of Arithmetic. Time passed on. People translated *The Elements* and made newer versions of it, Euclid passed away, the Library of Alexandria burned down, and the Greek world crumbled. When this happened, the Islamic world "inherited the remains" [2].

## 3 al-Fārasī and His Work

al-Fārasī was one of the scientists in the Islamic world which built off of Euclid's work. His primary focus was optics, but he also made a lot of great contributions to number theory. In *Tadhkira al-ahbab fi bayan al-tahabb* or "Memorandum for friends on the proof of amicability" he introduced a lot of different ideas regarding "factorization and combinatorial methods" [1]. al-Fārasī worked with amicable numbers. According to the *Merriam-Webster.com Dictionary*, **amicable numbers** are "either of a pair of numbers each of which equals the sum of the different exact divisors of the other excluding the number itself." Before he was able to work on combinatorial methods, al-Fārasī had to "consider the existence of the factorization of an integer into prime numbers and to use uniqueness properties to determine the divisors" [3]. In *Tadhkira al-ahbab fi bayan al-tahabb* he shows that:

$$2^k pq, 2^k r \text{ whenever } p = 3 * 2^{k-1} - 1,$$
$$q = 3 * 2^{k-1} and\ r = 9 * 2^{2k-1}$$
$$\text{are all prime}, k \geq 2$$

al-Fārasī was the first one to state "every positive integer can be written as a finite product of prime numbers", which the equation above proves [9]. al-Fārasī's work sadly ended there in regards to the Fundamental Theorem of Arithmetic.

## 4 Prestet- New Beginning or Dead End?

Prestet came along in 1689 as a new light. Publishing *Nouveux Elemens de Mathematiques* he released the following theorem:

**Theorem.** *If two numbers b and c are relatively prime then the product bc is the least number each of them can divide exactly without remainder.*

Following this, Prestet wrote many different corollaries in hopes of "finding all the divisors of a given integer, computing the number of divisors of a given number, or determining the common measure of two numbers" [8]. Prestet used combinatorial arguments, like al-Fārasī and Pascal's arithmetical triangle, in order to find the precise number of divisors and conclude on his search for all divisors [8]. Prestet neither stated the existence nor the uniqueness of the Fundamental Theorem of Arithmetic, however he states in Corollary IX:

**Corollary IX.** *If the numbers a and b are simple, every divisor (of) aab of the three a, a, b is one of the three 1, a, aa or one of the different products of these three by b; that is to say, one of the six 1, a, aa, bb, ab, aab. Because all the alternative planes [i.e., obtained by multiplying the different factors two by two] of the simple a, a, b are aa and ab. [Analogous statements for aabb; aabbb; aab3cc; aab3ccd]. And so with the others [8].*

Corollary IX is an equivalent to the uniqueness theorem, only a portion of the Fundamental Theorem of Arithmetic [3]. All-in-all, Prestet's nontraditional work was not widely influential and added no new information [8]. The search for proof of the Fundamental Theorem of Arithmetic halts at another dead end.

## 5 Will Euler Be Our Hero?

To put it shortly, no. Euler does not save the day and prove the Fundamental Theorem of Arithmetic. He did, however, claim the Fundamental Theorem of Arithmetic existed. Since Euler was concerned with finding divisors, he only made a "method for finding the decomposition of any number into prime factors" [3]. A more interesting discovery is Euler's Product Formula:

$$\sum_{n\in N, n>0} n^{-s} = \prod_{\text{primes p}} (1-p^{-s})^{-1}$$

This formula is proven by the Fundamental Theorem of Arithmetic [14]. Later it was discovered the Fundamental Theorem of Arithmetic is provable through Euler's Product Formula. Dr. Jack D'Aurizio gives us the proof:

The answer is affirmative. Since

$$\frac{1}{1-p^{-s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots,$$

we have the identity:

$$\prod_p \frac{1}{1-p^{-s}} = \sum_{n\geq 1} \frac{h(n)}{n^s}$$

where $h(n) \in \mathbb{N}_{\geq 1}$ counts the number of ways of writing $n$ as a product of powers of different primes. Assuming $h(n) > 1$ for some $n$, the identity

$$\zeta(s) = \sum_{n\geq 1} \frac{h(n)}{n^s}$$

cannot hold for every $s \in \mathbb{R}_{>1}$. This proves the fundamental theorem of arithmetic.

Figure 1: Euler's Product Formula Proving the Fundamental Theorem of Arithmetic [4]

Sadly, this was only proven after Euler's death. Traveling back to 1700s, people are left with only knowing that the existence of the Fundamental Theorem of Arithmetic existed, but die-hard mathematicians craved the proof. The race to prove the theorem commenced.

## 6 The Winner

In 1801, Carl Freidrich Gauss published the *Disquisitiones Arithmeticae*. He had developed this book in his teenage years through abstract reasoning and numerical experimentation [4]. In this book he gave the proof for the Fundamental Theorem of Arithmetic and let the existence be known due to "elementary considerations" [3]. Due to this theorem, Gauss was able to share a link between the Euclidean algorithm and the factorial property "(which, however, was not explicitly clear, in Gauss's treatise, partly because of the presentation in terms of congruences)" [8]. *Disquisitiones Arithmeticae* is still a widely read book due to its relevance in number theory. Mathematicians claim for it to be a "work of genius" which opens up ideas and information to areas of mathematics which are still being explored today [4]. Gauss was a revolutionary in the field of mathematics for his groundbreaking proof of the Fundamental Theorem of Arithmetic.

## 7 So What Now?

Gauss helped solve the millennium long problem of "What is the Fundamental Theorem of Arithmetic?," but what came from the finding? A multitude of explanations came from the discovery and there was support to Euler's Product Formula as mentioned above. It also proved why one is not a prime number and how, because of the uniqueness theorem, it has different, and more distinctive, properties than a prime number. Alongside those discoveries, the Fundamental Theorem of Arithmetic helps mathematicians who were looking for divisors in their search proving that there is an individual make-up of each number (aside from the order). It also opened the floodgates for new mathematical discoveries in the field of number theory due to the "central concern" of number theory being prime numbers [15].

Nowadays, number theory is "essential in the design of public-key cryptographic algorithms" [15]. Public-key cryptography is used to secure processes like online transactions [5]. Number theory has also been used in areas like error-correcting code, numerical integration, computer arithmetic, and random and quasi-random number generation [5]. Since the Fundamental Theorem of Arithmetic has been proven and developed, the principles discovered from it have been able to help give a deeper understanding and meaning in the world of mathematics.

The quest for developing the Fundamental Theorem of Arithmetic is over. Since Gauss proved it in 1801, others have went to prove it in their own unique ways. The history behind the theorem goes to show how working together and building off of other's ideas is helpful, and it goes to show that even the small discoveries matter, and can lead to something huge.

## References


[1] Aldosray, Falih A.M. "Perfect, Amicable and Numbers of Equal Weights (Historical Notes)." *International Journal of Scientific and Innovative Mathematical Research (IJSIMR)*, vol. 4, no. 1, Jan. 2016, pp. 71–77., https://doi.org/https://www.arcjournals.org/.

[2] Allen, Donald G. "Euclid, Fl. 300 BCE." *Euclid.pdf*, https://www.math.tamu.edu/ dallen/masters/Greek/euclid.pdf

[3] Ağargün, A.Göksel, and E.Mehmet Özkan. "A Historical Survey of the Fundamental Theorem of Arithmetic." *Historia Mathematica*, vol. 28, no. 3, 2001, pp. 207–214., https://doi.org/10.1006/hmat.2001.2318.

[4] "Books." *Some Classical Maths*, 13 Jan. 2016, https://someclassicalmaths.wordpress.com/resources/books/.

[5] Cook, John D. "Applications of Number Theory Consulting." *John D. Cook — Applied Mathematics Consulting*, 24 June 2020, https://www.johndcook.com/blog/applied-number-theory/.

[6] D'Aurizio, Jack. "Is Euler Product Formula Equivalent to Fundamental Theorem of Arithmetic (Unique Factorization Theorem)?" *Mathematics Stack Exchange*, 29 Dec. 2014, https://math.stackexchange.com/questions/1084765/is-euler-product-formula-equivalent-to-fundamental-theorem-of-arithmetic-unique.

[7] Fortunado, Ismael. "Analyses and Formulas for the Set of Composite Numbers and the Set of Prime Numbers." *Science Journal Publication*, 2016, http://dx.doi.org/10.7237/sjms/110.

[8] Goldstein, Catherine. "On a Seventeenth Century Version of the 'Fundamental Theorem of Arithmetic.'" *Historia Mathematica*, vol. 19, no. 2, 1992, pp. 177–187., https://doi.org/10.1016/0315-0860(92)90075-m.

[9] Granville, Andrew. "The Fundamental Theorem of Arithmetic." *Fundamental.pdf*, Department De Mathematiques Et Statistique, Universite De Montreal, https://dms.umontreal.ca/ andrew/.

[10] Joyce, David E. "Proposition 14." *Euclid's Elements*, Book IX, Proposition 14, https://mathcs.clarku.edu/ djoyce/elements/bookIX/propIX14.html.

[11] Joyce, David E. "Proposition 30." *Euclid's Elements*, Book VII, Proposition 30, https://mathcs.clarku.edu/ djoyce/elements/bookVII/propVII30.html.

[12] Joyce, David E. "Proposition 31." *Euclid's Elements*, Book VII, Proposition 31, https://mathcs.clarku.edu/ djoyce/elements/bookVII/propVII31.html.

[13] Mullin, A. A. "Models of the Fundamental Theorem of Arithmetic." *Proceedings of the National Academy of Sciences*, vol. 50, no. 4, 1963, pp. 604–606., https://doi.or g/10.1073/pnas.50.4.604.

[14] "Primes-II." Primes-II.pdf, https://www.maths.tcd.ie/, https://www.maths.tcd.ie/pub/Maths/Courseware/428/Primes-II.pdf. If you go to https://www.maths.tcd.ie/pub/Maths/Courseware/428/ you are able to find the PDF. It is labelled Primes-II.

[15] Stallings, William. Cryptography and Network Security: Principles and Practice. Pearson. Education, Inc., 2019.

[16] Sprows, David J. "Irrationals and the Fundamental Theorem of Arithmetic." *The American Mathematical Monthly*, vol. 96, no. 8, 1989, p. 732., https://doi.org/10.2307/2324726.