Historia Mathematica **28** (2001), 207–214
doi:10.1006/hmat.2001.2318, available online at http://www.idealibrary.com on IDEAL®

A Historical Survey of the Fundamental Theorem of Arithmetic

Department of Mathematics, Yıldız Technical University, Davutpaşa Yerleşim Birimi, 34210 Esenler, İstanbul, Turkey

The purpose of this article is a comprehensive survey of the history of the Fundamental Theorem of Arithmetic. To this aim we investigate the main steps during the period from Euclid to Gauss. © 2001 Academic Press

Dans cet article nous donnons une vue d'ensemble de l'histoire du Theorème Fondamental de l'Arithmètique. Pour ce but nous considerons les moments principaux dans la periode de Euclide à Gauss. © 2001 Academic Press

MSC 1991 subject classifications: 01A30, 11-03, 11A51
Key Words: al-Fārisī; Euclid; Fundamental Theorem of Arithmetic.

1. INTRODUCTION

The concept of unique factorization stretches right back to Greek arithmetic and yet it plays an important role in modern commutative ring theory. Basically, unique factorization consists of two properties: existence and uniqueness. Existence means that an element is representable as a finite product of irreducibles, and uniqueness means that this representation is unique in a certain sense. Unique factorization first appeared as a property of natural numbers. This property is called the Fundamental Theorem of Arithmetic (FTA).

The history of the FTA is strangely obscure. We state the FTA as follows. Any natural number greater than 1 can be represented as a product of primes in one and only one way (up to the order). As we have stated it, it does not appear in Euclid's *Elements* [Heath 1908]. Nonetheless, Euclid played a significant role in the history of the FTA. Specifically, Books VII and IX contain propositions which are related to the FTA.

In his *Tadhkirat al-Ahbāb fī bayān al-tahābb* [Rashed 1982] al-Fārisī proved the existence of a prime decomposition, and subsequently gave all that is needed to prove its uniqueness. His Proposition 9 determines all of the divisors of a given number from a prime factorization. An analogous result can be found in Prestet's *Nouveaux Elemens de Mathématiques* (1689) [Goldstein 1992].

Following Prestet we can also mention Euler. In his book *Vollständige Einleitung zur Algebra* [Euler 1770] Euler assumed the existence property of the FTA and stated a result similar to al-Fārisī's and Prestet's to find all the divisors. Later Legendre proved the existence part of the FTA in his book *Théorie des nombres* [Legendre 1798] and assumed uniqueness when listing the factors of a given number but he did not state the FTA explicity. The first clear statement and proof of the FTA seem to have been given by Gauss in his *Disquisitiones Arithmeticae* [Gauss 1801]. After Gauss, many mathematicians provided different proofs of the FTA in their work [Ağargün & Fletcher 1997].

0315-0860/01 $35.00

2. EUCLID AND THE FTA

Euclid's *Elements* [Health 1908] consists of 13 books. The arithmetic Books VII to IX contain basic results in the theory of numbers. Although the FTA does not appear in the *Elements*, there are two very significant propositions, VII.30 and VII.31, which have a close connection with it. There is a third proposition, IX.14, which is a uniqueness theorem. In fact, the FTA follows from the propositions VII.30 and VII.31.

> VII.30. If two numbers by multiplying one another make some number, and any prime number measure the product, it will also measure one of the original numbers [i.e., if a prime number c measures ab, then c will measure a or b, where "measure" can be translated as "divide," although repeated subtraction would be nearer to the spirit of the Greek word].

> VII.31. Any composite number is measured by some prime number.

Easily, we get the existence (any natural number greater than 1 can be represented as a product of primes) by VII.31, and the uniqueness (i.e., this representation is unique up to the order) by VII.30. Nowadays many mathematicans would prove the FTA by using these propositions. For the uniqueness suppose $p_1 \cdots p_n = q_1 \cdots q_m$ are two prime decompositions of any given positive integer. Then, from VII.30 we have $p_1 \mid q_1$, say, and hence $p_1 = q_1$. Similarly we have the same thing for all p's and q's and so it follows that $n = m$. However, Euclid did not state the FTA following the above propositions in Book VII.

In Book IX we meet Proposition 14 which states that "If a number be the least that is measured by prime numbers, it will not be measured by any other prime number except those originally measuring it."

There are many similarities between the FTA and IX.14. Proposition IX.14 is one kind of uniqueness theorem. It is a good partial demonstration of the uniqueness condition for the FTA, but it is clear that IX.14 does not cover the case of numbers which possess a square factor. For this reason some authors (e.g., [Hendy 1975, Mullin 1965]) have examined IX.14, and have correctly asserted that the two results (IX.14 and the FTA) are not technically equivalent.

In addition, we have to note that without implying the existence of a prime decomposition IX.14 starts with a collection of primes while the FTA starts with an integer. The starting points of the two theorems are completely different.

Nowadays, textbooks commonly take the FTA as a fundamental theorem. They begin with the definition of prime numbers and prove the uniqueness of factorization into primes. This is followed by the properties of relatively prime integers and greatest common divisors. This approach seems to have originated with Gauss. In Euclid's number theory things are organized just in the reverse order. Euclid begins with the division algorithm to find the greatest common divisor of integers, and then he obtains an operative definition of relatively prime integers. From the investigation of being relatively prime, he eventually finds results on prime numbers, including in particular the important Proposition VII.30, and then he states Proposition VII.31 (see above) in the reverse order again. In Euclid's theory the FTA would lose much of its significance. Far from being fundamental, IX.14 is placed at the end of Euclid's arithmetic theory. It does not make use of propositions other than VII.30 and VII.36. It cannot be considered the culmination of any major part of the theory, nor it is used in any subsequent result.

3. AL-FĀRISĪ AND THE FTA

Kamāl al-Dīn al-Fāriśī, who died ca. 1320, was a great Persian mathematician, physicist, and astronomer. His work represents perhaps the most significant step toward the FTA made by mathematicians before Gauss. His results appear in *Tadhkirat al-Ahbāb fībayān al-tahābb* (which means "memorandum for friends explaining the proof of amicability"). His main concern was amicable numbers, and his aim was to prove by a different method the theorem of Ibn Qurra that states "if three numbers $p = 3.2^{n-1} - 1,\ q = 3.2^n - 1$, and $r = 9.2^{2n-1} - 1$ are prime, and if $p, q > 2$, then the pair $2^n pq$ and $2^n r$ are amicable" [Hogendijk 1985]. Ibn Qurra (836–901) had worked only lightly on the decomposition of integers and combinatorial methods. Al-Fāriśī was led to develop new ideas in the theory of numbers, and he investigated the decomposition of integers more thoroughly than Ibn Qurra did. Before he could introduce combinatorial methods it was necessary to consider the existence of the factorization of an integer into prime numbers and to use uniqueness properties to determine the divisors.

In [Ağargün & Fletcher 1994] we produced an English translation of his first nine propositions and provided a commentary on al-Farisi's methods. The main aim of these nine propositions is to know and to find the divisors of a given number and hence is a preparation for the work on amicable numbers.

One could say that Euclid takes the first step on the way to the existence of prime factorization, and al-Fāriśī takes the final step by actually proving the existence of a finite prime factorization in his first proposition.

PROPOSITION 1. *Each composite number can be decomposed into a finite number of prime factors of which it is the product.*

Suppose that $a > 1$ is a composite integer. Therefore, from Euclid VII.31 it possesses a prime divisor b. Then for $1 < c < a$,

$$a = bc.$$

If c is prime then the proposition is proved; otherwise c possesses a prime divisor d and for $1 < e < c$ we write

$$c = de.$$

If e is prime then the proposition is proved since $a = bde$. Otherwise we repeat the process a finite number of times and at the end we decompose a composite factor into two prime factors since a finite number cannot be made up of an infinite product of numbers. Then we write for prime k

$$a = bd \cdots k$$

This proposition is the first known statement and proof of the existence of a prime factorization for any composite number. After al-Fāriśī, Prestet did not state it but used it to determine all the divisors of a given integer. Euler stated and used it to find divisors. Eventually Legendre stated and proved it.

Al-Fārisī's propositions 2 to 5 are the following:

PROPOSITION 2. *When three numbers a, b, c, are given, the ratio of the first to the third is composed from the ratio of the first to the second and from the ratio of the second to the third.*

PROPOSITION 3. *The ratio of* 1 *to any composite number is composed of its ratio to each of the prime factors.*

PROPOSITION 4. *Any two composite numbers which have the same decomposition into factors are identical.*

PROPOSITION 5. *Any two distinct composite numbers do not have the same decomposition into factors.*

After Proposition 5 al-Fārisī took the first step to determine all the divisors of an integer. He did not consider the integer itself as a divisor. There, as with Prestet and Euler, the main starting point was the prime decomposition.

PROPOSITION 6. *If a composite number a is decomposed into prime numbers b, c, d, e, . . . , k, then two by two bc, bd, be, . . . , etc., three by three bcd, bce, . . . , etc., and so on, all of these are divisors of a.*

Then al-Fārisī proved Proposition 7, which he used in proving Proposition 8.

PROPOSITION 7. *If* $a \nmid b$, *then for* $n = 3, 4, \ldots, a^2 \nmid ba$ *and* $a^n \nmid ba$; $a^3 \nmid ba^2$ *and* $a^{n+1} \nmid ba^2$; $a^4 \nmid ba^3$ *and* $a^{n+2} \nmid ba^3$ *and so on.*

Here we give Proposition 8, which is used in the succeeding proposition.

PROPOSITION 8. *Here, if a composite number a is decomposed into its prime factors as* $a = bcd \cdots k$, *then if one of them, say b, does not repeat in a then* $b^2 \nmid a$ *and for* $n = 3, 4, \ldots, b^n \nmid a$. *And if b repeats once only then* $b^2 \mid a$ *but* $b^n \nmid a$. *And if b repeats twice only then* $b^2 \mid a$, $b^3 \mid a$, *but* $b^{n+1} \nmid a$.

To determine all of the divisors of a given composite integer, al-Fārisī proved Proposition 9. In this proposition we observe that all of the previous propositions are used directly or indirectly. We see a similar result in Prestet and Euler, but of course Proposition 9 was presented long before, and as far as we know this is the first known result to determine all the divisors of a given composite number. Once more, there the main starting point was the prime decomposition.

PROPOSITION 9. *If a composite number a is decomposed into its prime factors as* $a = bcdh \cdots kl$, *then a has no divisor except* 1 *and* $b, c, d, h, \ldots, k, l$, *and two by two* $bc, bd, \ldots,$ *etc., and three by three* $bcd, bch, \ldots,$ *etc.,* $\ldots,$ *and the products of all factors except one:* $cdh \cdots kl, bdh \cdots kl, \ldots, bcdh \cdots k$.

Obviously $1, b, c, d, \ldots, k, l$ are divisors of a. The others are immediately divisors from Proposition 6. Suppose a has another divisor z which is either prime or composite. If z is a prime then we consider a as b $(cdh \cdots l)$ and $z \mid b(cd \cdots l)$ implies $z \mid cdh \cdots l$ from Euclid VII.30. Similarly $z \mid c(dh \cdots l)$ implies $z \mid dh \cdots l$. Therefore, by the same process we have $z \mid kl$. Hence $z \mid k$ or $z \mid l$ and this implies $z = k$ or $z = l$. This is a contradiction. Suppose now z is a composite number and it is distinct from those previous divisors already stated. Therefore, from Proposition 5 there exists one among the prime factors of z which does not appear among the factors of a, or if this one factor does not exist, then there is one factor of z which does not repeat the same number of times in z and a. Thus we have three possible cases: (i) z has a prime factor which does not appear among the factors of a, or if z has no such factor then (ii) one factor of z has more repetitions than in the factors of a, or (iii) one factor of a repeats itself more than in the factors of z.

If it is the first and h is a prime number distinct from all factors of a, then this is a contradiction from the previous case, where z is assumed to be a prime number.

If it is the second, that is one factor of z, say p, repeats n times in z but less than n times in a, then $p^{n+1} \mid z$ and $p^{n+1} \mid a$, which is impossible, from Proposition 8.

If it is the third, that is, all factors of z do not repeat more times than in the factors of a, then z becomes a divisor of a, which had been mentioned, and this is a contradiction.

We see that al-F$\bar{a}$ris$\bar{\imath}$ made an important advance towards the FTA, although he did not state it. He stated and proved the existence part of the FTA, but he did not state and did not intend to prove the uniqueness of prime factorization since the FTA was not important for him. This does not mean he did not know the uniqueness. If al-F$\bar{a}$ris$\bar{\imath}$ had wished to state and prove the uniqueness, he would have been able to do so. al-F$\bar{a}$ris$\bar{\imath}$ knew the uniqueness very well as can be seen from both the statement and the proof of his Proposition 9. In fact, he proved Proposition 9 in order to determine all the divisors of a composite number and he used it to give a new proof of ibn Qurra's theorem on amicable numbers. However, he showed all that is needed to prove the uniqueness. Therefore we can consider Proposition 9 to be equivalent to the uniqueness part of the FTA.

4. PRESTET'S RESULTS

In this section we present some results published by Jean Prestet in his 1689 *Nouveaux Elemens de Mathématiques* [Goldstein 1992]. They confirm that before modern times a prime factorization was not looked upon as something of interest in its own right, but as a means of finding divisors.

Prestet stated neither the existence nor the uniqueness of the FTA. He was influenced by Euclid and was concerned with divisors. Like al-F$\bar{a}$ris$\bar{\imath}$ and Euler he gave the main results in order to find all the divisors of a given number. In particular his Corollary IX has a significant role. This result makes us believe that Prestet knew the FTA. We think he could have proved it, but he was not concerned with it.

In Chapter 6 of his first volume, we meet the following theorem.

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

As a corollary of this theorem Prestet stated:

COROLLARY III. *If d measures exactly a product bc of two numbers b & c and if c and d are relatively prime; the number d is a divisor of the other number b.*

The object of the next corollaries was to determine all the divisors of a number expressed as a product of prime factors.

COROLLARY IV. *If two different numbers a & b are simple, every divisor of their plane, or product ab, is* 1*, or a, or b, or ab.*

Prestet continued with Corollaries V and VI using the same argument for a product of three different prime numbers (*solid*) and of four prime numbers (*supersolid*), then five, and so on indefinitely.

In the following corollary he studied the powers of some prime number.

COROLLARY VIII. *If the number a is simple, every divisor of its square aa is one of the three* 1*, a, aa. And every divisor of its cube* a^3 *one of the four* $1, a, a^2, a^3$ $(\cdots)$*. And so with the others to infinity.*

Finally, he gave

> Corollary IX. *If the numbers a & 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,* 1*b, 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 & ab.* [Analogous statements for $aabb$; $aabbb$; aab^3cc; aab^3ccd]. *And so with the others.*

It is clear that Prestet does not state the FTA in his work because his aim was to make explicit the relationship between any factorization of a given number into primes and all its possible divisors. However, Prestet's results are very close to the FTA, and in the sense of implying each other his Corollary IX may be considered as equivalent to the uniqueness of the prime factorization.

5. EULER'S STATEMENTS

In his *Vollständige Einleitung zur Algebra* [Euler 1770] Leonard Euler stated the existence part of the FTA without proving it properly, and also he gave a statement for the uniqueness part analogous to al-Fārisī's Proposition 9 and Prestet's Corollary IX.

In Article 41 of Chapter IV of Section I of Part I Euler stated the existence of prime factorization and provided a partial proof of it. But his proof omits some details.

> 41. All composite numbers, which may be represented by factors, result from the prime numbers above mentioned; that is to say, all their factors are prime numbers. For if we find a factor which is not a prime number, it may always be decomposed and represented by two or more prime numbers. When we have represented, for instance, the number 30 by 5×6, it is evident that 6 not being a prime number, but being produced by 2×3, we might have represented 30 by $5 \times 2 \times 3$, or by $2 \times 3 \times 5$; that is to say, by factors which are all prime numbers.

In Article 43, for instance, Euler gave a method for finding the decomposition of any number into its prime factors:

> 43. Hence, it is easy to find a method for analysing any number, or resolving it into its simple factors. Let there be proposed, for instance, the number 360; we shall represent it first by 2×180. Now 180 is equal to 2×90, and
>
> $$90 \quad \text{is the same as} \quad 2 \times 45$$
> $$45 \quad \text{is the same as} \quad 3 \times 15$$
>
> and last
>
> $$15 \quad \text{is the same as} \quad 3 \times 5,$$
>
> so that the number 360 may be represented by the simple factors $2 \times 2 \times 2 \times 3 \times 3 \times 5$, since all these numbers multiplied together produce 360.

Euler did not state the uniqueness of factorization into primes, but he gave a related statement without proof in Article 65 of Chap. VI of Sect. 1 of Part 1 of Euler [1770].

> 65. When, therefore, we have represented any number assumed at pleasure, by its simple factors, it will be very easy to exhibit all the numbers by which it is divisible. For we have only, first, to take the simple factors one by one, and then to multiply them together two by two, three by three, four by four, &c. till we arrive at the number proposed.

We observe that Euler was only interested in finding all divisors of a number and he was following the tradition of al-Fārisī and Prestet. In Article 65, Euler tells us that all divisors of a number are obtained from the prime factors which appear in the representation of the number as a product of prime numbers and this is the only way to have all the divisors of

the number. Therefore this may be considered as the uniqueness of the prime factorization. Euler also gave an example at the end of Article 64: It follows that 60, or $2 \times 2 \times 3 \times 5$, may be divided not only by these simple numbers, but also by those which are composed of any two of them; that is to say, by 4, 6, 10 and 15; and also by those which are composed of any three of its simple factors; that is to say, by 12, 20, 30, and last also, by 60 itself.

6. LEGENDRE

Here we give Legendre's statement which can be found in [Legendre 1798, Art. VIII]:

> Any not prime number N can be represented by a product of several prime numbers α, β, γ, etc., each raised to some power, so that one can always suppose $N = \alpha^m \beta^n \gamma^p$, etc.

Then his proof immediately follows as:

> The method to follow in order to perform this decomposition, consists in trying to divide N by each of the prime numbers 2, 3, 5, 7, 11, etc., starting with the smallest. When the division is successful with one of these numbers α, one repeats it as many times as is possible, for example, m times, and calling the last quotient P, we have
>
> $$N = \alpha^m P.$$
>
> The number P cannot be divided by α, and it is useless to try to divide P by a prime number less than α, for if P were divisible by θ, where θ is less than α, it is clear that N would also be divisible by θ, contrary to the hypothesis. We must therefore try to divide P by prime numbers greater than α; thus we will obtain in succession
>
> $$P = \beta^n Q, \quad Q = \gamma^p R, \text{ etc.},$$
>
> which will give $N = \alpha^m \beta^n \gamma^p$, etc.

As we see by this proof, for any number we always have the same decomposition into prime factors according to Legendre's method. Clearly we cannot suppose that this is equivalent to the uniqueness part of the FTA. However, a statement related to uniqueness is given in Article X:

> A number N being expressed in the form $\alpha^m \beta^n \gamma^p$, etc., each divisor of N will also be of the form $\alpha^\mu \beta^\nu \gamma^\pi$, etc., where the exponents μ, ν, π, etc. will not be greater than m, n, p, etc. . . .

In this article, in fact, Legendre intended to find the number of all divisors of a number, and at the same time the sum of these same divisors. From this statement we can easily prove uniqueness.

7. GAUSS

Gauss gave the unique factorization property for positive integers in Article 16 of his *Disquisitiones Arithmeticae* [Gauss 1801]. Section II opens with the following article.

> 13. THEOREM. *The product of two positive numbers each of which is smaller than a given prime number cannot be divided by this prime number.*

Then Gauss reproduced Theorem VII.32 of Euclid's *Elements* and its generalization.

> 14. If neither a or b can be divided by a prime number p, the product ab cannot be divided by p.

15. If none of the numbers *a, b, c, d,* etc. can be divided by a prime p neither can their product $abcd$, etc.

Here we give his Article 16.

16. THEOREM. *A composite number can be resolved into prime factors in only one way.*

Gauss himself did not spell out a proof of the existence part of the FTA. He claimed that it is clear from elementary considerations, which of course is. He began his demonstration by stating that "It is clear from elementary considerations that any composite number can be resolved into prime factors, but it is tacitly supposed and generally without proof that this cannot be done in many various ways." Then he considered a composite number $A = a^\alpha b^\beta c^\gamma$ etc. with a, b, c, etc. unequal prime numbers and showed that A cannot be resolved into prime factors in another way which has any other primes except a, b, c, etc., or which has some prime numbers which appear in one decomposition more often than in the other.

Thus, the first clear statement and proof of the FTA seem to have been given by Gauss in his *Disquisitiones Arithmeticae*. Since then many different proofs have been given. In [Ağargün & Fletcher 1997], we have investigated different proofs of the FTA and classified them.

REFERENCES

Ağargün, A. G. & Fletcher, C. R. 1994. al-Fārisī and the Fundamental Theorem of Arithmetic.*Historia Mathematica* **21**, 162–173.

———1997. The fundamental theorem of arithmetic dissected. *Mathematica Gazette* **81**, No. 490, 53–57.

Euler, L. 1770. *Vollständige Einleitung zur Algebra.* St. Petersburg; French translation with *Additions* by Joseph L. Lagrange. Lyon, 1774; republished in Vol. 7 of Lagrange's *Oeuvres* and in Vol. (1)1 of Euler's *Opera*; English translation *Elements of Algebra* [trans. John Hewlett, London, 1840], reprinted Berlin/Heidelberg/New York: Springer-Verlag, 1985.

Gauss, C. F. 1801. *Disquisitiones Arithmeticae*. Leipzig; Translated into English by A. C. Clarke. New Haven, CT: Yale University Press, 1966.

Goldstein, C. 1992. On a seventeenth century version of the fundamental theorem of arithmetic. *Historia Mathematica* **19**, 177–187.

Heath, T. L. 1908. *The Thirteen Books of Euclid's Elements*, Vol. 2. Cambridge, UK: Cambridge University Press.

Hendy, M. D. 1975. Euclid and the Fundamental Theorem of Arithmetic. *Historia Mathematica* **2**, 189–191.

Hogendijk, J. P. 1985. Thabit ibn Qurra and the pair of amicable numbers 17296, 18416. *Historia Mathematica* **12**, 269–273.

Knorr, W. R. 1976. Problems in the interpretation of Greek number theory: Euclid and the Fundamental Theorem of Arithmetic. *Studies in the History and Philosophy of Science* **7**, 353–368.

Legendre, A. M. 1798. *Théorie des Nombres*, 3rd ed. Paris: Firmin Didot, 1830; reprinted Paris: Hermann, 1990.

Mullin, A. A. 1965. Mathematico-philosophical remarks on new theorems analogous to the Fundamental Theorem of Arithmetic. *Notre Dame Journal of Formal Logic* VI, No. 3, 218–222.

Rashed, R. 1982. Matériaux pour l'histoire des nombres amiables. *Journal for the History of Arabic Science* **6**, 209–278.