al-Fārisī and the Fundamental Theorem of Arithmetic

AHMET G. AĞARGÜN

Matematik Bölümü, Fen Fakültesi, Yildiz Üniversitesi, Istanbul, Turkey

AND

COLIN R. FLETCHER

Department of Mathematics, University of Wales, Aberystwyth, Dyfed SY23 3BZ, United Kingdom

The work of al-Fārisī on amicable numbers begins with nine propositions of elementary number theory. The purpose of this article is to produce an English translation of these propositions and to provide a commentary on al-Fārisī's methods. In particular we consider whether he proved, or attempted to prove the Fundamental Theorem of Arithmetic. © 1994 Academic Press, Inc.

L'oeuvre d'al-Fārisī concernant les nombres amiables, débute avec neuf propositions de la théorie des nombres élémentaires. Le but de cet article est de donner une traduction en anglais de ces propositions ainsi qu'un commentaire sur les méthodes d'al-Fārisī. En particulier l'on examine s'il a démontré, ou essayé de démontrer, le théorème fondamental de l'arithmétique. © 1994 Academic Press, Inc.

Das Werk über befreundete Zahlen von al-Fārisī beginnt mit neun Sätzen der elementaren Zahlentheorie. Das Ziel dieses Aufsatzes ist, eine englische Übersetzung dieser Sätze zu geben und einen Kommentar über al-Fārisīs Methoden beizusteuern. Insbesondere prüfen wir, ob er den Fundamentalsatz der Arithmetik bewiesen hat oder versucht hat zu beweisen. © 1994 Academic Press, Inc.

MSC 1991 subject classifications: 01A30, 11-03, 11A51
KEY WORDS: al-Fārisī, amicable numbers, Fundamental Theorem of Arithmetic.

1. INTRODUCTION

The Persian mathematician Kamāl al-Dīn al-Fārisī, who died circa 1320, was the author of a mathematical treatise, "Tadhkirat al-Aḥbāb fī bayān al-Taḥābb," which could be translated as "Memorandum for Friends Explaining the Proof of Amicability." Rashed edited the Arabic text in [7] and investigated sections of it in [8]. Brentjes disagreed with part of Rashed's analysis in [1].

The main concern of al-Fārisī was amicable numbers, and his aim was to prove afresh the theorem of Thābit ibn Qurra (see, e.g., Hogendijk [4]) on the construction of amicable numbers, which was rediscovered by Fermat and Descartes in the 17th century. However, in order to achieve this aim, al-Fārisī first set down certain theorems of elementary number theory. It is the purpose of this article to produce an English translation of these theorems and to give a commentary, in

0315-0860/94 $6.00
Copyright © 1994 by Academic Press, Inc.
All rights of reproduction in any form reserved.

particular with regard to the so-called Fundamental Theorem of Arithmetic (FTA), that is, the existence and uniqueness of prime decompositions of positive integers.

Rashed, in an apt sentence [8, 124] claims that

> Parmi les grands théorèmes, rares sont, il est vrai, ceux qui ont une histoire, aussi pauvre que celle du théorème fondamental de l'arithmétique.[1]

But he sees the FTA in the work of al-Fārisī. In his view Proposition 1 is a statement and proof of the existence of prime decompositions, and Propositions 4 and 5 are al-Fārisī's (unsuccessful) attempt to prove uniqueness. (The latter two results are designated Propositions 2 and 3 in [8].) Our analysis of these theorems is somewhat different. In one sense al-Fārisī comes out of this badly, because the actual statement of uniqueness disappears, while in another, his reputation is enhanced. We conclude that Propositions 4 and 5 actually prove what they purport to prove (and are thus "successful"), and that, moreover, the statement and proof of Proposition 9 come closer to the concept of uniqueness than any other known work before its time. Amicable numbers are defined in terms of divisors, and al-Fārisī in this Proposition 9 determined the divisors of an integer in terms of a prime decomposition. To our modern eyes it seems inconceivable that a mathematician, having proved the existence of prime decompositions and with their uniqueness within his grasp, would miss the chance of stating such a celebrated theorem, even as a mere corollary to Proposition 9. But al-Fārisī clearly was not influenced by the number theory produced between 1801 and 1993. He proved that he could find the divisors of an integer from a prime decomposition, whose existence he also proved. Since he did not need uniqueness, he left it out. It would be tempting to add that he also left it out because it was obvious, in much the same way as Prestet 400 years later [3] or Legendre 100 years after that [5]. What is obvious, although never stated, is that the set of divisors of an integer is unique, but this has nothing to do with the FTA. The set of divisors of any element in any system, whether this system possesses uniqueness of factorization or not, is a unique set, simply because the concept of a divisor is well defined.

2. TRANSLATION AND COMMENTARY

This work of al-Fārisī is clearly modeled on the *Elements* of Euclid. It takes the same form with a list of definitions followed by propositions. The definitions are his own, whereas all of Euclid's definitions are assumed to be known. When al-Fārisī refers to one of Euclid's propositions to justify a step in a proof, he omits the name of Euclid and simply refers to the book and proposition numbers.

In what follows we have tried to steer a middle course between a literal translation and a more modern version. For example, the word for "side" has been translated as "factor," and that for "area" as "product." On the other hand the

[1] Rashed then steps aside from al-Fārisī, and delivers a well-aimed broadside at commentators who see in Euclid's *Elements* something which is plainly not there, or who offer excuses on Euclid's behalf because it is not there. This section, pages 124–126, is, in our opinion, one of the best critiques of the mathematical literature concerning Euclid and the FTA.

word "measure" has been retained to emphasize subtraction rather than division. We have inserted extra words in square brackets where these are deemed necessary, either as an explanation of a possible ambiguity or to flesh out the English sentence. We begin the translation with the definitions, contained in six paragraphs.

> Each number made up by multiplying a number with another number, I call it (thunā'ī) a double number. And if it is made up by multiplying a number with another number then with a third, I call it (thulāthī) a triple. And if it is made up by multiplying a triple with a fourth, I call it (rubāᶜī) fourthfold, and so on.
>
> And the factors of each composite [number] are either equal or not. I call the first type (mutasāwiyah al-aḍlāᶜ) of equal factors; the second type (mutafāḍilah al-aḍlāᶜ) of different factors, either all of its factors are different as in the [number] composed of *a*, *b*, *c*, or some of its factors are different as in the number composed of *a*, *b*, *b*.
>
> And if the numbers of factors of two composite numbers are the same, then I call these two [composite numbers] (mutamāthilā al-aḍlāᶜ) corresponding in factors, or if not [I call them] (mutafāḍilāhā) different in them.

The word "prime" has not yet been mentioned, and indeed does not occur until the first proposition. As for the technical term "corresponding in factors," this is not altogether clear, but it seems to indicate that the total number of (not necessarily distinct) factors is the same for each composite number, and the inference is that al-Fārisī is considering the factors to be prime.

> Two composite numbers which have the same decomposition into factors (mutaḥaddā al-aḍlāᶜ) are those which have equal and corresponding (mutamāthil) factors, where each repeated factor in one of them is repeated the same number [of times] in the other.
>
> The genera [i.e., the powers] of a number are its (murabbaᶜ uhu) square and its (mukaᶜᶜabuhu) cube and so on indefinitely.
>
> The (silsilah) chain of a number is the series of numbers beginning with the number itself, and second its square, then its cube, and so on for the rest of the consecutive genera. The number itself and its genera are the terms of this chain.
>
> PROPOSITION 1. *Each composite [number] can necessarily be decomposed into a finite number of prime factors of which it is the product.*
>
> Let *a* be a composite number; since it is composite it is necessarily measured by a prime from Book VII.31 of the Elements. Let this [prime] be *b*, and let it [i.e., *b*] measure it [i.e., *a*] by *c*. If *c* is a prime then it is shown that it [i.e., *a*] is made up by multiplying prime *b* and prime *c*. If it [i.e., *c*] is composite then let it be measured by a prime *d* according to the number *e* [i.e., $c = de$]. If *e* is prime then it is clear that *a* is made up by multiplying the prime numbers *b*, *d*, and *e*. Otherwise we perform our operation until the composite factor is in the end decomposed into two prime factors. Then *a* is made up from the previous primes together with those two primes. If it never can be decomposed into two prime factors, then it would necessarily follow that the finite would be made up from an infinite product of numbers, which is absurd. And that is what we wanted.

This is the first known statement and the first known proof of the existence of a prime decomposition of a given composite number. The Euclidean result quoted states that "any composite number is measured by some prime number" [2, 332]. This is the first step on the road to proving al-Fārisī's Proposition 1, but it is not the existence theorem itself. No amount of juggling with words or economizing with the truth can turn the statement of VII.31 into Proposition 1. Note that al-Fārisī, in the final stage, uses an argument by contradiction.[2]

> PROPOSITION 2. *If there are three numbers a, b, c the ratio of the first to the third is made up from the ratio of the first to the second and from the ratio of the second to the third.*
>
> Thus let the square of b be h, and let its product with a be d, and with c be z. Since d is composite—its factors are a, b—and z is composite—its factors are b, c—the ratio of d to z is made up from the ratios of a to b and of b to c from Book VIII.5. But since b was multiplied by itself and a to get h and d [respectively], so the ratio of a to b is equal to the ratio of d to h from Book VII.18; and similarly the ratio of b to c is equal to the ratio of h to z. Then ex aequali the ratio of a to c is equal to the ratio of d to z, which is made up from the other two ratios. And this is what we wanted.

This proposition raises several questions. The proof itself is a little strange, although we are confident of our interpretation. The statement of the result appears correct, although it is not entirely clear what al-Fārisī's view of the statement is. The difficulty concerns his understanding of the composition of ratios. The only likely explanation is that al-Fārisī was considering the compounding of ratios, but this posed a problem, whether he realized it or not, because nowhere in the *Elements* does Euclid define this operation on ratios [2, 132]. The standard practice (see Euclid [2, 132] and Mueller [6, 87]) in compounding two ratios $k:l$ and $m:n$ was to find u, v, w such that

$$k:l = u:v \qquad \text{and} \qquad m:n = v:w.$$

Then

$$(k:l)(m:n) = u:w,$$

where the compound operation is denoted here by juxtaposition.

Proposition 2 states that for any three numbers a, b, c

$$(a:b)(b:c) = a:c,$$

which follows immediately from the standard procedure. There must be some explanation as to why al-Fārisī did not follow this course. It may well be that he was unaware of the procedure for compounding ratios. Alternatively he may have been concerned about the general definition of compounding. How does one find u, v, and w? Without further information it cannot be done, but for natural numbers Euclid had already solved the problem in VIII.4 of the *Elements*.[3]

[2] This contradiction argument is akin to the use of the Archimedean axiom. If b is the first prime factor of a determined by the construction, then $b < a$, and by the axiom there is a multiple of b which exceeds a. Hence the product of the primes will eventually exceed a if the number of these primes is unlimited. Another method would be to consider the diminishing sequence of composite divisors and then use the descending chain condition (i.e., Fermat's method of infinite descent) or the well-ordering principle.

[3] There are other possibilities. The work was clearly based on Euclid's *Elements*, and it would have been natural to follow Euclid's way, not give the definition and work within the Euclidean corpus. In any case, al-Fārisī's main concern was amicable numbers and not the theory of proportions.

For the proof al-Fārisī puts

$$b^2 = h, \qquad ba = d, \qquad bc = z.$$

Then $d : z = ba : bc = (a : b)(b : c)$ from VIII.5. For the proof that $d : z = a : c$ al-Fārisī uses ex aequali (VII.14), although a straightforward application of VII.18 would have seemed the obvious route, especially as he has to use VII.18 twice anyway.

Since

$$a : b = ba : bb = d : h \qquad \text{(VII.18)}$$

and

$$b : c = bb : bc = h : z \qquad \text{(VII.18)}$$

then ex aequali

$$a : c = d : z \qquad \text{(VII.14)}$$

and the result follows.[4]

PROPOSITION 3. *The ratio of the unit to any composite number is made up from its ratio to each of its prime factors.*

Thus let the composite number be a and let its prime factors be [as follows]. Let there first be two [prime factors] b, c; then we say that since b was multiplied by c to get a [so] the ratio of b to a is equal to the ratio of the unit to c. And the ratio of the unit to a is made up from the ratios of the unit to b and of b to a. So the ratio of the unit to a is made up from its ratios to b and c.

Let the factors be more than two, namely b, c, d, and let [the number] made up of b times c [be] h. Since a is made up from h and d, the ratio of the unit to a is made up from its ratios to h and d. And the ratio of the unit to h is made up from its ratios to its two factors [i.e., the factors of h], I mean b and c; [therefore] the ratio of the unit to a is made up from its ratios to b and c and d. And similarly we prove [it] if the factors are more than three. This is what we wanted.

Here al-Fārisī is showing that a ratio $1 : a$ can be expressed as the compound of several ratios, and he uses Proposition 2.

If $a = bc$ then $b : a = b : bc = 1 : c$ from VII.18. And from the previous proposition

$$\begin{aligned} 1 : a &= (1 : b)(b : a) \\ &= (1 : b)(1 : c). \end{aligned}$$

In fact his proof breaks down when he considers three prime factors b, c, d because he cannot claim that

$$1 : a = (1 : bc)(1 : d)$$

[4] It is perhaps worth mentioning that VII.14 (ex aequali) can be looked upon as the proof of the uniqueness of the compounding operation. Euclid is silent on this point (as are Heath (in [2]) and Mueller [6]).

from the first part since bc is not prime. However the situation is easily rectified since all references to the word "prime" may be omitted.

> PROPOSITION 4. *Any two composite numbers which have the same decomposition into factors are corresponding* [*i.e., identical*];
>
> such as a and b, each of which is composed of the factors c, d, e. The reason is [that] the ratio of the unit to each of them is made up from its ratios to each of c, d, e, so the ratios of the unit to the two of them [i.e., a and b] are equal. Therefore they are corresponding. This is what we wanted.

If $a = cde$ and $b = cde$ then from Proposition 3

$$1:a = (1:c)(1:d)(1:e) \qquad \text{and} \qquad 1:b = (1:c)(1:d)(1:e).$$

Therefore $1:a = 1:b$ and so $a = b$. This last step is not explained by al-Fārisī. Perhaps it was regarded as obvious or perhaps he was using a result from the *Elements* without giving a reference. Two likely candidates are V.9 ($x:a = x:b$ implies $a = b$) and VII.19 ($u:a = v:b$ if and only if $ub = va$). We note that, strictly speaking, al-Fārisī requires Proposition 3 in its general form since the factors of a and b are not stated specifically to be prime.

> PROPOSITION 5. *Any two distinct composite numbers do not have the same decomposition into factors,*
>
> but it is necessary that the prime factors of one [of them] be different from the [prime] factors of the other, either some of these [factors] are different if they are different in factors, or they are different in the number of repetitions of some of them if they are corresponding in factors; if not then they have the same decomposition into factors and therefore they are corresponding [i.e., identical], but they were assumed to be distinct. This is a contradiction. That is what we wanted.

This proposition is the contrapositive of the previous one, and is therefore equivalent to it. The proof follows immediately via a contradiction argument. But there is a *prima facie* doubt about the status of the first part of the argument contained in the opening sentence. It is only here that the word "prime" is used. The statement of the proposition and the remaining proof can stand together without the word "prime" and without the opening sentence. It is possible that al-Fārisī in this sentence is expressing the proposition in the form in which he is going to need it in Proposition 9; that is, if a is a composite number expressed as a product of primes, and S is the set of all numbers expressed as products of these primes leaving out at least one prime factor when forming each product, and if $z \notin S$, then the prime decomposition of z must differ from the prime decomposition of each $s \in S$.[5]

> PROPOSITION 6. [*For*] *each composite number which is decomposed into its prime factors,* [*the numbers*] *composed of these factors, double and triple and so on, until the product named according to the number of factors minus one, all of these are parts* [*i.e., divisors*] *of it* [*i.e., the given number*].

[5] Here al-Fārisī is following the Euclid who gave the definition of a prime number rather than the Euclid who proved VII.2; in other words, he does not allow a number to divide itself.

Let the composite number be a and let us decompose it into the prime numbers b, c, d, e. Then I say that [the number] made up from b and c measures a, because if it is composed with [the number] made up from d and e, then the result is a. So it measures it. And similarly for the rest of the double and triple [numbers]. But neither the product named according to the number of the factors is a part of it [i.e., the given number] because it is not less than it, nor the products named according to a number more than [the number of] the factors, since this is not possible due to the absence of an additional factor. And so what was asked has been established. That is what we wanted.

This is the first half, the easy part, of al-Fārisī's construction of the divisors of a given composite number. If the composite number is expressed as a product of primes, then the numbers made up from these primes are divisors. The more difficult part is to show that these are the only divisors.

PROPOSITION 7. *If a number does not measure [another] number, then neither its square [i.e., of the former] nor any of its further powers measure the product [of the latter] with it [i.e., that number]. And neither its cube nor any of its further powers measure the product of its square [with the latter]. And neither the square of its square [i.e., its fourth power] nor any of its further powers measure the product of its cube with it [i.e., with the latter]. And so on.*

Thus let a not measure b. Let c be the square of a, e its cube, h its fourth power, d the product of b and a, z the product of b and c, and t the product of b and e. I say that neither c nor the further powers of a measure d, neither e nor the further powers of a measure z, and neither h nor the further powers of a measure t.[6] The reason is [that] if a is multiplied by itself and by b to give c and d [respectively], the ratio of c to d is equal to the ratio of a to b, from Book VII.18 of the *Elements*, but a does not measure b, so c does not measure d. Similarly [for] e and h and the other further powers [of a], because if one of them measures d, and c measures that power,[7] then c measures d, and this is a contradiction. Similarly, c was multiplied by a and b to give e and z [respectively], so the ratio of e to z is equal to the ratio of a to b. So e cannot measure z either, similarly [for] h and the further powers [of a]. Similarly we show that h and the further powers [of a] cannot measure t. And that is what we wanted.

At first glance this result may appear to have some connection with uniqueness of factorization, yet in reality it holds for any nonzero element in a system which obeys the Cancellation Law.

The proposition states that if $a \nmid b$ then

$$a^2 \nmid ab, a^3 \nmid ab, \ldots$$
$$a^3 \nmid a^2b, a^4 \nmid a^2b, \ldots$$
$$a^4 \nmid a^3b, a^5 \nmid a^3b, \ldots$$

and so on.

al-Fārisī sets $c = a^2$, $d = ab$; then $c:d = a^2:ab = a:b$ from VII.18 and $c \nmid d$. Also $e:z = a^3:a^2b = c:d$. Hence if $e \mid d$ then $e \mid ad$, or $e \mid z$. But then $c \mid d$. Contradiction.

[6] This last sentence is a translation of a suggestion of Rashed based on a corrupt text.

[7] Choosing the variant reading "c."

PROPOSITION 8. *If a composite number is decomposed into its prime factors and one number of them [i.e., one of these factors] does not repeat, then it [i.e., the composite number] is not measured by the square of this [prime] number nor by one of its powers. And if it [i.e., the prime factor] repeats once only then amongst its powers its square alone measures it, but not the remaining [powers]. And similarly if it repeats twice only then its square and cube alone measure it but not the remaining [powers] and so on.*

Let the composite number be a. It has been decomposed into its prime factors b, c, d, then I say that b, for example, since it does not repeat in it [i.e., in a] so its square [b^2] does not measure it [i.e., a]. This is because b is relatively prime to c and d, so is also relatively prime to the product of c and d by Book VII.24. [The number] b has been multiplied by itself and by the product of c and d, to give its square and a [respectively], so the square does not measure a by Book VII.25, and then clearly its power cannot measure a.

Also let b repeat among them [i.e., the factors], and let the factors be b, b, c, d. It is evident that its square which is one of its double products measures it [i.e., a]. But I say that its cube does not measure it, since b does not measure the product of c and d as previously [proved], and its square has been multiplied with the two of them and the results were its cube and a [respectively] which are in the same ratio. So the cube cannot measure a, and clearly the further powers cannot measure it.

If it [i.e., b] repeats twice, as for example b, b, b, c, d, so the square of b and the cube of b measure a, but not the remaining [powers], because b does not measure the product of c and d, and its cube has been multiplied by them to give its fourth power and a [respectively], which are in the same ratio, so its fourth power does not measure a. Similarly [for] the rest of its powers, and this is what we wanted.

Unlike the previous proposition, this one does concern uniqueness of prime factorization. This is clear from the statement, and also from the use of VII.24 in the proof. Euclid's result is that if $(k, n) = 1 = (l, n)$ then $(kl, n) = 1$. al-Fārisī also used VII.25 which is the special case of VII.24 with $k = l$ above.[8]

In symbols the statement of Proposition 8 is as follows, where different letters denote different numbers.

If $a = bcd$, a prime decomposition, then $b^2 \nmid a$, $b^3 \nmid a$, ...
If $a = b^2cd$, a prime decomposition, then $b^3 \nmid a$, $b^4 \nmid a$, ...
If $a = b^3cd$, a prime decomposition, then $b^4 \nmid a$, $b^5 \nmid a$, ...
and so on.

The proof involves a mixture of VII.24, VII.25, and Proposition 7, although as was the custom with al-Fārisī, the use of his own propositions is not spelled out. The actual thought process of al-Fārisī in the initial stages of this proof is not clear. He had to prove that $b \nmid cd$, but is it enough to prove that b and cd are relatively prime? We would say "yes," but perhaps al-Fārisī said "no" since he used VII.25 presumably to prove that b^2 and cd are relatively prime. He began by saying that b is relatively prime to c and to d, and hence also to cd by VII.24. Here he does not claim that $b \nmid cd$, although in the second paragraph he asserted

[8] Euclid could have used VII.24 and VII.25 to prove the "uniqueness" proposition VII.30, i.e., if a prime divides a product then it divides one of the factors. For suppose that $p \mid ab$ but $p \nmid a$ and $p \nmid b$. From VII.29 the pairs p and a and p and b are relatively prime, from VII.24 p and ab are relatively prime, and from VII.25 p^2 and ab are relatively prime, which is false. Note that although we accept the equivalence of the two statements "$(k, n) = 1$" and "k and n are relatively prime," Euclid would not recognize the former since for him a greatest common measure has to be nonunit.

that this result had already been proved. Instead he multiplies both by b to obtain b^2 and a, and then concludes that $b^2 \nmid a$ using VII.25. It appears that al-Fārisī missed the following steps:

(i) b^2 and cd are relatively prime (VII.25) and hence (ii) $b \nmid cd$.

He then used Proposition 7 to complete the proof.[9]

No indication of the proofs for higher powers or repeated factors was given, but clearly the repeated use of VII.24 and/or VII.25 suffices for this purpose.

Proposition 9. *Each composite [number] decomposed into its prime factors has no other part [i.e., divisor] except the unit and its prime factors, and also the double [numbers] made up from [two] of its factors if there are more than two, and also the triple [numbers] if there are more than three and so on until we end at the product named according to the number of factors minus one.*

Let a be a composite [number] and let us decompose it into its prime factors b, c, d, e. I say that it has no part except the unit and b, c, d, e, and the double [numbers] made up from b and c, b and d, b and e, c and d, c and e, d and e, and the triple [numbers] made up from b and c and d, b and c and e, b and d and e, c and d and e, and these are [the products] named according to the number of factors minus one.

The reason is if it were possible that it has a part other than those which have been mentioned then let it be z which is either prime or composite. If it is prime and measures a [which is] made up from b, c, d times e, then by Book VII.30 it [i.e., z] necessarily measures one of its [i.e., a's] two factors, and [it] cannot measure the prime e, so it has to measure [the number] made up from b, c, d. But since it measures this product which is made up from the product of b and c times the prime d, then as in the previous argument, it has to measure the [number] made up from b, c and since it measures this product then it measures one of its two prime factors, or it is one of them, and both cases are impossible.

If z is a composite [number], and it is distinct from the abovementioned products, then necessarily its prime factors cannot be identical with the factors of those products. Therefore either there exists amongst the prime factors of z one which does not appear amongst the factors of a, or not. If it does not exist either there is among them one factor of z [which] repeats itself a number [of times] but is not repeated [as many times] amongst the factors of a, or one factor of a [which] repeats itself a number [of times] but is not repeated [as many times] amongst the factors of z. And these are three cases.

If it is the first then let this prime [factor] distinct from all the factors of a be h. Then h is prime, and the abovementioned contradiction follows when z was assumed prime.

If it is the second, one factor from the factors of z, let it be b, is repeated [say] once [in z], and b is not repeated in the factors of a. So the [number] made up from b and itself measures z, and [so] it measures a and [yet] it is not repeated in the factors of a, which is impossible. And similarly we can prove a contradiction if it [i.e., b] is repeated twice or more. And let b be repeated twice in the factors of z and once in the factors of a, so [the cube of b] necessarily measures z and so measures a, but it is not repeated more than once in its [i.e., in a's] factors, and this is a contradiction. And similarly the contradiction occurs whenever the number of times b repeats in the factors of z is more than its number [of repetitions] in the factors of a. If it is the third [case], I mean some factor of a is repeated a number of times in it [but] not repeated as [many times] in the factors of z, then it is clear that in this case z becomes one of the parts of the product [already mentioned]. Therefore the theorem is established. This is what we wanted.

[9] The alternative reading is to consider VII.25 as a step in the proof that $b^3 \nmid a$ rather than in the proof that $b^2 \nmid a$. Since b and cd are relatively prime it follows that $b \nmid cd$, and by Proposition 7, $b^2 \nmid a$. Now use VII.25 to prove that b^2 and cd are relatively prime. This implies that $b^2 \nmid cd$ and Proposition 7 again gives $b^3 \nmid a$.

In other words, all the divisors of a given number can be found from any prime factorization whatever. One more step is required to show that this implies the existence of a single prime factorization for any number but this step is not taken by al-Fārisī.

The proof of the proposition is valid in general, but, as usual, al-Fārisī deals only with a specific case.

Let $a = bcde$ be a prime factorization; then the only divisors of a are 1, b, c, d, e, bc, bd, be, cd, ce, de, bcd, bce, bde, cde. The proof is by a reductio ad absurdum. Suppose a number z different from those above divides a. If z is prime, then z divides $(bcd)e$, and by repeated use of VII.30, z must divide one of the prime factors b, c, d, e, which is impossible.

If z is composite it has a prime factorization (Proposition 1) and since z is not one of the divisors listed above, it cannot have the same prime factorization as any of these divisors (Proposition 5). So there are three cases.

(i) z has a prime factor which is not a factor of a.

If (i) does not hold then all prime factors of z appear amongst the factors of a. This possibility splits into two cases.

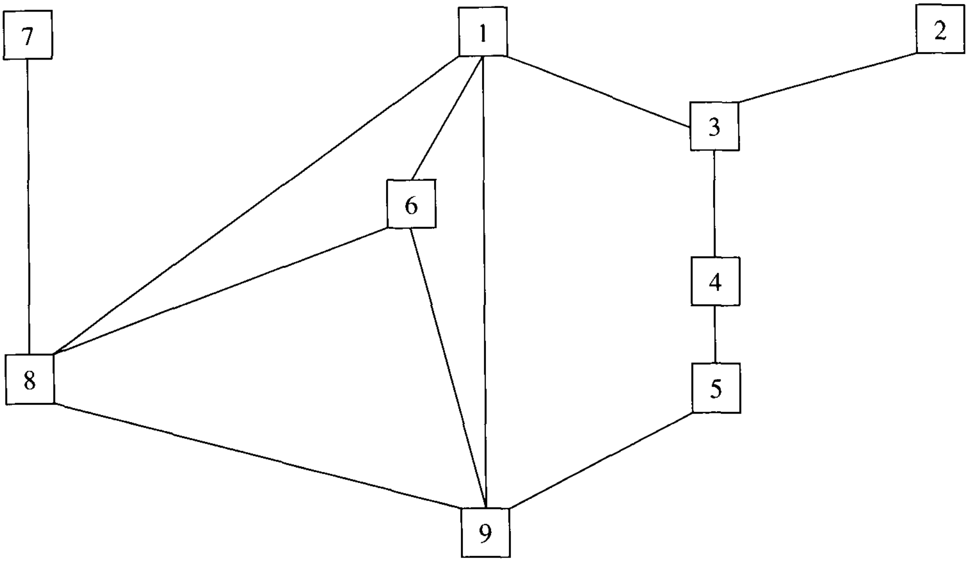
(ii) There is a prime factor of z which repeats more times in z than in a.

(iii) There is a prime factor of a which repeats more times in a than in z.

The first case reduces to the previous possibility of z prime. The second case requires Proposition 8. If b^2 divides z but b appears only once in the factorization of a then b^2 divides a and b^2 does not divide a. The other possibilities can be dealt with similarly. In the third case z must be one of the numbers already made up from the prime factors of a.

3. INTERPRETATION

The internal structure of these nine propositions is as follows. (An upper number is used in the proof of a lower number.)



The structure is self-contained apart from a handful of Euclidean theorems, and it shows clearly that most roads start from Proposition 1 and end with Proposition 9, propositions proving the existence of a prime factorization and the consequent determination of all divisors. It also shows that Propositions 4 and 5 are merely links in the chain which al-Fārisī constructs in order to get to his ultimate aim of proving Proposition 9. It does not indicate that Propositions 4 and 5 are equivalent, but either this was not known to al-Fārisī or it was known but of no particular interest to him in this study. As we have seen, all the statements of his propositions are valid. So too are all the proofs, including the proof of Proposition 2. Rashed claims that the proof of Proposition 5 is flawed [8, 123], but in our reconstruction this is not so, as al-Fārisī used a simple contradiction argument.

Let us now return to the question of al-Fārisī and the FTA. There is no doubt that he proved the existence part of the FTA, namely that every positive integer (>1) can be expressed as a product of primes. Although the statement of Proposition 1 concerns composite numbers only, all al-Fārisī lacks is the trick of calling a prime number a product of one prime factor. As far as we know, this is the first statement and proof of the theorem.

As for uniqueness, Rashed's opinion is plainly stated: "Ces deux dernières propositions [our Propositions 4 and 5] sont, de toute évidence, destinées à établir l'unicité de la décomposition en facteurs premiers" [8, 123].

Our reading of the text disagrees with this verdict. In our estimation, al-Fārisī neither stated nor proved uniqueness, and it was not his intention to do so. As we have seen, Propositions 4 and 5 fit snugly into the general scheme of his overall argument. In claiming too much for al-Fārisī, Rashed paradoxically casts doubt on his reputation as a mathematician. For if al-Fārisī was trying to prove uniqueness in Propositions 4 and 5, he clearly confused the theorem with its converse. Our analysis, on the contrary, suggests that al-Fārisī expressed precisely what he wanted to say. The statement and proof of Proposition 9 indicate that he was well aware of the uniqueness of a prime decomposition. If he had wanted to prove uniqueness, then he certainly would have been able to do so. He would not have bungled the statement, getting it the wrong way round (twice), and forgetting to mention that the factors should be prime.

ACKNOWLEDGMENTS

We thank Kamal A Hammad and Zeynep Ağargün for their help and advice during the preparation of this paper. We also owe a great debt to Sonja Brentjes and Jan Hogendijk for their patient assistance. Our profound thanks to them both.

REFERENCES

1. S. Brentjes, On Some Theorems to Elementary Number Theory by Kamāl al-Dīn al-Fārisī (d. ca. 1320), preprint, Leipzig: University of Leipzig, 1990.

2. Euclid, *The Thirteen Books of Euclid's Elements*, Vol. 2. trans. from the text of Heiberg with introduction and commentary by T. L. Heath, Cambridge: University Press, 1908; reprinted New York: Dover, 1956.

3. C. Goldstein, On a Seventeenth Century Version of the "Fundamental Theorem of Arithmetic," *Historia Mathematica* **19** (1992), 177–187.
4. J. P. Hogendijk, Thābit ibn Qurra and the Pair of Amicable Numbers 17296, 18416, *Historia Mathematica* **12** (1985), 269–273.
5. A.-M. Legendre, *Théorie des nombres*, 3rd ed., Paris: Firmin Didot, 1830; reprinted Paris: Hermann, 1900.
6. I. Mueller, *Philosophy of Mathematics and Deductive Structure in Euclid's Elements*, Cambridge: MIT Press, 1981.
7. R. Rashed, Matériaux pour l'histoire des nombres amiables, *Journal for the History of Arabic Science* **6** (1982), 228–267.
8. R. Rashed, Nombres amiables, parties aliquotes et nombres figurés aux XIII$^{\text{eme}}$ et XIV$^{\text{eme}}$ siècles, *Archive for History of Exact Sciences* **28** (1983), 107–147.