HISTORIA MATHEMATICA 2 (1975), 189-191

EUCLID AND THE FUNDAMENTAL THEOREM OF ARITHMETIC

BY M.D. HENDY
MASSEY UNIVERSITY, NEW ZEALAND

SUMMARIES

Slight changes or benevolent interpretations of certain theorems and proofs in Euclid's Elements *make his demonstration of the fundamental theorem of arithmetic satisfactory for square-free numbers, but Euclid's methods cannot be adapted to prove the uniqueness for numbers containing square factors.*

Kleine Änderungen oder wohlwollende Deutungen gewisser Theoreme und Beweise in Euclids Elementen *machen seine Beweisführung hinsichtlich des Grund-theorems der Arithmetik annehmbar für quadrat-freie Zahlen. Jedoch können Euclids Methoden nicht übernommen werden, um die Einmaligkeit der Faktorisierung der Zahlen mit Quadratfaktoren zu beweisen.*

「ユークリッド原論」における定理とその証明に創意的解釈を加えると、ユークリッドの「あらゆる数はただひとつの方法で素因数に分解できる」という定理は、互いに素である数の積によって成り立つ数については応用できるが、自乗数を含む数については応用できない。

The distinction between prime and composite integers was familiar to the early Greek geometers and probably earlier, but the first known formulation of the proposition now called the fundamental theorem of arithmetic is in Euclid's *Elements*. [Heath, Bk. IX, Pr. 14] The geometrical language of Euclid has led to differing interpretations by his commentators, and there is dispute as to what precisely is proven in IX, 14.

It is convenient at this stage to introduce a distinction, due to A.A. Mullin [1965], between two traditional forms of the fundamental theorem: Let n be any natural number greater than one, whose prime divisors are p_i, then:

(1) the expression $n = p_1 p_2 \ldots p_r$ (which allows repetitions among the p_i's) is unique up to the order of the prime factors (the "primordial Euclidean form");

(2) the expression $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$, with $p_i < p_{i+1}$ and $\alpha_i > 0$, is unique (the "standard Gaussian form").

Euclid's proposition is of the first form. The notation by which the second form is expressed was not available until the end of the sixteenth century.

In his commentary on Euclid, Heath [vol. 1, p. 403] claims that Euclid has shown that "a number can be resolved into prime factors in only one way," and claims that a complete proof of form (1) has been given. Mullin [p. 218] less emphatically states of his form (1): "This uniqueness theorem of Euclid contains the spirit, if not the full essence of what is now called by many texts the Fundamental Theorem of Arithmetic and by nearly as many others the Unique Factorization Theorem." Hardy and Wright in their text [1965, 10] state that form (1) "does not seem to have been stated explicitly before Gauss," and later [p. 182] attribute the following remarks to Prof. S. Buchner: "It might seem strange at first that Euclid having gone so far could not prove the fundamental theorem itself; but this view would rest on a misconception. Euclid had no formal calculus of multiplication and exponentiation, and it would have been most difficult for him even to state the theorem. He had not even a term for the product of more than three factors. The omission of the fundamental theorem is in no way casual or accidental. Euclid knew very well that the theory of numbers turned upon his algorithm and drew from it all the return he could."

In order to judge for ourselves the depth of Euclid's propositions we need to translate his geometrical ideas into the modern language of arithmetic. Heath's commentary on Books VII and IX is not adequate for this purpose. For example, IX,14 depends in part on VII,12. In the latter, the translation reads: "Let A, B, C, D be as many numbers as we please...," but the ensuing argument uses A,B,C and D explicitly as four numbers. It could be argued that there is an implied generalisation here which Euclid may well have stated and proved had not his notational handicap prevented him. Heath has made this assumption, and his commentary on the proposition carries a proof which is perfectly general, relating to an unspecified number of numbers, a, a^1, b, b^1, c, c^1, ... A similar, but not so trivial generalisation is given by Heath in the main proposition, IX,14. Euclid gives his proposition as: "If a number be the least that is measured by prime numbers it will not be measured (divisible) by any other prime number except those originally measuring it." To demonstrate this general proposition Euclid proves only the explicit case where a number A is the product of three primes, B, C and D. Heath generously, but not rigourously, generalises this to an unspecified number of factors again. About this generalisation Mullin makes the following comments: The Greeks established their uniqueness result with the maximum generality (number of factors) that they clearly conceived with their geometrically oriented notation. Since the analogous result with two factors (not given in the *Elements*) is not a corollary of the result with three

factors, it is reasonable to assume that formal induction either did not occur to them, or else was considered logically unacceptable."

Mullin in the same also comments: "His argument in Book IX, Proposition 14 holds not only for square-free numbers, but also for factors with repetition too...." However, it does not appear that such a conclusion is justified. Euclid begins his proposition with the hypothesis: "Let the number A be the least that is measured by primes B, C, D." If we allow the possibility of B, C and D not being distinct, then the number A above must be their least common multiple, rather than product. If we accept the definition A = BCD with at least two of B, C, and D equal, then Euclid's subsequent proof breaks down. Suppose $B = C \neq D$ are primes, then the smallest number they measure is BD, rather than B^2D, and so we should not admit numbers with square divisors into this construction. If we bypass Euclid's original initial proposition and allow $A = B^2D$, the construction of a number F, with the same prime divisors as A, but strictly less than A, can now no longer lead to a contradiction.

Thus we must conclude that Euclid has only shown in this proposition, that any square-free number with three prime divisors can be factored as a product of primes uniquely to within order. By a simple extension of Euclid's proof we could establish a similar theorem for any square-free number, but his method cannot be readily adapted to admit all natural numbers.

CITED PUBLICATIONS

Hardy, G.H. and E.M. Wright 1965 *An Introduction to the Theory of Numbers* 4th ed. Oxford.

Heath, Sir Thomas L. 1956 *Euclid's Elements* 2nd ed. New York (Dover).

Mullin, Albert A. 1965 "Mathematico-philosophical remarks on new theorems analogous to the fundamental theorem of arithmetic," *Notre Dame J. Formal Logic* 6(3), 218-222.