Notre Dame Journal of Formal Logic
Volume VI, Number 3, July 1965

MATHEMATICO-PHILOSOPHICAL REMARKS ON NEW THEOREMS ANALOGOUS TO THE FUNDAMENTAL THEOREM OF ARITHMETIC

ALBERT A. MULLIN

The author dedicates this paper to the memory of Professor Thoralf Skolem; philosopher, logician, and mathematician.

Introduction: *Circa* 300 B.C., Euclid of Alexandria (*not* Euclid of Megara) borrowing partly, but not altogether, from the Pythagorean School proved (*Elements*; Book IX, Proposition 14) the following result as rendered into modern language from the Greek [1]: *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.* This uniqueness theorem of Euclid contains the spirit if not the full essence of what is now called by many texts (see, e.g., [2], [3], and [4]) the *Fundamental Theorem of Arithmetic* (abbreviated FTA) and by nearly as many other texts (see, e.g., [5] and [6]) essentially the *Unique Factorization Theorem* (abbreviated UFT), *viz.*, Every natural number $n > 1$ has a *unique* representation of the form $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$, where k is a natural number and the p_i are primes with possible repetitions. The proof given by Euclid for his Proposition 14 of Book IX makes use of Proposition 30 of his Book VII, *viz.*, *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.* The modern texts cited above, among others, use this result together with formal induction in order to establish uniqueness of prime decomposition. The principal argument against Euclid having known the essence of the FTA is that throughout the *Elements* his products contain at most three factors (his argument in Book IX, Proposition 14 *holds* not only for square-free numbers with at most three factors, but for factors with repetition too; further T. L. Heath [1] in his *Scholium* to the Proposition 14 explicitly states, "In other words, a number can be resolved into prime factors in only one way."). 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 to 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.

Received April 23, 1963

The FTA as we know it through Gauss [7], *viz.*, $n = p_1^{\alpha_1} \cdot \ldots \cdot p_m^{\alpha_m}$, where m and α_i are natural numbers and the p_i are *distinct* primes is a highly sophisticated analogue of Euclid's model which makes use of the notion of an exponent which had been introduced into mathematics in the meantime. Gauss seems to have been the first person to give a complete published proof to the FTA as we usually know it, although, e.g., Newton, Wallis, and Euler made use of it in their arithmetical investigations. The main purpose of this paper is to show by analogical reasoning and formal induction that infinitely many other "models" of the FTA are available. The simplest of those "models" is shown to yield a rich vein of new theorems for elementary, algebraic, and analytic number theories.

Uses for the FTA: In order to appreciate more fully the potential of new models of the FTA let's review briefly some of the applications of Gauss' model of the FTA. First, Hardy [8], Ingham [4], and Mordell [9] write to the effect that the Fundamental Theorem *is* the foundation of all of higher arithmetic, and that which gives deep significance to the study of prime numbers themselves beyond that of intellectual curiosity. Secondly, Gauss' theory of residues and congruences hinges to no small extent upon the FTA as does Euler's Identity (which Hardy and Wright [3], among others, call "an analytic expression of the FTA.") Thirdly, the Fundamental Theorem of finitely generated abelian groups makes essential use of the FTA for the case of finite abelian groups. More recently K. Gödel [10] in his epoch paper of 1931 uses the FTA to number the wffs and proofs in his axiomatic number theory that has undecidable propositions. Lastly those engaged in information theory have made use for FTA in order to establish the form of the entropy function of that theory (see, e.g., [11]).

New Models of the FTA: With these points in mind let's search for *new* models of the FTA remembering that, *if* uses for these new models *do* come, it may be centuries into the future. The basic tool for our investigation is mathematical induction—one of the most powerful methods of logic, algebra and number theory, indeed, of analysis itself. The method is called *reflexive induction*, i.e., *when possible apply a rule to a portion of the entity obtained from a prior application of that same rule*. An induction upon the *whole* object considered as an unanalyzed entirety is called *irreflexive induction*. E.g., Euclid's Algorithm is obtained from the Division Algorithm by reflexive induction upon the Division Algorithm. But a concatenated repetition of an entire pattern is an irreflexive induction upon that pattern. Further a reflexive induction may be either *finite* as with a continued fraction expansion of a rational number or *infinite* as with a continued fraction expansion of an irrational number. Similarly an irreflexive induction may be either *finite* as with a finite iterative array of canonic cells or *infinite* as with a nonterminating array of canonic cells.

Can one use reflexive induction upon the FTA? Yes! One may apply the FTA to its own natural number exponents. Clearly, by the Well-ordering Principle, the reflexive induction is finite. Call the final *unique* configuration of primes *alone* that represents a natural number, a *mosaic*. E.g., the mosaic of *400* is $2^{2^2}.5^2$. Thus, *Lemma* (*new model of FTA*). *There* *exists a one-one effectively calculable function from the natural numbers onto the mosaics identify 1 with the "empty" mosaic* .

From this formulation comes a number of interesting functions at the interface between recursive function theory and numbertheory [12], [13], [14], [15]. E.g., define ψ by $\psi(n)$ is the ordinary product of primes alone in the mosaic of n, and $\psi(1) = 1$. Clearly ψ is effectively calculable, and the square-free natural numbers, among infinitely many others, are invariant under ψ. Also $\psi(m) \neq m$ for infinitely many m. The interesting fact is that if one puts $\alpha(n) = \text{card}\{a \varepsilon N \ \ a \leqslant n, \ \psi(a) = a\}$ and $\beta(n) = \text{card}\{a \varepsilon N{:}\, a \leqslant n, \psi(a) \neq a\}$, where $n \varepsilon N$ and N is the set of natural numbers, then it can be shown that $\lim\limits_{n \to \infty} [\alpha(n)/\beta(n)] = 7/(\pi^2 - 7)$, which is transcendental over the rational numbers; see [15]. Further, we are in a position to generalize the classical concept of a multiplicative function. Recall that a number-theoretic function f is called *multiplicative* when $f(a \cdot b) = f(a) \cdot f(b)$, if $(a, b) = 1$. Call a number-theoretic function g *generalized* multiplicative when $g(a \cdot b) = g(a) \cdot g(b)$, if the mosaics of a and b have no prime in common. Upon defining $\psi^2 = \psi(\psi(\cdot))$, it should be clear that every multiplicative function is generalized multiplicative, and that ψ^2 is an example of a generalized multiplicative function which is *not* multiplicative. By analogy, call a number-theoretic function h *generalized* additive when $h(a \cdot b) = h(a) + h(b)$, if the mosaics of a and b have no prime in common. Then every additive function is generalized additive, and $\log \psi^2$ is a generalized additive function which is not additive. Further there are infinitely many *generalized* multiplicative functions which are *not* multiplicative.

Another interesting effectively calculable, number-theoretic function ψ^* is defined by $\psi^*(n)$ is the sum of the primes alone appearing in the mosaic of n, and $\psi^*(1) = 0$. Clearly ψ^* is additive, i.e., $\psi^*(a \cdot b) = \psi^*(a) + \psi^*(b)$, if $(a, b) = 1$. Interestingly enough ψ^* maps the natural numbers > 1 *onto* themselves. This result follows by the famous theorem of Schnirelmann (proved *circa* 1930) which asserts that *every natural number* > 1 *is the sum of a finite number of primes*. Another interesting fact about ψ^* is that the distribution function of its fixed-points is essentially the distribution function for the primes. Finally one can easily relate ψ and ψ^*. Thus define ψ^{**} by $\psi^{**}(n)$ is the sum of the primes alone in the classical Euclidean model of the FTA. E.g., $60 = 2 \cdot 2 \cdot 3 \cdot 5$ and thus $\psi^{**}(60) = 12$. As with ψ^*, Schnirelmann's theorem established *ontoness* for ψ^{**}. Then $\psi^* = \psi^{**}(\psi(\cdot))$.

Within the present framework one can easily start to formalize the intuitive notion of an exponential number theory to supplement the standard additive and multiplicative number theories. Here one studies, e.g., exponentiated sequences $p_1^{p_2 \cdots p_N}$ so convenient for establishing, e.g., that ψ is *onto* the natural numbers. By analogy to super-additive and super-multiplicative number-theoretic functions one can show that e^{ψ} satisfies an interesting functional inequality of the form $f(a \cdot b) \ f(a)^{f(b)}$, if $(a, b) = 1$. By analogy to the author's concept of a *generalized* number-theoretic function, one can define a *generalized super-exponential* function g as one which satisfies the inequality $g(a \cdot b) \leqslant g(a)^{g(b)}$, if the mosaics of a and b have no prime in common.

Upon applying Gauss' model of FTA to its exponents (uniformly for *all* natural numbers) any prescribed finite number of times we intuitively obtain a model of FTA. If two *schemes* for uniquely representing all natural numbers by an effective method provide the same presentations for all the natural numbers then the two *schemes* are said to be the same. Intuitively there cannot be more than $\aleph_0$ classically conceived models of the FTA, since the set of all finite complexes of natural numbers has this cardinality. But might there be only finitely many models of the FTA? No. By considering exponentiated sequences the schemes obtained by applying Gauss' model to its exponents any prescribed finite number of times uniformly across all natural numbers can be shown to yield *distinct* schemes (i.e., for any pair of such schemes there exists in a constructive sense a natural number with two different presentations by means of those two schemes. Thus there is at least (and hence *precisely*) $\aleph_0$ *classically conceived models* (e.g., involving the *concrete* prime numbers and composite numbers) of the FTA. Each of these schemes is *mixed* in the sense that, in general, the natural numbers will be represented by both primes and composites. A countable infinitude of *pure* models (determined by primes alone as with Euclid's model and the "mosaic model" given by the Lemma) can be generated from those mixed models by expanding their composite numbers with Euclid's model (which is significant for additive and exponential theiries but *not* for a multiplicative theory) or with sufficient repetitions of a mixed model. Hence new models of the FTA are available in abundance, and in a vague sense, complement with *arithmetical* results the discovery of non-Euclidean *geometries* during the last century. By striking analogy to the geometric situation with its Euclidean geometry, Riemannian geometry, and Lobachevskian geometry, the arithmetical situation has three forms, *viz.*, the Euclidean, the *pure* non-Euclidean, and the *mixed*. In both the arithmetical case and the geometrical case the forms are mutually exclusive and exhaustive.

In closing we note that no mention is made of schemes for expanding the exponents in Gauss' model of the FTA by means of sums of k^{th} powers of natural numbers (i.e., introducing the general Waring problem) nor is probàbilistic number theory considered. Other contexts in which analogous results to the present paper hold are: unique factorization domains (e.g., polynomial domains), ordinal factorization of finite relations [16], ideal theory (especially Dedekind's formulation of the Fundamental Theorem of Ideal Theory), generalized primes [17], and computable number theory, [14] and [18].

REFERENCES

[1] T. L. Heath, *Euclid's Elements* (Volume II), New York, 1948.

[2] G. Birkhoff and S. Mac Lane, *A Survey of Modern Algebra*, New York, 1953.

[3] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford, 1960.

[4] A. E. Ingham, *The Distribution of Prime Numbers*, Cambridge, 1932.

[5] W. J. Le Veque, *Topics in Number Theory* (Volume I), Reading, Mass., 1956.

[6] I. M. Vinogradov, *Elements of Number Theory*, New York, 1954.

[7] C. F. Gauss, *Disquisitiones Arithmeticae*, Leipsig, 1801.

[8] G. H. Hardy, A Mathematician's Apology, Cambridge, 1940.

[9] L. J. Mordell, "An Introductory Account of the Arithmetic Theory of Algebraic Numbers and its Recent Developments," *Bull. Amer. Math. Soc.*, vol. 29 (1923) pp. 445 and following.

[10] K. Gödel, "Über formal unentscheidbare Satze der Principia Mathematica und verwandter Systeme I," *Monats. f. Math. u. Physik*, vol. 38 (1931) pp. 173-198.

[11] A. Feinstein, *Foundations of Information Theory*, New York, 1958.

[12] A. A. Mullin, "Some related number-theoretic functions," *Bull. Amer. Math. Soc.*, vol. 69 (1963) pp. 446-447.

[13] A. A. Mullin, "Models of the Fundamental Theorem of Arithmetic," *Proc. Nat. Acad. Sci. USA*, vol. 50 (1963) pp. 604-606.

[14] A. A. Mullin, "A Contribution Toward Computable Number Theory," *Zeitschrift f. Math. Logic Grundlagen*, vol. 11 (1965), pp. 117-119.

[15] A. A. Mullin, "On a final multiplicative formulation of the Fundamental Theorem of Arithmetic," *Zeitschrift f. math. Logik Grundlagen*, vol. 10 (1964), pp. 159-161.

[16] C. C. Chang, "Ordinal factorization of finite relations," *Trans. Amer. Math. Soc.*, vol. 101 (1961) pp. 259-293.

[17] E. M. Horadam, "The Euler ϕ-function for generalized integers," *Proc. Amer. Math. Soc.* vol. 14 (1963), pp. 754-762

[18] R. L. Goodstein, *Recursive Number Theory*, Amsterdam, 1957.

Lawrence Radiation Laboratory,
University of California
Livermore, California