Notre Dame Journal of Formal Logic
Volume XIX, Number 1, January 1978
NDJFAM

FOUNDATIONAL PROBLEMS OF NUMBER THEORY

YVON GAUTHIER

I want to address myself in this paper* to the thesis that realism is a viable philosophy of mathematics and I am going to attack the thesis by examining number theory and by proposing a foundational framework that purports to explain fundamental results in arithmetic and analysis without having to resort to realism. My main philosophical target or pretext will be Hilary Putnam's philosophy of mathematics (the pre-Marxist one).

1 Putnam is said to have argued that ontological realism can be combined with an empiricist epistemological attitude which would assimilate mathematics to theoretical physics at least as far as hypothetico-deductive reasoning and inductive confirmation of hypotheses are concerned. For example, it would be legitimate according to Putnam, to accept the truth of Fermat's last theorem and Goldbach's conjecture on the ground that these hypotheses have been tested sufficiently to warrant our acceptance—Fermat's last theorem asserts that it is impossible to find a natural number with a power greater than two such that it is the sum of two other natural numbers with the same power, e.g., a cube cannot be the sum of two cubes, etc. . . . and Goldbach's conjecture says that every even number from six onwards can be represented as the sum of two prime numbers other than two. Now if one is interested in number theory, one knows that in the case of Goldbach's conjecture related problems have been solved e.g., "Every sufficiently large odd number is representable as the sum of three odd primes" and "Almost every even number is representable as the sum of two odd primes."[1]

But I want to go a little further: an important theorem by Dirichlet says that if a and b are relatively prime (such that they have no common divisor, 1 excepted), there are infinitely many primes of the form $ax + b$, that is in any arithmetical progression. Dirichlet gave a proof of that statement using analytical methods (L-functions or Lolomorphic functions

*I am indebted to Bas C. van Fraassen, Gonzalo Reyes and Georg Kreisel for helpful comments.

Received June 10, 1974

of complex analysis, infinite series, limits, and so on), but there are more recent elementary methods (methods that use only arithmetical properties, approximations instead of limits, for example) by Selberg, Zassenhaus, and others. These methods are constructive in contrast to the transcendental methods of analysis. Before attempting to draw a philosophical lesson from these results of number theory, let me point two problems for which there is not as yet a pinch of a hint.

Conjecture No. 1 *There are infinitely many primes of the form* $x^2 + 1$, e.g., 2, 5, 17, 37, 101 . . .
Conjecture No. 2 *There are infinitely many pairs of primes* (3.5), (5.7), (17.19).

(The list of unsolved problems in number theory includes at least 250 items, following H. Hasse). I remark here that all the problems, solved or unsolved, that I have mentioned, have to do with infinity. I could have mentioned also Euclid's proof of the infinity of primes or the elementary proof by Selberg and Erdös of the prime number theorem which asserts that the ratio of the number of primes in a large set x to $x/\log x$ tends to the limit 1 as x tends to infinity, that is

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1.$$

2 I am interested in the significance these results have for foundations of mathematics. All the results I have referred to have been obtained by elementary methods (except the results on Goldbach's conjecture). My approach is the following: infinity in number theory does not refer to an actual infinity, an infinite set or a closed totality. It does not refer either to a potential infinity, which, in my view, is an ambiguous concept, if not a contradictory one—my contention is that, because potentiality always supposes actuality, at least in the Aristotelian sense, the concept of potentiality has only a chronological, not an ontological content, but this is a different matter. Rather, the fundamental idea conveyed by the word infinity in number theory is that of a process, a process which produces the series of numbers according to a rule specified by the construction of the *number-concept and the form of its definition. I call a process finite, if it* has finite bounds pre- and post-positionally determined (I exclude infinite bounds); a process is effinite if it does not have finite bounds and I maintain that all we can use is that truly negative concept of *effinite* (from ex-finitus), meaning beyond the finite, outside the finite. An effinite process is a process which a finite performance with initial and terminal states cannot exhaust. My concept of process cannot be reduced to a processing Turing machine, possibly with no end state (or to any other characterization of recursive functions). Of course, I do not accept Church's Thesis which identifies effectively computable functions with recursive ones. Kreisel has given an example[2] of a constructive function which is not mechanical: we have **HA**, Heyting arithmetic which is constructively valid, p_n represents a constructive proof of a formal derivation n (with Gödel number) in **HA**

$$fn = \begin{cases} 0, \text{ if } n \text{ is not a derivation of any closed formula of the form } \exists x\mathcal{A} \\ 0, \text{ if } p_n \text{ does not provide a specific numerical instance satisfying } \mathcal{A}, \\ \text{e.g., } \exists x\mathcal{A} \text{ has been inferred from } \forall x\mathcal{A} \\ x + 1, \text{ if } x \text{ is the number verifying } \mathcal{A} \text{ which is provided by } p_n. \end{cases}$$

The mechanical counterpart to this would be

$$f'n = \begin{cases} 0, \text{ if } n \text{ is not a derivation in } \mathsf{HA} \text{ of any closed formula } \exists x\mathcal{A} \\ x + 1, \text{ otherwise for } x \text{ as the argument of } \mathcal{A} \text{ in the shortest deriva-} \\ \text{tion of a formula of the form } \mathcal{A}x. \end{cases}$$

I wish to give a more abstract characterization of process, allowing for abstract and intensional operations like constructions. I call *stasis* the intensional equivalent of state, initial and terminal states become prepositional and postpositional bounds. A non-terminating process is effinite, that means it cannot be numbered and it cannot be conceived as a set. Only finite multiplicities can be formed as sets, that is totalities or unities seen as containing all their members. An effinite process can be quantified upon, but it cannot be totalized: what I want to say is that one is entitled to refer to all natural numbers, meaning effinitely many, but one cannot form the set of all natural numbers, make a whole of them, since this would amount to having terminated a non-terminating process or exhausted an inexhaustible process. For me, then, when all qualifies a non-finite multiplicity, it signifies an every-expanding process and not a set or a totality. (I have indicated elsewhere how the universal quantifier can give rise to the idea of infinite multiplicities as sets or completed totalities; the intuitionistic notion of species has also to be modified here.)

3 This conceptual framework would, in my mind be sufficient for non-analytical methods in number theory. But let us suppose that certain analytical methods do not have an elementary counterpart (e.g., Vinogradov's method for Goldbach's problem). How can we explain those results in our conceptual framework? Analytical methods involve essentially the use of all or every for infinite multiplicities, for example, in the definition of such properties as continuity and analyticity; real and complex analysis rest upon non-denumerable infinities.

Take the simple example of the definition of continuity: we have X and Y as metric spaces, $E \subset X$, $p \in E$ and f: $E \rightarrow Y$: then we say that f is continuous at p if

$$\forall x \in E \forall e > 0 \ \exists \delta > 0 \ [(\mathrm{d}_X(x, p) < \sigma) \rightarrow (\mathrm{d}_Y(f(x), f(p)) < e)]$$

Analytical concepts seem to require a transcendental frame of reference, i.e., existence of infinite sets of numbers (transfinite cardinals). My point of view is here again the effinite. The process I want to consider is abstract: let us assume a stasis, the intensional equivalent of a state; a process on or over such a stasis, I call a metastasis. A continuous function would then be a *metastasis*, a continuous functional a third-order stasis (the notion of a measurable cardinal similarly requires a third-order stasis).

How can we differentiate between my approach and the classical one? The classical approach allows for arbitrary properties or subsets of a given infinite set. Nowhere do I postulate the existence of completed effinite sets or of universal properties. On the contrary, all constructions are supposed to be incomplete. Only infinite sets and local properties can be considered as complete constructions, their universal analogues belong to ideal structures. For the sake of clarity, let us compare the above description with second-order number theory and set theory. Higher-order logic admits quantification over predicate or function symbols by assuming a completed universe of subsets of a given infinite set: we have the second-order induction postulate for number theory

$$\forall X(X(0) \wedge \forall y(X(y) \rightarrow X(Sy)) \rightarrow \forall y\; X(y))$$

or the second-order comprehension axiom for set theory

$$\forall a\; \forall X\; \exists x\; \forall y\,[y \in x \leftrightarrow (y \in a \wedge X(y))]$$

In both cases, the set of all natural numbers and the set of all their subsets are assumed.

From my viewpoint, these assumptions are unnecessary; they, in fact, lead to ambiguous, dialectical and possibly paradoxical structures (not constructions). Since our constructions for processes, stases and the effinite guarantee us all what we need-remember that "all" leads into the effinite or out of the finite and that at the same time we do not need "all" instances of our construction, simply because we have only a finite number of stipulations or directions for our constructions—hierarchical theories of types, ranks, and levels are extensionally—disguised intensional theories; they do not involve new operations, only fuller ranges for the given operations and this makes for over-saturated realism.

4 It is time to draw some philosophical implications from our analysis of those few mathematical concepts. Conceptual analysis has had the task, traditionally, to critizise concepts either from the point of view of common sense (philosophical or not), linguistic analysis or more generally from the standpoint of a more or less explicit philosophical scheme. Personally, I privilege a constructivist viewpoint, which strives for total explicitness. In this view, concepts are either constructed or structured. A *constructed* concept is finitely integrated, that is, it refers to actual intellectual experience, a *structured* concept is finitely derived from elementary constructions.[3] That is to say, not all of our experience is constructed, that part of it which is common structure can be traced back to past constructions in the history of man's intellectual, conscious and linguistic (which is not always conscious) experience. Here, experience *tout court* would be meaningless.

Concepts are *construction-absolute,* if they refer to direct intuitive and evidential intellectual experience, *completion-absolute* if they are intended to refer to possible experience. Completion-absolute concepts are clearly not constructed, but rather structured concepts (most concepts of the philosophical tradition are of this kind, the Absolute, Being, the World, etc. . . .). How does this relate to the realist ontology and the empiricist epistemology, allegedly held in conjunction by Putnam? In our version of number theory with finite and effinite processes, numbers being free creations of the mind (as Dedekind liked to put it), can be formed into any finite set of numbers; the process of forming a set is itself an idealization which consists of considering as a unity a gathering of well-defined objects of our thought or our intuition (as Cantor liked to put it). Rational and real numbers are gotten in the usual way. Putnam seems to think, in his *Philosophy of Logic*,[4] that we need the sets of all natural, rational, and real numbers as completed totalities. I have argued to the contrary. The concepts of such totalities are completion-absolute, they do not have any actual reference; they are intended to refer to possible or ideal experience of rather to the possible completion of experience, but in this case as in most cases the completion is excluded by our constructions. Universal quantification is still permissible, provided we do not bag the "all" of quantification into a whole, all, as we have seen, meaning effinitely many. (Maybe we should use a new symbol "Ɏ" for that universalization which does not yield a universe). Putnam is obsessed by the amount of set theory that is needed in physics. On his realistic account of physics, Putnam maintains that the notion of distance requires the existence of functions from space-points to reals. But Putnam, being after nominalism here, shows only that the linguistic formulation of nominalism is inadequate, not that realism is a necessary condition for expressing the statements of physics. For we could construct distance in such a way as to allow only finite measurements (or numericalizations, as Putnam says) without having to recognize reals as completed numbers.[5]

Ontological realism (the realist ontology of mathematics here), then, seems to contain unnecessary assumptions. The objections Putnam raises against nominalism do not register against constructivism,[6] since constructivism does permit the introduction of abstract operations of various complexity. What I have attempted to show is that in order to quantify over numbers and functions on them, one is not forced to consider "all" as a whole or to put all numbers in what I call "the ontological bag".

5 Finally, I briefly address myself to the second part of Putnam's thesis, the empiricist epistemology of mathematics.[7] While the realist ontology was intended to deal with the status of mathematical entities, the empiricist epistemology is interested in the status of mathematical statements. Mathematical statements that have been proven are certainly true. Putnam wants to go further; for him, statements which do not have yet any proof, but have been *sufficiently* tested should also be considered true (the case of Goldbach's conjecture or Fermat's theorem), simply because the amount of empirical evidence supporting them is considerable. In my opinion, such a view is mistaken. Take, as an example, the continuum hypothesis. A great number of people, let us say before Cohen, were inclined to think that it was true. Now most logicians tend to believe that it is false, although

Cohen's proof does not have any bearing on its truth or falsity and still, one could say that it has been sufficiently tested. A simple number-theoretic statement like Fermat's theorem is more easily tested in terms of finite values of its variables than a transfinite number-theoretic statement which has no finite value or computational meaning. But the number of unsolved problems in elementary number theory should be an indication that testing is not sufficient. For example, Vinogradov's result "that each sufficiently large odd number is representable as a sum of three odd prime numbers" contains the phrase "sufficiently large" which has no computational meaning. We can say that a constructive proof is a conclusive test; but any test which does not amount to a proof is just a "counter-counterexample." Intuitionistically, if one has not tested the falsity of a given statement one cannot conclude to its truth, the principle of the excluded middle being "excluded" for non-finitely valued statements.

If I express Fermat's last theorem in the following form

$$(\mathsf{F}) \qquad \forall n > 2\ \forall xyz(x^n + y^n \neq z^n)$$

then I can classically define a natural number m by having

$$m = \begin{cases} 0, \text{ if } \mathsf{F} \\ 1, \text{ otherwise} \end{cases}$$

but this is not constructive, since **F** is not decided. So, let us suppose that we have a constructive proof of Fermat's theorem, which is certainly not excluded. Then I could define constructively or recursively a number m and the classical and the constructive definitions would coincide. But, in the absence of a proof, constructive or non-constructive, I cannot do better classically, even with all the individual value-tests that I can imagine, since **F** has not been proven.

Kreisel points out to the same problem from another angle in his review of Putnam's paper "Mathematics without Foundations".[7] In connection with Fermat's problem, Putnam wants a modal translation of a counterexample to Fermat's last theorem which is stated as follows

$$\Box[\mathrm{Ax}(\mathsf{S}, \mathsf{P}) \supset \mathsf{F}(\mathsf{S}, \mathsf{P})]$$

(for Ax a set of axioms of reduced number theory, S, sum and P, product). The statement says that it is necessary that if we have a counterexample to Fermat's last theorem, then the negation of Fermat's last theorem is implied by a set of axioms of reduced number theory. But Putnam fails to notice, as Kreisel points out, that such a Σ_1^0 sentence does not extend to a Π_1^0 sentence of the arithmetical hierarchy, i.e., for a sentence of the form

$$\mathsf{P}(\mathcal{A}) \leftrightarrow \mathsf{Q}x_1 \ldots \mathsf{Q}x_n\, \mathsf{R}(\mathcal{A}, x_1, \ldots, x_n)$$

where R is recursive and $\mathsf{Q}x_i$ is $\forall x_i$ ($\exists x_i$ for a Σ_1^0 sentence) and, of course, does not extend to second-order validity. All this *suffices*, in my opinion, to show the implausibility of Putnam's thesis that empirical evidence can establish the truth of a mathematical statement. What Putnam is trying to say in his empiricist epistemology is that our belief in the truth of **F** is based on an inductive argument, but I have argued that the probability of the belief is not the measure of the truth of a mathematical statement. Inductive evidence never amounts to mathematical truth.

6 I have attempted to show that number theory[8] is given a natural interpretation in a constructivist framework and that constructivist foundations of mathematics fare better than realism or empiricism. Despite the machinery I have introduced, constructivism is far from being completely justified. But in matters philosophical, complete justification is not attainable, as philosophical programmes seek for the most comprehensive understanding of the most extensive experience. Constructivist philosophy is not completely constructible, it has to be constructed *ad effinitum.*

POSTSCRIPT

Historically, the approach sketched here can be linked with the investigations of Hermann Weyl in his book *Das Kontinuum* (Leipzig, 1918). Weyl wants to build analysis on elementary categories (Grundkategorien) of objects to which are added properties and relations as ideal elements through substitution and iteration. Weyl thought that in this way he could escape type construction which led, for him, to an artificial and useless system (op. cit., p. 23).

It is interesting to note that Gödel in his paper "Ueber eine bisher noch nicht benützte Erweiterung des finiten Standpunktes" (*Dialectica*, vol. 12 (1958), pp. 280-287), uses essentially the same procedures, substitution and iteration (or recursion) on finite types, to obtain his proof of the consistency of classical arithmetic. Gödel's interpretation of number theory with functionals (extended to analysis by Spector and others) is no more strictly constructive in Weyl's sense: Weyl requires in his strict procedure, "engeres Verfahren", that the existential quantifier be applied only on the objects of elementary categories (op. cit., p. 21). Functionals of finite types make essential use of quantification on variables of arbitrary type (see Gödel's paper, op. cit., p. 284). Kreisel has also proposed in "Ordinal logics and the characterization of informal concepts of proof" (*International Congress of Mathematicians*, Edinburgh (1958), pp. 289-299) a more abstract scheme where enters the notion of finitist proof, which evidently is not finitist (i.e., combinatorial), but abstract or "ideal".

Our own notion of "metastasis" provides an intensional framework for such a scheme: it is not a type structure, but a system of reflection levèls, whereby operations on the primary level of the effinite series of natural numbers are seen to correspond to abstract performances; levels or strata are never supposed to be completed extensionally. Intensional closure suffices to guarantee the passage from one level to the other. Operations, not properties, are of the essence. Whether or not such a framework gives rise to a coherent theory of the continuum remains for the moment an open question.[9] But it is certainly consistent with the constructivist ideal.[10]

NOTES

1. These results have been proven by Vinogradov. See K. Prachtar *Primzahlverteilung*, Springer, Berlin (1957), pp. 177 and *ss*. These results have not yet been constructivized.

2. See G. Kreisel "Church's Thesis: a kind of reducibility axiom for constructive mathematics" in *Intuitionism and Proof Theory*, ed. by Kino, Vesley and Myhill, North Holland, Amsterdam (1970), pp. 124-124. See also, G. Kreisel, "Lawless sequences of natural numbers,:" *Compositio*, vol. 20 (1968), pp. 222-248, in particular, pp. 227-235. Kreisel makes also the basic distinction between mechanically effective and humanly effective (called *m*-effective and *h*-effective respectively by Kreisel). See "Which number-theoretic problems can be solved in recursive progressions on Π_1^1-paths through 0?" in *The Journal of Symbolic Logic*, vol. 37 (1972), pp. 311-334. Although some recent results by Prawitz and Mints, in particular on the functional equivalence of derivations and proofs, seem to cast doubt on Kreisel's intended use of the example, as Kreisel himself told us in conversation, it remains that the abstract (intensional) notion of proof is not reducible to the mechanical calculus of derivations. Whence the intrinsic value of the example.

3. See my "Constructivisme et structuralisme dans les fondements des mathêmatiques" to be published.

4. Harper Torchbooks (1971).

5. As for Putnam's treatment of predicative set theory, it assumes infinite sets to be definable without having to give a procedure to produce them.

6. Putnam has difficulties with conventialism, which is weaker than constructivism, for it does not justify conventions.

7. See H. Putnam "Mathematics without foundations," *Journal of Philosophy* (1967), pp. 5-22. Kreisel's Review is in *The Journal of Symbolic Logic*, vol. 37 (1972), pp. 402-404.

8. I have not examined algebraic number theory in this paper, but, from my point of view, algebraic concepts are structural ones, although some degree of constructivization can be achieved there. See Andrê Weil's remark in his *Basic Number Theory*, Berlin-Heidelberg-New York (1967), p. V, on the unification of prime field completions (real-number and *p*-adic fields) through adêle rings. For the combined (and harmonious) use of algebraic and analytic methods, see Jean-Pierre Serre *Cours d'arithmêtique*, Paris (1971). We have emphasized here problems in prime number theory. There are other problems in number theory which have an analytic solution, but do not have as yet an elementary one. One such problem is the so-called Dirichlet's class-number formula for quadratic forms

$$C(-p) = \frac{B - A}{p}$$

where C is the class of reduced forms of discriminant $-p$, B the sum of all the quadratic non-residues and A the sum of all the quadratic residues (mod p).. Dirichlet gave a proof of the equation using infinite series. The fact that this formula does not have an elementary proof is dramatized by the remark that it simply asserts the equality of two natural numbers (see H. Davenport, *The Higher Arithmetic*, 3rd Ed., London (1968), pp. 146-148). This does not affect, however, our foundational scheme where infinistic methods are "effinitized".

9. Hermann Weyl's approach to the foundations of analysis has been pursued by P. Lorenzen, *Einführung in die operative Logik und Mathematik*, Zweite Auflage, Springer-Verlag, Berlin-Heidelberg-New York (1969), who uses the notion of "Sprachschichten" or "language strata". For a still different constructivist approach to analysis, see E. Bishop's *Foundations of Constructive Analysis*, McGraw-Hill, New York (1967), where "complemented sets" play an essential rôle. Finally, Brouwer's treatment of the continuum has been developed by

R. E. Vesley in "The intuitionistic continuum," chapter III of *The Foundations of Intuitionistic Mathematics* by S. C. Kleene and R. E. Vesley, North-Holland Co, Amsterdam (1965).

10. It should be noted finally that there are interesting parallels between Weyl's ideas and Hilbert's finitist constructivism. In his paper "Ueber das Unendliche", *Mathematische Annalen*, vol. 95 (1926), Hilbert speaks of the introduction of ideal elements in mathematics in a manner similar to Weyl's (the example of Kummer's ideals). But the general metamathematical certainty (Sicherheit) explains the choice of our topic. It should also be pointed out that Skolem's construction of elementary arithmetic through the use of primitive recursive functions follows a finitist line; the radical elimination of quantifiers or "apparent" variables does not provide a sufficient basis for analysis however (see "The foundations of elementary arithmetic established by means of the recursive mode of thought, without the use of apparent variables ranging over infinite domains" in J. van Heijenoort *From Frege to Gödel*, Cambridge, Massachusetts (1967). The approach sketched here could be called an "effinitist" extension of the finitist standpoint.

University of Montrêal
Montrêal, Quêbec, Canada