What Were Thought to be the Foundations of Mathematics Before 1850?

(Talk given at regional AMS meetings, Miami, FL, April 1, 2006)

A letter Kummer wrote in 1846 states that Gauss, fifty years earlier, when he was writing the *Disquisitiones Arithmeticae,* had at his disposal a concept like Kummer's newfound "ideal prime factors," but that he did not include it in the *Disquisitiones* because he had not been able to put it on a firm foundation ("er dieselben aber nicht auf sicheren Grund zurückgeführt hat"). The question of my title refers to the "foundations of mathematics" in this sense. What, for Gauss, would have constituted a firm foundation?

Another reference to the foundations of mathematics in the first half of the 19th century was Abel's complaint in the opening pages of his article on the binomial series (1826) that even such a frequently used tool as the binomial series for fractional exponents had not been rigorously investigated. He said, "The number of theorems regarding infinite series that can be regarded as rigorously established is very limited." What did "rigorous" mean to him?

I hope you will readily agree that in neither case did the question have anything to do with set theory, the subject that in our day has somehow become identified with "the foundations of mathematics."

Abel states a specific goal: "Find the sum of the series

$$1+\frac{m}{1}x+\frac{m(m-1)}{1\cdot 2}x^2+\frac{m(m-1)(m-2)}{1\cdot 2\cdot 3}x^3+\cdots$$

for all values of x and m, real or imaginary, for which it converges." That is admirably specific, but it says nothing about how he will "rigorously establish" his answer. He offers no definition of "real numbers", much less of "imaginary numbers." He cites Cauchy's "Cours d'analyse" and states what is today called the Cauchy convergence criterion, but his statement of the criterion refers to "limits" with no explanation whatever of the limit concept.

These observations about what Abel does *not* say about the foundations point to a major difficulty in discovering what mathematicians in the past thought of as the foundations of mathematics. The foundational ideas are the ones everyone knows and agrees on, so they are the ones that need—and get—no explanation. In Abel's case, it would seem that "number" and "limit" are such ideas. The mathematical culture of a period is the common property of all readers of the period, but once those readers are gone it is very hard to reconstitute the things they were all expected to understand.

An instance of this phenomenon that I am particularly fond of, for a reason you will see in a moment, is the following experience I had in connection with my book on Galois theory. Galois's famous memoir on the algebraic solution of equations is notoriously terse, and on no point is it more terse than in the proof of his crucial Lemma III. I won't take the time to explain what that lemma states or what he offers in the way of proof. Suffice it to say that in my book I gave a reconstruction of what I believed to be Galois's argument, and that Peter Neumann in his prize-winning review of the book called my reconstruction "far-fetched." The main step in the reconstruction—Galois's key idea, as I saw it—was that *if two polynomials have just one root in common, then that root can be expressed rationally in terms of the coefficients of the polynomials.*

Some years later I was delighted to find this very statement in a work of Abel, preceded by the phrase "as everyone knows" ("comme l'on sait"). The issue is a little more nuanced than I have painted it, and I may not be doing justice to Neumann's criticism of my reconstruction, but I think you can see my point. It is almost impossible to understand a text from a byegone era without understanding what readers were expected to know, and, especially in the case of mathematical writing, it is difficult to discover what readers were expected to know because—well, because it wasn't written. Everybody was expected to know it.

I have long believed that Kummer's brief paper introducing his ideal prime factors gives an exceptional window into the foundational ideas of his time, because he was trying to present a profound new idea in a way that would be attractive and comprehensible to his contemporaries. What we learn from reading this paper, I believe, is that Kummer's approach to his subject was fundamentally *algorithmic.* He made no attempt to say what ideal prime factors *were,* and said only how to *compute* with them. (A few decades later, Dedekind would complain about this very property of Kummer's method.) Given a rational prime, Kummer described how to determine its ideal prime factors in a given cyclotomic field and, for any cyclotomic integer, how to determine the multiplicity with which it is divisible by a given ideal prime factor. In other words, he gives an operational definition of the ideal prime factors.

Their usefulness lies in the theorem which states that one cyclotomic integer divides another if and only if each ideal prime that divides it divides the other with multiplicity at least as great. All of this is entirely algorithmic, and it was firmly founded on what we know were voluminous *calculations* on Kummer's part. (In fact, in a few cases, Kummer's conclusions were based *only* on voluminous calculations, and the proofs he gave of some of them needed to be shored up years after they had been published.)

More generally, I believe the same is true of most of higher mathematics in the first half of the 19th century. *What everybody was expected to know was how to compute.* The focus was not on "what is a number?" or "what is a limit" but "how do you effectively compute with numbers?" and "how can you evaluate a limit?" Abel's study of the binomial series was directed at *evaluating the sum* whenever the series converges.

My thesis is that the metaphysical question "what is a number?", although it may have received some attention in connection with the solution of algebraic equations in the 16th, 17th, and 18th centuries, and although it received great attention in the second half of the 19th century—one thinks in particular of Dedekind and Cantor—was not a major issue during the period under discussion, at least not among the mathematicians we regard today as having been the foremost of their contemporaries.

Without question, *the* foremost was Gauss, and the extent to which he avoided metaphysical questions is especially noteworthy. The *Disquisitiones Arithmeticae* are of course about *arithmetic,* which is to say about *whole numbers.* Was this an avoidance of metaphysical questions by staying with the solidest of mathematical subjects, the arithmetic of whole numbers? Hardly. He *begins* with the notion of congruence of numbers. This is a subject on which much useless nonsense has been written in our time, stating that one is "really" dealing with *equivalence classes of integers.* From a set-theoretic point of view, it is probably inevitable to think of congruences in that way, but clearly Gauss did not think of them in that way, and set theory plays no role in his exposition. He says what it means for two numbers to be congruent mod n and observes, in essence, that this relation is consistent with addition and multiplication in the sense that if $a \equiv a' \bmod n$ and $b \equiv b' \bmod n$ then $a + b \equiv a' + b' \bmod n$ and $ab \equiv a'b' \bmod n$. He *uses* the congruence concept to frame his proofs and to simplify his computations, but he pays no attention whatever to what its metaphysical significance might be.

This occurs at the very outset of the *Disquisitiones Arithmeticae.* There are at least two later points in the book where he noticeably omits metaphysics and remains firmly in the realm of computation.

One is his treatment in Section 5 of the operation of *composition of forms*—one of his great innovations and one of his great contributions to mathematics. Again he defines in a clear algorithmic way what it means to say that a binary quadratic form *composes* two others. This is a subject on which much has been written to explain what a composition "really" is. But Gauss gives it not a moment's attention. In a *tour de force* of algebra, from his stupendously general and concrete definition of the notion of composition, he deduces necessary and sufficient conditions for a given pair of forms to have a composition and, when they do have one, to find them all.

This is certainly the hardest part of the book, and much effort has been spent on it in the last two centuries to try to simplify it and say what it is "really" about. For example, there is a sort of associative law involved with compositions that one feels "should" have a much more evident formulation than the one Gauss gives it. But Gauss is pitiless, and many of the attempts to simplify and explain this part of the book have been misguided and have lost a great deal in the translation.

(Much of what has been written in "explanation" of Section 5 ignores the fact that Gauss does not "compose" two forms, but says what it means to say that a form "composes" two others. It is in no way a binary operation in the way that many treatments of it would have us believe. Two given forms may not be composed by any form, but if they are composed by one form they are composed by infinitely many.)

The third place in the *Disquisitiones* where Gauss conspicuously avoids metaphysics is in the last section, Section 7, on the division of the circle. Here he makes use not only of fractions—in a book about arithmetic, mind you—but also of *complex numbers.* In one place (§353) he computes the 19th roots of unity to 10 decimal places! How does he justify the introduction of such alien topics in his book?

"The reader might wonder that such researches are included in a book that at first glance would seem to be dedicated to such different topics." The reader might well wonder. He goes on to say only that "the treatment itself will, however, show clearly in what close connection this topic stands to the higher arithmetic." Indeed, it is in this part of the book that he proves a theorem that can be interpreted as describing the number of solutions of $x^3 + y^3 + z^3 \equiv 0 \bmod p$. (To give you the number-theoretic flavor of the subject, let me say that this problem in the *Disquisitiones* is the beginning of the study of arithmetical properties of elliptic curves. The amazing answer he found is that the number of such solutions, counted as in projective geometry, is $p+1+A$, where A is is determined by two conditions $4p = A^2 + 27B^2$ and $A \equiv 1 \bmod 3$.) No one could deny that that is a theorem in higher arithmetic. Certainly the use of complex numbers is not essential to his proof of the result, but it would seem that in Gauss's mind there was no need to keep them out if they were convenient to use. Certainly he didn't worry at all about the question "what are real numbers" or "what are complex numbers" that would be worried about to such an extent later in the 19th century.

There are reasons these attitudes changed—chief among them was the success of Fourier analysis and its encouragement of the most general possible conception of the notion of a function of a real variable—but I feel that much was lost when they did change, and that it is useful to remember that our present-day tendency to see the foundations of mathematics as being inextricably linked with set theory is at the very least optional.

Not many mathematicicans today share my belief that the modern set-theoretic approach to the foundations of mathematics is harmful to mathematics. But it seems to me indisputable that such modern prejudices are harmful to the study of the mathematics of the first half of the 19th century. Let us recognize this, and oppose efforts by our non-historian mathematical colleagues to tell us what Gauss, in his clumsy way, was "really" trying to say.