Fermat Meets SWAC: Vandiver, the Lehmers, Computers, and Number Theory

Leo Corry

IEEE Annals of the History of Computing, Volume 30, Number 1, January-March 2008, pp. 38-49 (Article)

Published by IEEE Computer Society

Fermat Meets *SWAC*: Vandiver, the Lehmers, Computers, and Number Theory

Leo Corry
Tel Aviv University

This article describes the work of Harry Schultz Vandiver, Derrick Henry Lehmer, and Emma Lehmer on calculations related with proofs of Fermat's last theorem. This story sheds light on ideological and institutional aspects of activity in number theory in the US during the 20th century, and on the incursion of computer-assisted methods into pure fields of mathematical research.

The advent of the electronic digital computer opened a new era of unprecedented possibilities for large-scale number crunching. Beginning in the late 1940s, these gradually increasing possibilities were duly pursued in many branches of science. Some of them, like meteorology, geophysics, or engineering science, underwent deep and quick transformations. Pure mathematical disciplines such as number theory can be counted among the less receptive audiences for these newly opened possibilities. One way to account for this somewhat ironic situation is to examine the main research trends that shaped progress in the algebraic theory of numbers from the second half of the 19th century on. Central to such trends was a conscious attempt to develop powerful conceptual tools for solving theoretical problems "purely by ideas" and with "a minimum of blind calculations." Indeed, this became an ethos that gradually came to dominate most fields of pure mathematics after 1930.

This conceptual approach was developed by leading German mathematicians such as Richard Dedekind (1831–1916) and David Hilbert (1862–1943) on the basis of ideas that first appeared in the work of the great Berlin number-theorist, Ernst E. Kummer (1810–1893), in the 1850s. But Kummer's own work actually features many massive computations with particular cases that would eventually disappear from the algebraic theory of numbers by the turn of the 20th century. Among other things, Kummer's research led in 1859 to a famous result, namely, that Fermat's last theorem is true for all prime exponents less than 100. Extending this result beyond 100 involved, above all, straightforward (if tedious) computations. Yet, little work was devoted to such computations before 1920, and even then, this remained an essentially marginal trend within number theory.

Thus, when electronic computers started to became available in the late 1940s, few mathematicians working in the core, "pure" fields of the discipline incorporated them in their research agendas. Even fewer did so for Fermat's last theorem. Harry Schultz Vandiver (1882–1973) was one of the few to do so. He joined forces with the couple Derrick Henry Lehmer (1905–1991), and Emma Lehmer (1906–2007). The Lehmers possessed the necessary expertise that combined deep knowledge in both number theory and the use of electronic computers. They also had the institutional connections that facilitated the use of computing resources with SWAC (Standards Western Automatic Computer) on behalf of this project.

This article describes the work of these three mathematicians in connection with Fermat's last theorem, and how they came to introduce electronic computers to research on that problem.

From Sophie Germain to Kummer

Sometime after 1630, Pierre de Fermat wrote in the margins of a book that the equation $x^n + y^n = z^n$ has no nontrivial integer solutions x,y,z, when $n > 2$. He also claimed to have found a proof for this fact, which the margins of his book were too narrow to contain. Eventually, this unproved conjecture became

 Published by the IEEE Computer Society 1058-6180/08/$25.00

known as Fermat's last theorem. Attempts to prove it, and indeed to find Fermat's putative proof, were unsuccessful. The problem increasingly attracted the curiosity of mathematicians and amateurs alike, while becoming the object of many legends. The mythical dimension of its story was greatly heightened after the grand finale provided by the brilliant, surprising, and highly complex proof, advanced in 1994 by Princeton mathematician Andrew Wiles that turned the theorem, and many names associated with it, into the focus of unusual public attention.[1] But as a matter of fact, an attentive reading of the historical record shows that from its very inception, this was an open conjecture to which few mathematicians (and above all few outstanding number theorists) dedicated sustained research efforts worthy of that name—the kind of attention they devoted was mostly passive.

Born on the physical margins of a book, for more than 350 years Fermat's theorem essentially remained at the margins of the mathematics profession, brought occasionally into the limelight before the work of Wiles.[2] Still, the theorem's history is important in many senses, and this is also the case concerning the question of the relationship between conceptual breakthroughs and intense calculation in mathematics.

In the early 19th century, some of the sporadic efforts toward proving the theorem yield interesting results that set the scene for the vast majority of subsequent contributions (prior to Wiles' proof that eventually came from a completely different direction). In this section, I cursorily present those results and the concepts associated with them, inasmuch as they are necessary for understanding the starting point of Vandiver's work.

An early, significant result specifically arising from attempts to prove the theorem was advanced by Sophie Germain (1776–1831). As a woman, Germain initially worked outside the mathematical establishment of her time, and corresponded with Carl Friedrich Gauss using a pseudonym. The theorem that was later associated with her name implied that Fermat's last theorem can be fully elucidated by handling the following two separate cases:

- Case I—none of the integers x,y,z is divisible by p;
- Case II—one, and only one, of the integers x,y,z is divisible by p.

Germain proved case I for all primes under 197.

Adrian Marie Legendre (1752–1833) was a prominent French mathematician who was among the first to acknowledge Germain's talents. He corresponded with her and tried to use her methods for proving additional cases. Case II turned out to be much more difficult from the beginning. For $p = 5$, case II was proved only in 1825 in separate, complementary proofs of Legendre and Peter Lejeune Dirichlet (1805–1859). Dirichlet also proved in 1832 case II for $n = 14$, and he did so while trying to prove it for $p = 7$. This latter case turned out to be especially difficult, and it was finally proved in 1839 by Gabriel Lamé (1795–1870).[3]

The next significant contribution came from Kummer. His line of attack originated in his efforts to address what he considered to be the most important question in number theory, namely, the so-called higher reciprocity laws. Kummer's interest in Fermat's last theorem was only ancillary to this, but he relied on an important insight discovered as part of these efforts, namely the identification of a special class of prime numbers, later called "regular." In 1850, Kummer proved that the theorem is valid for all regular primes.

Kummer also provided an algorithm based on the use of so-called Bernoulli numbers, B_n, in order to tell for a given prime number whether or not it is regular. Using the values of B_n known at the time, he worked out all the computations necessary to see the only nonregular primes he found below 164 were 37, 59, 67, 101, 103, 131, 149, and 157. He did not go beyond 164, possibly because of the complexity and length of the calculations involved. At any rate, Kummer initially believed that there would be infinitely many regular primes, and indeed that only a few primes would be irregular.

Kummer naturally asked himself how to go about the case of irregular primes. He brilliantly developed three criteria that provided a sufficient condition for the validity of Fermat's last theorem for a given irregular prime p. Checking the criteria for any given p involves a considerable computational effort, but they do yield clear results. Kummer was by no means intimidated by the need to make the necessary calculations. And, indeed, in 1857 he published a famous article that broke new ground, both conceptually and in terms of specific calculations[4] It introduced the three said criteria and proved that each of the three irregular primes smaller than 100 satisfies them. He thus achieved the impressive result that Fermat's last theorem is valid for all exponents under 100.

Kummer never published his calculations nor explained any specific formula that perhaps facilitated these calculations. Clearly, the latter were lengthy and demanding. Indeed, Kummer's work turned out to contain some relatively minor inaccuracies, but this was found out for the first time only in 1920 by Vandiver. It was clear at this point, at any rate, that Kummer's results might be extended with additional calculations involving Bernoulli numbers. In particular, it would be necessary to add new values to the list of known ones. Leonhard Euler had initially calculated values up to B_{15}. After his work, the values up to B_{31} were calculated in 1840 by Martin Ohm (1792–1872), the younger brother of the physicist Georg Ohm.[5] These values were known to Kummer, and his results of 1857 relied on them. Thereafter, additional values were calculated only much later, by John Couch Adams (1819–1892) in 1878 (up to B_{62}) and by an obscure Russian mathematician Sergei Serebrenikoff in 1906 (up to B_{92}). To be sure, neither of them calculated these values as part of an effort to prove Fermat's last theorem.[6] Adams, for instance, was a leading British astronomer. His calculations were related with his involvement in the formulation and publication of astronomical tables. Despite their possible application to Fermat's last theorem, no other mathematician seems to have thought that calculating further values was worth the effort.

Computing from Kummer to Vandiver

Following Kummer, it was possible in principle to continue the search for irregular primes. For each new irregular prime found, one might check if Kummer's criteria applied. As the criteria did not suffice to prove all cases, it was evident that there was also room for refining and further elaborating criteria of this kind, in order to find more efficient tests for a given prime irregular exponent. As it happened, however, very little research was done in this direction in the following decades. As an example, an important fact about irregular prime numbers—namely, that there are infinitely many of them—was proved only in 1915. The proof did not contain any conceptual innovation, and it was published by an unknown student in an obscure Danish journal.[7] The first report of this result in an English publication appeared only in 1928.[8]

On the other hand, Kummer's theory of ideal numbers opened a new conceptual direction, which served as a starting point for important developments in number theory in the second half of the 19th century, although these developments had little to do with proving Fermat's last theorem. Mainly under the influence of an approach embodied in Dedekind's work on the theory of ideals, new ideas on the theory of algebraic fields gradually developed in a direction that explicitly distanced itself form the kind of calculational efforts developed by Kummer himself. At the turn of the 20th century, particularly in the wake of Hilbert's influential *Zahlbericht* [Report on Numbers], published in 1897, a clear emphasis on the ''conceptual'' perspective became dominant. Results based on specific calculations with particular examples were not favored under this view, which was most clearly presented in the introduction to the *Zahlbericht*. Hilbert thus wrote:

> It is clear that the theory of these Kummer fields represents the highest peak reached on the mountain of today's knowledge of arithmetic; from it we look out on the wide panorama of the whole explored domain since almost all essential ideas and concepts of field theory, at least in a special setting, find an application in the proof of the higher reciprocity laws. I have tried to avoid Kummer's elaborate computational machinery, so that here … proof can be completed not by calculations but purely by ideas.[9]

The deep influence of the approach espoused by Hilbert and by some of his colleagues helps explain why the way originally opened by Kummer, or other methods involving lengthy calculations of particular cases, eventually become marginal to the mainstream of 20th-century number theory.

Back in the second part of the 19th century, however, there was still much number-theoretical activity, especially in France and Belgium, where calculations with individual cases was central. As part of this kind of research, a few results pertaining to the theorem were published between 1856 and 1915. These involved varying degrees of mathematical sophistication and represented little real progress over what Kummer had already achieved.[10] Three illustrative examples concerning case I are the following:

- Edmond Maillet proved in 1897 that case I is valid for $p < 223$,
- Dimitry Mirimanoff (1861–1945) extended this in 1904 to $p < 257$,
- In 1908, Leonard Eugene Dickson (1874–1954) introduced new methods to prove

that case I is true for every exponent $p < 7000$.

For case II, almost nothing new was achieved.

A different direction of progress started with the work of Arthur Wieferich (1884–1954), who proved that if p were an exponent for which case I is valid, then the following identity would hold: $2^{p-1} \equiv 1 \pmod{p^2}$. Mirimanoff in 1910 extended this result by proving that the same p would satisfy $3^{p-1} \equiv 1 \pmod{p^2}$. Subsequently, the same congruence $m^{p-1} \equiv 1 \pmod{p^2}$ was proved true in relation with case I for higher values of m in a series of works, including the following:

- In 1912, Philip Furtwängler (1869–1940) proved that the condition $r^{p-1} \equiv 1 \pmod{p^2}$ holds true for every factor r of x (in case x is not divisible by p), and for every factor r of $x^2 - y^2$ (in case $x^2 - y^2$ is not divisible by p),
- In 1914, Vandiver proved the congruence for 5^{p-1},
- In 1914, Georg Ferdinand Frobenius (1849–1917) proved the congruence for 11^{p-1} and for 17^{p-1}.

Now, here is where mechanized calculation makes its appearance, albeit still in a modest way. Based on works such as just mentioned, it became possible to determine a lower bound for the value of integers for which the Diophantine equation associated with case I could be satisfied. This required, however, increased amounts of rather complex calculations. In 1913, Waldemar Meissner combined Furtwängler's general theorem with recent results known through tables that had been obtained by arduous calculations.[11] Meissner referred to a recent Russian textbook on number theory, written by Ukrainian mathematician Dimitri Grawe (1863–1939), which contained a table of residues modulo p of the ratios $2^{p-1} - 1/p$, for all prime numbers $p < 1000$. Grawe had stated his belief that Wieferich's congruence holds for no prime p. ''Had he continued to the next 1000,'' Meissner wrote, ''he would have found that the prime number $p = 1093$ does satisfy the congruence. Indeed, this is the smallest number under 2000 to satisfy the congruence.''

The next related result came only in 1925 when a Dutch high school teacher, N.G.W.H. Beeger (1884–1965), proved that between 2,000 and 14,000, the only exponent p that satisfies the Wieferich congruence is 3,511.[12] Beeger explained the method of his calculations, his checking, and why he was so confident of them. Moreover, he disclosed, that he ''constantly used W.J. Odhner's 'Brunsviga' calculating machine.'' Given the calculations' complexity, one suspects that Meissner may also have used some kind of machine, but he never said as much. So, with Beeger we find the first explicit testimony about a mechanical device being used in relation with Fermat's last theorem.[13] Beeger returned to this problem once again in 1939, and, using Dickson's result of 1907, he proved that case I is valid for exponents up to 16,000,[14] including both regular and irregular prime exponents.

Vandiver, the Lehmers, and Fermat

Andrew Wiles devoted no fewer than eight full years of his professional life to work out a complete a proof of Fermat's last theorem. Before him, and despite the legendary status of the problem, there was only one other professional mathematician—Harry Schultz Vandiver—to have ever spent a significant part of his career pursuing the same task while achieving many nontrivial results. Although Vandiver published in other (related) fields of research as well, such as cyclotomic fields, associative algebras, ring theory, reciprocity, and quadratic forms, Vandiver devoted his entire professional life to a well-known problem that aroused curiosity but that had remained on the margins of number theory for decades. Together with some conceptual advances over his predecessors, Vandiver undertook a research program involving massive calculations with individual cases. When he aided himself with electromechanical—and later on, electronic—devices for his calculations, he was certainly in the minority of number-theorists who would consider this an exercise worthy of a true mathematician's time.

Vandiver's first article on Fermat's last theorem appeared in 1914 in Crelle's *Journal*.[15] As already mentioned, it comprised an extension to base 5 of the Wieferich-Mirimanoff type of criterion. Over the years, he continued to present short communications to the American Mathematical Society (AMS) containing improvements and simplifications of Kummer's criteria or of results related to his own 1914 article. Thus, for instance, in 1920 he identified and then corrected a mistake in a central argument of Kummer's important 1857 article.[16]

In 1931, Vandiver was awarded the first Cole prize established by the AMS for outstanding research in number theory. This came in recognition to a series of works on

Figure 1. Dick Lehmer probably around the time of his graduation from the University of California, Berkeley, c. 1927. (Courtesy of Laura Gould.)

Fermat's last theorem published beginning in 1926 and summarized in a detailed article published in 1929 in the *Transactions of the AMS*.[17] Among other things, this work implied the first meaningful advance since the time of Kummer in dealing with case II. It took care of, among other things, case $p = 157$, which could not be accounted for by Kummer's criteria. Vandiver undertook to develop new criteria that would yield a proof for this case, and in doing so, he actually extended the validity up to $p = 211$. In fact, even before the article appeared in print, Vandiver had realized that his arguments were valid for exponents $p < 269$.

Besides refining the Kummer-type criteria for proving the theorem in the case of irregular exponents, Vandiver also worked on the side of the Bernoulli numbers. He proved several congruences involving such numbers in order to allow more efficient calculations related to the criteria. In addition, together with his collaborators, he sought ways to improve the methods for calculating increasingly high instances of Bernoulli numbers. He also coordinated the work of graduate students who would perform specific calculations for sets of cases they were assigned. The students were aided by the use of Monroe and Marchant electromechanical calculators. Vandiver also relied on existing mathematical tables of various kinds, but he systematically reassured readers of his articles that these tables had been rechecked independently by his comparing one with the other.

In 1937, Vandiver published his first work in collaboration with the Lehmers. That this collaboration took place at all was far from a coincidence. Dick Lehmer was greatly influenced by the work of his father, a University of California, Berkeley, mathematician, Derrick Norman Lehmer (1867–1938). The latter published in 1909 a *Factor Table for the First Ten Millions* and in 1914 a *List of Prime Numbers from 1 to 10,006,721*.[18] As an undergraduate, Dick built a number sieve based on a set of bicycle chains hanging on sprockets attached to a shaft and turned by an electric motor. In 1929, Derrick Norman published his *Factor Stencils* that gave a method of factorizing a number using cards with holes punched in them. Dick was directly involved in this project. In 1932, Dick constructed, now with his father's help and encouragement, a highly ingenious photoelectric number sieve.[19] The use of mechanical or other aids to computation was a main theme in Dick Lehmer's professional life, and so was the question of factorizations and primes. In the 1930s, he devised the famous Lucas-Lehmer primality test for Mersenne numbers.

It was also through his father that Dick (see Figure 1) came to know his future wife and mathematical partner of a lifetime, Emma Trotskaya (see Figure 2). This occurred when she was an undergraduate student at Berkeley attending Derrick Norman's class. Dick went to Chicago for doctoral studies with Dickson, but stayed there for only one year. The couple married the year Emma graduated and moved to Brown University, where in 1930 Dick completed his PhD under Jacob D. Tamarkin while Emma was awarded her MSc.[20]

Emma and Dick moved to Lehigh University in 1932, and it is there that the collaboration with Vandiver (see Figure 3) began. The work by the Lehmers was funded by a Penrose Scholarship granted to Vandiver by the American Philosophical Society. Part of the money went to renting a 10-10-20 electric Monroe machine (http://www.xnumber.com/xnumber/pic_monroe_electr.htm) at a cost of US$25 per month. The rest helped pay the Lehmers, even though this collided with the terms of Dick's employment at Lehigh. In 1934, Dick Lehmer wrote to Vandiver:

> As I see the situation, you have to assure the APS that I am doing at least 1/3 of the work,

> whereas I have to assure Lehigh University that I am merely supervising the work and only spending a few hours a week on this research, printed accounts of the project to the contrary notwithstanding. I think that both of these may be possible although they are somewhat contradictory.[21]

At the same time, he reassured Vandiver that "after a little experimenting the work of computing the B_i's will become quite routine." Dick had little doubt that if he could "get Mrs. L. to do more than her share of the work (while I teach freshmen)" progress would come soon.

An immediate concern addressed by the Lehmers related to the improvement of the recurrence formulas for calculating Bernoulli numbers. Dick devised a new method based on "lacunary recurrence," namely, one in which only some of the previous values are used for calculating each new one.[22] He took as reference the tables prepared by Adams and by Serebrenikoff (whom he dubbed "intrepid calculators"), and applied his newly developed method to check, in the first place, that the results coincided. Then, he went on to calculate values of up to B_{196}.

In the correspondence of these years, important topics arise that attest to the Lehmers' clear conception of what a properly implemented computing procedure would comprise. For example, they were always sensitive to the degree of efficiency of the methods used for calculations, the estimated timings, the reliability of the results, and, no less than that, the clarity of presentation. As Dick wrote in 1934:

> We have B_{96} and are well on the way towards B_{99}. I think that the average time required for each B will simmer down to abut 20 hours. About 1/3 of this time is used in typing results and 1/10 of it in checking. Of course, the final check (the exact division of a 250-digit number by a 50-digit number) would be sufficient, but coming as it does at the end of 20 hours it is necessary to check more frequently. We use as an additional check the casting out of 1000000001.[23]

Calculating the value of B_{105}—he reported a few weeks later—had required 70 hours to complete.

But the question that more recurrently appears in these as well as in later letters concerns the matter of publication: who would want to publish this kind of results, and what exactly should be published? What tables? How many results for each case? As a matter of fact, Dick understood that the very task of calculating new values of Bernoulli numbers was not one that his mathematical colleagues would hold in high esteem. He thus opened his 1935 article by trying to justify the task itself. He wrote:

Figure 2. Emma (Trotskaya) Lehmer at her wedding in 1928. (Photo courtesy of Laura Gould.)

> The reader may question the utility of tabulating more than 93 Bernoulli numbers, and hence the need of giving formulas for extending their calculations. It is true that for the ordinary purposes of analysis, for example in the asymptotic series of Euler MacLaurin summation formula, a dozen Bernoulli numbers suffice. There are other problems, however, which depend upon more subtle properties

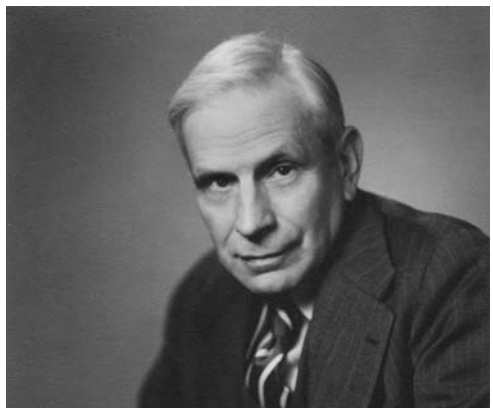

Figure 3. Harry Schultz Vandiver, c. 1936. (Creator: Walter Barnes Studio. Courtesy of the Center for American History, University of Texas at Austin.)

> of the Bernoulli numbers, such as the divisibility by a given prime. Examples of such problems are the second case of Fermat's Last Theorem and the Riemann Zeta-function hypothesis. Our knowledge as to the divisibility properties of the Bernoulli numbers is still quite primitive and it would be highly desirable to add more to it even if the knowledge thus gained be purely empirical.[24]

Still in connection with this issue, it should be noted that the actual values he calculated were published in the then-new *Duke Mathematical Journal*.[25] This not-accidental choice concerned the contents of the article and the reactions it elicited. As Dick wrote to Vandiver:

> I had tried the *Annals* but received an immediate rejection from Lefschetz on the grounds that it is against the policy of the *Annals* to publish tables. He suggested that the tables be deposited with the AMS library or else published in some obscure journal. So I tried the Duke journal.[26]

Solomon Lefschetz (1884–1972) was at the time president of the AMS and editor of the prestigious *Annals of Mathematics*. His reported reaction merely hints to the much broader and complex phenomena of the status within the mathematical community (in the US and elsewhere) of mathematical tables, their elaboration, and publication.[27] Evidently, Vandiver and the Lehmers did not view this question eye-to-eye with the mathematical establishment. They published the results of their collaboration in *Duke* and in the *Proceedings of the National Academy of Science* (*PNAS*), rather than in mainstream mathematical journals of the time. In fact, Dick Lehmer's institutional connections sensibly differed from those of most mathematicians across the country. As will be explained, he worked for the National Bureau of Standards, and in 1938 he was involved in the committee of the *Mathematical Tables Project*, sponsored by the NBS.[28] In addition, he was among the founders of the new journal, *Mathematical Tables and Other Aids to Computation*, published by the National Research Council beginning in 1943. In 1960, the journal's name was changed to *Mathematics of Computation*, and it was only in 1962 that the AMS became associated with its publication. When one considers today the professional prestige that this journal has come to achieve, it is evident that its changing status reflects an interesting underlying (and yet to be told) story of six decades of change in scientific values, in approaches to research, and in institutional structure in American mathematics.

The first results of the Vandiver–Lehmer collaboration were also published in *Duke*. Vandiver was listed as the author, and he explicitly acknowledged the collaboration of the Lehmers. This article established the theorem for exponents p, $2 < p < 619$, except possibly for 587.[29] The latter case raised some computational difficulties which were nevertheless soon overcome and the result published in 1939.[30] It was also clear, by this time, that above 619 the calculations became prohibitively long and laborious for being carried out with a desktop calculator.

In 1940, Dick accepted a position offered to him at Berkeley. Then, in 1945 Dick went to work on the ENIAC project at the Aberdeen Proving Ground. Of course, most of his time was devoted to the task of computing trajectories for ballistics problems, but the Lehmers used some of the available time over the weekends to questions related with number theory. Above all, this period served as an important training in the use of electronic computers.

In August 1950, 24 faculty members who refused to sign a new oath of loyalty required by the authorities at Berkeley were dismissed. Dick was coerced to sign, but he took a leave of absence, and it was quite clear that he would not return unless the controversy were settled satisfactorily. He then became director of the Institute for Numerical Analysis recently established at UCLA. This period, of considerable historical interest in many respects, also opened the way to Dick's involvement with SWAC: the Standards Western Automatic Computer (see Figure 4), at the NBS.[31]

SWAC and number theory

Problems in pure mathematics, and especially in fields like number theory, were by no means among the first to be addressed during the early years of electronic computers. Mainstream mathematicians working in ''pure'' fields, did not show much interest in the possibilities opened for their disciplines by this new technology. In addition, operational costs of the new machines had to be justified with more mundane pursuits than those provided by, say, number theory. And yet, some classical problems in mathematics were soon seen as a challenging test for computing power as well as for programming skills with the new machines. Thus, for instance, as early as 1949 John von Neumann suggested using ENIAC to calculate the values of π and e to many decimal

places. The idea was to develop tests for measuring randomness in the distribution of digits appearing in these two cases.[32] The problem of Mersenne primes, $M_n = 2^n - 1$, and the Riemann conjecture also attracted attention from very early on. Alan Turing addressed both problems at the University of Manchester in the years 1951–1952. The Lehmers were, of course, natural candidates to pursue these kinds of problems with electronic computers.[33] In 1952, they harnessed the new power provided by SWAC, and, joining forces with Raphael Robinson, they found out that M_{521} was prime. They were happy to declare that: "Each minute of machine time is equivalent to more than a year's work for a person using a desktop calculator."[34]

Fermat's last theorem, a problem to which mainstream number-theorists had devoted so little interest since the time of Kummer, was also relatively late in receiving the attention of those who applied electronic computers to the field. One can only speculate how much longer it might have taken, if at all, were it not for the previous collaboration between Vandiver and the Lehmers. Although it represented a natural continuation of the work done between 1935 and 1940, with a new and much more powerful technology at hand, Vandiver did not immediately think that SWAC should be used for this purpose. Emma Lehmer continually informed Vandiver about progress on computations with Mersenne primes, and explicitly wrote him that "if you have some pet problem you would like to run, I might try my hand at coding it and maybe we can run it after hours."[35] Amazingly, as late as April 1952, Vandiver replied that "no particularly numerical problem occurs to me that may be handled by the machine; but if one does, I'll let you know."[36]

Actual work on the theorem started in June 1952, and the results of this joint research were published in 1954. Work was done in two parts:

- identifying all the irregular primes below 2,000; and
- checking that each irregular prime thus found satisfied necessary criteria for ensuring that the theorem held for that case.

The criteria introduced by Vandiver in 1929, and which improved on Kummer's, were not easily turned into programmable algorithms. Thus, Vandiver was required to modify them accordingly, which he did very successfully. For reasons of space, the criteria and the interesting way in which they were implemented in SWAC cannot be given in detail in this article.[37]

Figure 4. Harry Huskey sitting in front of the SWAC computer console, c. 1950. (Courtesy of the Computer History Museum.)

The irregular primes found in the first part were given as output by SWAC in the form of punched cards indicating all irregular primes. The SWAC output also listed the "ranks of irregularity"—namely, all indexes a_i ($a_i \leq (p - 3)/2$) of Bernoulli numbers B_{ai} divisible by p. The largest rank found in the cases examined was three.

In June 1953, the Lehmers cabled Vandiver and announced:

> SWAC discovers new irregular primes 389, 491, 613, 619, corresponding to Bernoulli subscripts 100, 168, 261, 214. Primes like 619 require 90 seconds.[38]

Actually, for values of $p < 619$, the results were checked against those obtained previously, in 1937. In principle, the results coincided, but with some exceptions: $p = 389$ and $p = 613$ were now found to be irregular. In addition, for $p = 491$, which was already known as irregular, a new index a was found, $a = 119$. These results were rechecked and found to be correct. It was discovered that out of the 302 prime numbers under 2,000, 118 were regular.

The second part of the procedure consisted in applying various known congruences involving Bernoulli numbers and Kummer-like criteria. These allowed checking the validity of the theorem for each of the irregular primes identified in the first part. The algorithm

devised for this second part was long and complicated, but it yielded a clear result for any given irregular prime exponent. What proved to be really stimulating for Vandiver and the Lehmers was the rather efficient way in which SWAC, with a proper codification of this algorithm, made this calculation: for the largest prime tested, SWAC had to run for only three minutes.

Vandiver also stressed how important these results were for the theory of cyclotomic fields. ''I do not think any specialist in algebraic numbers would have predicted,'' he wrote to the Lehmers, ''the outcome of the calculations.'' By this he meant, above all, the high percentage of regular primes under 2,000. Previously, since the irregulars were so dense under 600, Vandiver had assumed that ''the regular primes would fade out later.''[39] But now things looked different, and this had important consequences for the classification of cyclotomic fields. This problem seems to have been of less interest to the Lehmers, but gradually they became fully acquainted with it, to Vandiver's delight:

> I am surprised that the Lehmers seem to be sort of frightened at what they call the ''lore of cyclotomic fields.'' I recall that you were a bit flabbergasted at the apparent complexity of the formula that Kummer used as well as myself for testing the irregular primes; but when I started to explain it to you and began my discussion of possible simplifications, the Lehmers (d … n them) generally saw the tricks that I was introducing in advance of my explanations. …Yes, I am surprised. …
> Yours never …[40]

And Vandiver repeatedly discussed in his letters the exact manner in which this relevance of the results for cyclotomic fields should be properly stressed. A statement was finally published at the end of the article, in the following words:

> Irrespective of whether Fermat's Last Theorem is ever proved or disproved, the contents of the table given above constitute a permanent addition to our knowledge of cyclotomic fields, as its use will greatly simplify and facilitate the study of the units and ideals in such fields as defined for any $p < 2000$.[41]

An additional point frequently discussed in the correspondence concerned, as in their previous joint article, the expected venue of publication. The National Academy, Vandiver wrote to Emma:

> has a rule to the effect that any member presenting a paper for publication in the Proceedings is entitled to have it published; and in the twenty years since I have been a member, anything I have presented by whatever author or authors has been published. However, there seems to be exceptions to all rules and maybe if they see the name Lehmer on the paper, they will raise a question.[42]

One wonders how seriously this remark was meant and exactly how one must read what it says about the professional status of Lehmer among mathematicians. The fact is that the article was indeed published in the Academy *Proceedings*, and only there. Contrary to what was often the case with works appearing in the *Proceedings*, this work was never republished in a mainstream, purely mathematical journal.

Vandiver and the Lehmers continued to work on extending their results. This involved difficulties at both the institutional and mathematical levels. First there was the problem of being granted computing time with the SWAC. As Emma wrote to Vandiver:

> Tonight they are continuing the irregular primes run beyond 2000. Just how far we will be able to go, or what will be done after we leave is hard to predict at the moment because the whole place is in a state of uncertainty. If the Institute [for Numerical Analysis] goes to UCLA, as is hoped at the moment, then doubtless research time will be available for such projects…. Meanwhile, in the next two weeks we might be able to knock off a few more primes. We figure it would take 40 SWAC hours to get up to $l=3000$, and at $l=4000$ it would take an hour to examine each prime for regularity, so that there is not much hope for going beyond 5000 even with a formal arrangement to pay for the computing.[43]

Indeed, the Institute of Numerical Analysis devoted only a marginal amount of its efforts to problems in number theory, and the influential presence of the Lehmers since 1950 changed this situation only slightly,[44] but computation time was eventually granted for this undertaking, and it was pursued mainly by John Selfridge, at the time a graduate student at UCLA.

The mathematical difficulties were overcome by further refinements of the Kummer-like criteria. This was done partly by Vandiver himself, and partly based on independent work by the Finnish mathematician Kustaa

Inkeri (1908–1997). The results of this effort were published in two consecutive papers (still only in the *Proceedings*), that covered exponents p, $2{,}000 < p < 2{,}520$ and $2{,}520 < p < 4{,}002$, respectively.[45] Beyond the satisfaction for having proved Fermat's last theorem for all these exponents, Vandiver continued to stress the importance of two other facts encountered along the way: the high percentage of regular primes still appearing in this range, and the fact that all ranks of irregularity found were smaller than 3.

Concluding remarks

The use of electronic computers did not become a mainstream approach in number theory, certainly not in the short run. Neither did research interest in Fermat's last theorem. Still, the kind of work initiated by Vandiver and his collaborators opened a new direction of research, which is still alive and well. Calculation techniques with digital computers were rigorously developed after 1951, but their use in mathematics in general and in particular for finding proofs for various questions related with number theory evolved in a very slow and hesitant manner. Within this trend, additional proofs along similar lines continued to appear up to exponents over one billion, and case I up to values much higher than that.[46] In fact, Wiles provided a completely general proof that approached the problem from a completely different perspective, and comprised no calculations for specific exponents. And yet, articles in the tradition opened by Vandiver continued to be published even after Wiles' proof.[47]

Vandiver, at any rate, was never really fond of the abstract approaches dominant in algebra and number theory during the 20th century. He believed calculations to be the essence of the discipline. In 1958, he published in the National Academy *Proceedings* an article devoted to this issue. The venue of publication, it must be stressed, was an unlikely one for this kind of nontechnical article. Vandiver's opinion about computers in number theory was summarized as follows:

> Any investigation in the theory of numbers is likely to be experimental, at least in its initial stages. The number theorist may study special cases of results which he may conjecture to be true. … [H]e naturally likes to be able to use a rapid digital computing machines, or other means, to extend his computations. However, before the invention of any such machines, Euler, Gauss, Jacobi, Cauchy, and others of their time obtained some of the most important results we have concerning whole numbers. These men were expert computers and published papers containing extensive numerical data they had used in testing conjectures, which they were later able to prove or prove with modifications.[48]

Figure 5. Dick Lehmer in 1964. (Portrait courtesy of G. Paul Bishop Jr.)

The mathematical careers of Vandiver and of the Lehmers (see Figures 5 and 6) were self-styled in many senses and this is also manifest in their original efforts to harness electronic digital computers to problems in number theory. They were convinced of the importance of continued publication of tables, data, and calculations, and they spared no effort to doing this in their own fields of research and expertise.

Figure 6. Emma Lehmer, age 100. (Courtesy of Severo Ornstein.)

Web Extras

Visit the *Annals* Web site http://www.computer.org/portal/pages/annals/content/webextras.html for additional technical details on the work of Vandiver and the Lehmers, and on the theorem associated with Sophie Germain.

References and notes

1. Above all through the success of Simon Singh's best-seller *Fermat's Enigma* and its associated BBC TV program (produced in collaboration with John Lynch).
2. See L. Corry, ''El Teorema de Fermat y sus Historias'' [Fermat's Theorem and Its Histories], *Gaceta de la Real Sociedad Matemática Española*, vol. 9, no. 2, 2006, pp. 387-424 (in Spanish); L. Corry, ''Fermat Comes to America: Harry Schultz Vandiver and FLT (1914–1963),'' *Mathematical Intelligencer*, vol. 29, 2007, pp. 30-40.
3. For detailed explanations about the theorems and proofs mentioned in this and the next few paragraphs, as well as references to the original sources, see H.M. Edwards, *Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory*, Springer, 1977.
4. E.E. Kummer, ''Einige Satze über die aus den Wurzeln der Gleichung …'' [Some Theorems on the Roots of the Equation …], *Math. Abh. Akad. Wiss. Berlin*, 1857, pp. 41-74.
5. M. Ohm, ''Etwas über die Bernoulli'schen Zahlen'' [On the Bernoulli Numbers], *Journal für reine und angewandte Mathematik* [Journal for Pure and Applied Mathematics], (abbreviated hereafter as *J. für Math.*), vol. 20, 1840, pp. 11-12 (in German).
6. J.C. Adams, ''Table of the values of the first sixty-two numbers of Bernoulli,'' *J. für Math.*, vol. 85, 1878, pp. 269-272; S. Serebrenikoff, ''Novyi sposob vychisleniya chisel Bernulli'' [A New Method of Computation of Bernoulli Numbers], Zap. Akad. Nauk, Sankt Peterburg (Mémoires of the Imperial Academy of Sciences of St. Petersburg), vol. 19, no. 4, 1906, pp. 1-6 (in Russian).
7. K. Løchte Jensen, ''Om talteoretiske Egenskaber ved de Bernoulliske Tal'' [On Number Theoretical Properties of the Bernoulli Numbers], *Nyt Tidsskrift for Matematik*, vol. 26, 1915, pp. 73-83 (in Danish).
8. H.S. Vandiver and G.E. Wahlin, *Algebraic Numbers—II. Report of the Committee on Algebraic Numbers*, National Research Council, 1928, p. 182.
9. D. Hilbert, *The Theory of Algebraic Number Fields*, Springer 1998, p. ix. The expression ''a minimum of blind calculations'' quoted earlier in this same context appears in H. Minkowski, ''Peter Gustav Lejeune Dirichlet und seine Bedeutung für die heutige Mathematik'' [Peter Gustav Lejeune Dirichlet and his Significance for Contemporary Mathematics], *Jahresbericht der Deutschen Mathematiker-Vereinigung*, vol. 14, 1905, pp. 149-163 (in German).
10. For a complete bibliography, see the chapter on FLT in vol. 2 of L.E. Dickson, *History of the Theory of Numbers*, Chelsea, 1919. Except for items explicitly listed later, works mentioned in this section are all reported in Dickson's book.
11. W. Meissner (1913), ''Über die Teilbarkeit von 2^{p-2} durch das Quadrat der Primzahl $p = 1093$'' [On the Divisibility of 2^{p-2} by the Square of the Number $p = 1093$], *Berlin-Brandenburgische Akademie der Wissenschaften. Berichte und Abhandlungen*, [Berlin-Brandenburg Academy of Sciences. Reports and Treatises], 1913, pp. 663-667 (in German).
12. N.G.W.H. Beeger, ''On the Congruence $2^{p-1} \equiv 1 \pmod{p^2}$ and Fermat's Last Theorem,'' *Messenger of Mathematics*, vol. 55, 1925, pp. 17-26.
13. For other uses of this machine, see M. Croarken, *Early Scientific Computing in Britain*, Clarendon Press, 1990, pp. 13-15.
14. N.G.W.H. Beeger, ''On the Congruence $2^{p-1} \equiv 1 \pmod{p^2}$ and Fermat's Last Theorem,'' *Nieuw Archief voor Wiskunde*, vol. 20, 1939, pp. 51-54.
15. ''Crelle's *Journal*'' is the *J. für Math.*, founded by August L. Crelle in 1826. H.S. Vandiver, ''Extensions of the Criteria of Wieferich and Mirimanoff in Connection with Fermat's Last Theorem,'' *J. für Math.*, vol. 144, 1914, pp. 314-318.
16. H.S. Vandiver, ''On Kummer's Memoir of 1857 Concerning Fermat's Last Theorem,'' *Proc. Nat'l Academy of Science (PNAS)*, vol. 6, 1920, pp. 266-269. For a detailed account of Vandiver's work on FLT, see Corry, ''Fermat Comes to America,'' 2007.
17. H.S. Vandiver, ''On Fermat's Last Theorem,'' *Trans. Am. Mathematical Soc. (AMS)*, vol. 31, 1929, pp. 613-642.
18. D.N. Lehmer, *List of Prime Numbers from 1 to 10,006,721*, Carnegie Institution of Washington, 1914.
19. The machine is described in D.H. Lehmer, ''A Photo-Electric Number-Sieve,'' *Am. Mathematics Monthly*, vol. 40, 1933, pp. 401-406.
20. J. Brillhart, ''John Derrick Henry Lehmer,'' *Acta Arithmetica*, vol. 62, 1992, pp. 207-213.
21. D. Lehmer to Vandiver, 9 Oct. 1934. The bulk of the correspondence between Vandiver and the Lehmers is kept in the Vandiver Collection, Archives of American Mathematics, Center for American History, The Univ. of Texas at Austin (hereafter cited as HSV). Interesting material is also found at the Emma and Dick Lehmer Archive,

Univ. of California, Berkeley (hereafter cited as EHL). Letters are quoted here by permission.
22. D.H. Lehmer, ''Lacunary Recurrence Formulas for the Numbers of Bernoulli and Euler,'' *Annals of Mathematics*, vol. 36, 1935, pp. 637-648.
23. D. Lehmer to Vandiver, 20 Nov. 1934, HSV.
24. Lehmer, ''Lacunary Recurrence Formulas,'' p. 637.
25. D.H. Lehmer, ''An Extension of the Table of Bernoulli Numbers,'' *Duke Mathematical J.*, vol. 2, 1936, pp. 460-464.
26. Dick Lehmer to Vandiver, 10 Feb. 1936, HSV.
27. See M. Campbell-Kelly et al., eds., *The History of Mathematical Tables. From Summer to Spreadsheets*, Princeton Univ. Press, 2003.
28. See A.N. Lowan, ''The Computational Laboratory of the National Bureau of Standards,'' *Scripta Mathematica*, vol. 15, 1949, pp. 33-63. Lehmer is not mentioned in a recent account of the history of the project: D.A. Grier, ''Table Making for the Relief of Labour,'' Campbell-Kelly et al., *Mathematical Tables*, pp. 265-292.
29. H.S. Vandiver, ''On Bernoulli Numbers and Fermat's Last Theorem,'' *Duke Mathematical J.*, vol. 3, 1937, pp. 569-584.
30. H.S. Vandiver, ''On Bernoulli Numbers and Fermat's Last Theorem (Second Paper),'' *Duke Mathematical J.*, vol. 5, 1939, pp. 418-427.
31. See H.D. Huskey, ''SWAC—Standards Western Automatic Computer,'' *IEEE Annals of the History of Computing*, vol. 19, no. 4, 1997, pp. 51-61.
32. G.W. Reitwiesner, ''An ENIAC Determination of π and *e* to more than 2000 Decimal Places,'' *Mathematical Tables and Other Aids to Computation*, vol. 4, 1950, pp. 11-15.
33. E. Lehmer, ''Number Theory on the SWAC,'' *Proc. Symp. Applied Mathematics*, vol. 6, AMS, 1956, pp. 103-108.
34. R. Robinson, ''Mersenne and Fermat Numbers,'' *Proc. AMS*, vol. 5, 1954, pp. 842-846, on p. 844.
35. E. Lehmer to Vandiver, 7 Mar. 1953, HSV.
36. Vandiver to E. Lehmer, 3 Apr. 1953, HSV.
37. See L. Corry, ''Number Crunching vs. Number Theory: Computers and FLT, from Kummer to SWAC, and beyond,'' *Archives for History of Exact Science* (forthcoming).
38. Lehmers to Vandiver, cable, 16 June 1953, EDL.
39. Vandiver to E. Lehmer, 22 Sept. 1953, HSV. It should be said that to this day no proof exists of the infiniteness of the regular primes, but there are good arguments to believe that this is the case. See C.L. Siegel, ''Zu zwei Bemerkungken Kummers'' [On Two Remarks of Kummer], *Gött. Nachr.*, 1964, pp. 51-62 (in German).
40. Vandiver to E. Lehmer, 5 Oct. 1953, HSV. Quoted verbatim.
41. H.S. Vandiver, D.H. Lehmer, and E. Lehmer, ''An Application of High-Speed Computing to Fermat's Last Theorem,'' *PNAS*, vol. 40, 1954, pp. 25-33, on p. 33.
42. Vandiver to E. Lehmer, 30 Oct. 1953, HSV.
43. E. Lehmer to Vandiver, 14 Aug. 1954, HSV.
44. See J. Todd, ''Numerical Analysis at the National Bureau of Standards,'' *SIAM Rev.*, vol. 17, 1975, pp. 361-370.
45. H.S. Vandiver, ''Examination of Methods of Attack on the Second Case of Fermat's Last Theorem,'' *PNAS*, vol. 40, 1954, pp. 732-735; H.S. Vandiver, J.L. Selfridge, and C.A. Nicol, ''Proof of Fermat's Last Theorem for All Prime Exponents Less Than 4002,'' *PNAS*, vol. 41, 1955, pp. 970-973.
46. See, for example, S.S. Wagstaff, ''The Irregular Primes to 125,000,'' *Mathematics of Computation*, vol. 32, 1978, pp. 583-591; J.P. Buhler, R.E. Crandall, and R.W. Sompolski, ''Irregular Primes to One Million,'' *Mathematics of Computation*, vol. 59, 1992, pp. 717-722.
47. J. Buhler et al., ''Irregular Primes and Cyclotomic Invariants to 12 Million,'' *J. Symbolic Computing*, vol. 31, 2001, pp. 89-96.
48. H.S. Vandiver, ''The Rapid Computing Machine as an Instrument in the Discovery of New Relations in the Theory of Numbers,'' *PNAS*, vol. 44, 1958, pp. 459-464.

Leo Corry is director of the Cohn Institute for History and Philosophy of Science and Ideas, Tel-Aviv University. He is editor of the journal *Science in Context*. He has published extensively on the history of mathematics and physics between 1850 and 1950, including the recent *David Hilbert and the Axiomatization of Physics (1898–1918): From 'Grundlagen der Geometrie' to 'Grundlagen der Physik'* (Kluwer Academic Publishers, 2004).

Readers may contact Leo Corry about this article at http://www.tau.ac.il/~corry.