Arch. Hist. Exact Sci. (2008) 62:393–455
DOI 10.1007/s00407-007-0018-2

Number crunching vs. number theory: computers and FLT, from Kummer to SWAC (1850–1960), and beyond

Leo Corry

Received: 24 February 2007 / Published online: 16 November 2007

Abstract The present article discusses the computational tools (both conceptual and material) used in various attempts to deal with individual cases of FLT, as well as the changing historical contexts in which these tools were developed and used, and affected research. It also explores the changing conceptions about the role of computations within the overall disciplinary picture of number theory, how they influenced research on the theorem, and the kinds of general insights thus achieved. After an overview of Kummer's contributions and its immediate influence, I present work that favored intensive computations of particular cases of FLT as a legitimate, fruitful, and worth-pursuing number-theoretical endeavor, and that were part of a coherent and active, but essentially low-profile tradition within nineteenth century number theory. This work was related to table making activity that was encouraged by institutions and individuals whose motivations came mainly from applied mathematics, astronomy, and engineering, and seldom from number theory proper. A main section of the article is devoted to the fruitful collaboration between Harry S. Vandiver and Emma and Dick Lehmer. I show how their early work led to the hesitant introduction of electronic computers for research related with FLT. Their joint work became a milestone for computer-assisted activity in number theory at large.

Communicated by J.J. Gray.

L. Corry (✉)
Cohn Institute for History and Philosophy of Science,
Tel Aviv University, Ramat Aviv 69978, Israel
e-mail: corry@post.tau.ac.il

Contents

1 Introduction

In 1976, the mathematician Samuel Wagstaff announced a proof that Fermat's Last Theorem (FLT) is true for any exponent smaller than 100,000 [Wagstaff 1976]. The state of the art on the problem at the time was described by Harold Edwards in the following terms:

> Since 1850, work on the theorem has centered on proving more and more inclusive sufficient conditions [for the validity of FLT]. In one sense the best known sufficient conditions are now very inclusive, and in another sense they are very disappointing. The sense in which they are inclusive is that *they include all primes less than 100,000*. The sense in which they are disappointing is that *no sufficient condition for Fermat's Last Theorem has ever been shown to include an infinite set of prime exponents*. Thus one is in the position of being able to prove Fermat's Last Theorem for virtually any prime within computational range, but one cannot rule out the possibility that the Theorem is false for all primes beyond some large bound. [Edwards 1977, v–vi. Emphasis in the original]

This description appears in the introduction to Edwards *'Genetic Introduction to Algebraic Number Theory*, which comprises an authoritative account of the historical development of central ideas that arouse in relation with FLT. At this time, Andrew Wiles' ground-breaking general proof of FLT was almost 20 years away and the path that eventually led to it—sensibly diverging from all what had previously been done around the problem—had only been initially elucidated around in the work of Yves Hellegouarch [Hellegouarch 1972]. Indeed, the possible link between FLT and the Taniyama-Shimura conjecture (the link that lies at the heart of Wiles' proof) was clearly elaborated by Gerhard Frey in the mid-1980s. In the wake of Wiles' general proof, previous attempts to approach FLT by gaining insights on the basis of intensive calculations on specific cases (such as Wagstaff's) appeared more definitely than in the past as an obsolete perspective from which to gain new insights on the problem. Consequently, some of these attempts were essentially forgotten in historical accounts of FLT that were published after Wiles' impressive achievement. A main aim of the

present article is to describe in some detail this central thread within the history of FLT, which is seldom accorded the kind of separate attention it deserves.

In analyzing the role of computations with specific cases as part of the history of FLT one is lead to several interesting considerations. For instance, the prime numbers "within computational range" for which FLT can or cannot be proved is a historically determined concept. Being this the case, it seems relevant to discuss the kind of computational tools (both conceptual and material) available at any given point in time and the changing historical contexts in which these tools developed, were used, and affected work on FLT. Likewise, the changing conceptions about the role of computations within the overall disciplinary picture of number theory influenced the ways in which specific cases of the theorem were pursued, and the kinds of general insights thus achieved. The aim of this article, then, is to present and analyze the changing historical contexts of various computational efforts related with FLT.

The present article is part of an attempt to gain a broad and balanced picture of this often told, but sometimes ill-documented story. It is meant to be complemented (with some overlapping) by three additional publications. In [Corry 2007], I have presented a portrait of Harry Schultz Vandiver (1882–1973), the only mathematician—prior to Wiles—to have devoted a considerable part of his professional life to a well-conceived research program aimed at proving FLT. An interesting and rather forgotten figure, Vandiver is mentioned marginally, if at all, in most of the existing historical accounts. I have tried to explain the historical context of his lifelong quest for proving FLT. Here I provide additional details about the kind of calculations he pursued as part of his quest. Among other things, Vandiver aided himself with electronic computers being one of the first mathematicians to do so for a problem of this kind in number theory. His incursion into this field was in collaboration with the young couple Emma (1906–2007) and Derrick Henry (Dick) Lehmer (1905–1991). The story of this unique collaboration is the topic of [Corry 2007a], in which special attention is paid to the broader question of the slow and hesitant incursion of computer-assisted methods into the mainstream of research in pure mathematics (and particularly number theory). Again, here I provide additional details about the technical aspects of their computations.

In [Corry (forthcoming)], I will discuss the various historical contexts within which certain mathematicians paid more or (typically) less attention to FLT. Against the background of the mythical status of FLT in the mathematical lore, which was only intensified after the dramatic *grand finale* provided Wiles' general proof and the many publications that followed it, I claim that 350 years of history of FLT have enormously been over-dramatized in most existing accounts. My own account is, in the first place, an attempt to temper this over-dramatization with a more balanced picture. Essentially, FLT was a theorem to which few mathematicians—and, above all, very few outstanding number theorists—dedicated *sustained* research efforts worthy of that name. The theorem always aroused curiosity but mainly of the passive kind. Before the last stage that culminated in the work of Wiles, it attracted relatively little serious research work throughout the years.

The first main focus of the present analysis is in the work of Ernst Edward Kummer (1810–1893). Kummer was both an avid computer and a theory builder, and his contributions to FLT touch on both aspects of his mathematical personality. For important historical reasons, however, it was the second aspect that gained prominence as part

of the legacy bestowed upon the following generations. Indeed, through the combined efforts of leading number-theorists like Richard Dedekind (1831–1916) and Leopold Kronecker (1823–1891), the full elaboration of the important insights contained in Kummer's theory of "ideal complex numbers" led to a complete redefinition of how factorization properties are to be investigated in higher arithmetic (and even to a redefinition of "integers" in the more general domains that were now investigated).

While developing the theory of algebraic number fields in the wake of Kummer's work on ideal complex numbers, Kronecker and Dedekind mutually complemented the theorems, proofs and techniques elaborated by each other. Nevertheless, they represented two rather different, and in some sense opposed, approaches to the essence of mathematical practice. Kronecker represented what may be called a more "algorithmic" approach, whereas Dedekind was the quintessential representative of the so-called "conceptual" approach. This is not intended to mean that Kronecker introduced no new, abstract and general concepts or that he derived no results from an adequate use of them. Nor do I mean to say that one finds no computations in Dedekind. Rather, the point is that Dedekind's perspective allowed for the indiscriminate use of infinite collections of numbers defined by general abstract properties, whereas Kronecker insisted on the need to prescribe the specific procedures needed to generate the elements of such collections and to determine whether or not two given elements were one and the same. Dedekind did not seek or require such procedures and Kronecker did not consider it legitimate to ignore them.

A decisive factor in transforming Dedekind's approach into the dominant one in algebraic number theory and related fields at the turn of the twentieth century and thereafter was the influential *Zahlbericht*, published in 1897 by David Hilbert (1862–1943). The *Zahlbericht* was initially commissioned by the Association of German Mathematicians as an up-to-date report on the state of the art in the discipline. Hilbert indeed summarized the work of his predecessors but also added many new results and sophisticate techniques and opened new avenues for research in various fields. These avenues were indeed pursued by many leading researchers in the decades to come. The choices made by Hilbert in preparing the *Zahlbericht* were strongly influenced by both Dedekind and Kronecker. Still, Hilbert allowed for a clear emphasis on the "conceptual" perspective embodied in the former's work, over the "algorithmic" one of the latter. Eventually this kind of emphasis spread to all of algebra, via the influential work of Emmy Noether (1882–1935), of pervasive impact in twentieth-century mathematics [Corry 2004, pp.129–136].

While seeking to prescribe avenues for future research Hilbert also influenced the way in which previous work in the discipline came to be seen. Like Gauss and Kummer before him, Hilbert stressed the primacy of the problem of higher reciprocity within number theory. Hilbert also suggested that Kummer's approach comprised more of a computational component that he now considered necessary or advisable. Hilbert thus wrote [Hilbert 1998, p. ix]:

> 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 applica-

> tion in the proof of the higher reciprocity laws. I have tried to avoid Kummer's elaborate computational machinery, so that here too Riemann's principle may be realised and the proof completed not by computations but purely by ideas.

Hermann Minkowski (1864–1909)—who was Hilbert's close friend and collaborator and no less prominent number-theorist than him—systematically promoted a similar perspective in his work. He spoke of "the other Dirichlet principle", embodying the view that in mathematics "problems should be solved through a minimum of blind computations and through a maximum of forethought" [Minkowski 1905].

Kummer did invest great efforts in computations with particular cases as a mean to gain new insights on the new kinds of number domains he was dealing with. Such calculations, as will be seen below, appear in his research on unique factorization in cyclotomic fields and with the theory of ideal complex numbers. One well-known consequence of his research was a result of 1857 that FLT is true for all prime exponents less than 100. Although extending this result beyond 100 involved no more than straightforward (if tedious) computations of new values of so-called Bernoulli numbers, very little work was devoted to such computations before the late 1920s. It is interesting to consider why and when additional computations were not pursued, in the first place, and then, eventually, when and why they were resumed.

Kummer's work has been discussed in detail in existing historical accounts, with special emphasis on the processes that led to the rise of algebraic number theory. In Sect. 2, I rely strongly on Edwards' work, but at the same time, in preparation for the subsequent sections, it lays the stress on the computational aspects of Kummer's work and cites some additional, relevant material. From here I move to the other sections that constitute the more specific contribution of this paper. Section 3 discusses the kind of works that favored intensive computations of particular cases of FLT, or of any other result, as a legitimate, fruitful and worth-pursing number-theoretical endeavor. These works were part of a coherent and active, but essentially low-profile tradition within nineteenth-cnetury number theory. In Sect. 7, I discuss the involvement of Vandiver and the Lehmers on this tradition in connection with FLT, while indicating how their work became a milestone for computer-assisted activity in number theory. Prior to that, Sects. 4 and 5 discuss progress made in FLT by intensive computations performed on specific exponents p and using various techniques and approaches. Section 6 describes the collaboration between Vandiver and the Lehmers and how this prepared the ground for their joint, unlikely introduction of electronic computers for work related with FLT.

In some places I slightly deviate from the notation or symbolisms used in the original texts, and adopt terms introduced somewhat later. This is done for the sake of uniformity and simplicity, and it should not create any significant historical distortion. Unless otherwise stated, translations from original texts are mine.

2 Background: FLT from Sophie Germain to Kummer (1825–1857)

As is well known, at the center of FLT stands the Diophantine equation

$$x^n + y^n = z^n. \tag{1}$$

Fermat conjectured sometime after 1630 that Eq. (1) has no non-trivial integer solutions when $p > 2$, and he also famously claimed to have a proof which the margins of the book were too narrow to contain. The history of FLT traces various attempts to provide a general proof, be that Fermat's putative, original one or any other valid one. The early chapters of this story comprise some initial results by Leonhard Euler (1707–1783) and the publication in 1798 of a treatise on number theory by Adrien Marie Legendre (1752–1833) that included proofs of FLT for exponents $n = 3$ and $n = 4$. The first great treatise on number theory, *Disquisitiones Arithmeticae*, was published in 1801 by Carl Friedrich Gauss (1777–1855). It introduced the theory of congruences as main tool for the discipline (and it did not deal with FLT at all).

Against this background, the first important result that needs to be mentioned in the present account is due to Sophie Germain (1776–1831), who taught herself number theory by studying in detail and with great enthusiasm the treatises of Legendre and Gauss. Notice that, as a direct consequence of the proof of FLT for $n = 4$, the conjecture is proved once it is proved for all odd prime exponents. Also, it is easily seen that, without loss of generality, one may assume that x, y, and z are relatively prime. Germain's line of attack on FLT divided the possible solutions to be investigated into two separate cases, namely:

Case I—there are no three positive integer numbers x, y, z that satisfy $x^n + y^n = z^n$, and such that no one of them is divisible by n.
Case II—there are no three positive integer numbers x, y, z that satisfy $x^n + y^n = z^n$, and such that one and only one of them is divisible by n.

This separation was to become standard in many of the important contributions to the problem thereafter. Germain's own important theorem can be formulated by considering the following congruence:[1]

$$\xi^p + \eta^p + \zeta^p \equiv 0 \pmod{l}, \tag{2}$$

The theorem thus states:

Theorem 1 *Case I of FLT is true for an exponent p, if there is an auxiliary odd prime l for which the following two conditions hold:*

(1.1) *if congruence (2) is true for three integers* ξ, η, ζ *then either* $\zeta \equiv 0$ *(mod l), or* $\eta \equiv 0$ *(mod l), or* $\zeta \equiv 0$ *(mod l)*
(1.2) $x^p \equiv p$ *(mod l) is impossible for any value of x*

Based on this result, Germain proved that case I holds whenever n and $2n + 1$ are both prime. She also proved additional conditions involving congruences among primes of various forms. Based on these results, she performed detailed calculations, generating among other things values of the auxiliary prime l. She was thus able to prove that case I of FLT is valid for all prime exponents p smaller than 197.[2]

[1] This formulation is close to Vandiver's and I adopt it here, for the sake of uniformity in notation throughout the article.

[2] Since only a part of Germain's work became public through Legendre's book, it was common until recently to attribute her only with the proof for $p < 100$, whereas Legendre was attributed with its exten-

Somewhat surprisingly case II turned out to be much more difficult than case I. Thus, for instance, only in 1825, case II was proved for $n = 5$ 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 $n = 7$. This latter case turned out to be especially difficult, and it was finally proved in 1839 by Gabriel Lamé (1795–1870).[3]

In 1847 a group of mathematicians gathered at the Paris Academy—including Lamé as well as Augustin Louis Cauchy (1789–1857) and Joseph Liouville (1809–1882)—were involved in one of the most interesting interchanges of ideas in the history of FLT. On March 1, Lamé presented his colleagues with what he thought to be a possible way to prove the general case. Lamé used an idea originally suggested to him by Liouville, which involved a factorization of a sum of integers into linear complex factors of a certain type, as follows:

$$x^n + y^n = (x + y)(x + \zeta y)(x + \zeta^2 y) \cdots (x + \zeta^{n-1} y). \tag{3}$$

Here n is an odd natural number, and ζ is a complex number called a primitive n-root of unity, namely, a number that satisfies the condition: $\zeta^n = 1$ and $\zeta \neq 1$, n being the smallest integer for which this condition holds. Starting from this factorization, Lamé would apply an argument based on the method of infinite descent in order to lead to a contradiction that would prove FLT.

There were from the beginning some doubts about the validity of Lamé's argument, and Liouville himself was among those who manifested such doubts. On May 24 Liouville read to his friends a letter sent from Germany by Kummer, who had also sent an article published in 1844 and that retrospectively invalidated Lamè's alleged proof. Kummer's article directly showed that the factorization in question was not unique, as tacitly assumed by Lamé. Kummer had been working for several years now on generalizing ideas of Gauss about sub-domains of the complex numbers with a behavior similar to that of the integers. Indeed, as part of his work on the problem of biquadratic reciprocity Gauss introduced a new kind of numbers, the so-called "Gaussian integers", namely, complex numbers of the form $a + ib$, where a, b are any two integers. Gauss realized the Gaussian integers behave, in many important respects, like standard integers (or "rational integers" as they became known starting with the work of Dedekind). In particular, he identified those numbers that play the role of prime numbers within this domain, and used them to prove a corresponding version of the fundamental theorem of arithmetic, namely, that every number in the domain has a unique representation as a product of the corresponding primes in the domain of Gaussian numbers.

sion for all values up to $p < 197$ (see, e.g., [Laubenbacher & Pengelley 1999, 185–193]). However, [Del Centina 2007] has now presented this differently. Being the most detailed account of Germain's work to date and, based on a careful analysis of many of her unpublished manuscripts, Del Centina convincingly shows that Germain actually proved case I of FLT for all values of to $p < 197$.

[3] For detailed explanations about the theorems and proofs mentioned in this paragraph as well as references to the original sources, see [Edwards 1977, 59–75].

Kummer generalized this idea by considering domains of numbers $a + \rho b$, similar to the Gaussian numbers but with ρ being either any primitive root of unity (like in the case of Lame's proof), or a root of a negative integer other than -1. The following example shows why unique factorization mail fail to hold in such domains:

$$(4 + \sqrt{-5}) \cdot (4 - \sqrt{-5}) = 3.7 = 21. \tag{4}$$

Of course, in this case it is first necessary to show that all the factors involved (3,7 $4+\sqrt{-5}$ and $4-\sqrt{-5}$) count as "prime" in this domain, and this was done by Kummer in the examples he considered. But once this is done, what we have obtained here are two different representations of 21 as products of two prime factors in the domain of numbers $a + b\sqrt{-5}$.

Kummer's important insight implied that the traditional identification (going back to Euclid) of the two properties, primality and indecomposability, had to be abandoned in the case of certain, more general domains of numbers. But at the same time Kummer also developed a theory of "ideal complex numbers" meant to restore a kind of unique prime factorization into these generalized domains. The ideal complex numbers are factors which do not themselves belong to the domain in which the factorization is being considered. Then, rather than exhibiting explicitly the factors of any given number in the domain, one focuses on the *properties* that such factors should have, as if they were actually given. Thus, for example, to any number m belonging to a given domain of generalized complex numbers Kummer ascribed a list of "ideal prime numbers" and proved that this list satisfies all the division properties expected from the list of ordinary prime factors of an integer. Every "ideal prime factor" g belonging to the list of m is said to be "contained" in m. Kummer also defined for a prime ideal factor the meaning of being contained in m "with multiplicity greater than 1." In these terms, the main property one expects from the prime factors to satisfy is that m divides n if and only if every prime factor contained in m is also contained in n with at least the same multiplicity [Kummer 1847, 322–323]. It is curious that Kummer, apparently realizing the novelty implied in his ideas, took the unusual step of explaining his ideas to fellow mathematicians—in one of the expositions of his theory—with the help of an analogy taken from the realm of chemistry. The composition of complex numbers—he said—can be visualized as the analogous of a chemical combination: while the prime factors correspond to the elements, the ideal prime numbers can be compared to hypothetical radicals that do not exist in themselves, but only in combinations [Kummer 1851, 447–448].

Kummer's main motivation in studying these domains of generalized complex numbers and in developing his new factorization theory was a long-standing effort to address questions related to higher reciprocity laws. Very much like Gauss before him, Kummer declared that the problem of higher reciprocity was the "central task and the pinnacle of achievement in number-theoretical research." He conducted important research in this field, following on the footsteps of Carl Gustav Jacobi (1804–1851). Kummer even adopted the notation originally used by Jacobi when dealing with reciprocity [Edwards 1977, 1977a]. Of particular interest in the context are the cyclotomic fields, obtained as extensions of the field of rational numbers by adjoining a primitive p-root of unity ζ_p (with p prime, $p > 2$). The pth cyclotomic field $Q(\zeta_p)$ comprises

all complex numbers $f(\zeta_p)$ of the form

$$f(\zeta_p) = r_0 + r_1\zeta_p + \cdots + r_{p-1}\zeta_p^{p-1} \tag{5}$$

where $r_0, r_1, \ldots, r_{p-2}$ are rational numbers. If $r_0, r_1, \ldots, r_{p-1}$ are all integers, we then speak of the cyclotomic integers for that field, and this is one possible generalization of the idea of the Gaussian integers.

Kummer saw the ideal complex numbers as a tool for actual computation in relation with these domains of numbers, and not just as a useful, general theoretical conceptual tool. Thus, he wrote:

> The decomposition into prime factors gives at the same time a perfect knowledge of the complex numbers that appear in the theory of the division of the circle and a simple method for calculating them. For, as we have seen, all reduces to the problem of finding a prime complex factor of the number p, which can be represented either as an integer complex, if it exists as such, or as a root of some degree of an existing complex number, if it is ideal. The investigation of these prime factors can be easily performed by means of indirect methods that arise naturally. It would not be too onerous, and it would be very useful, to build up a table of all actual and ideal prime factors of the prime numbers up to one thousand. This table will provide all the numbers necessary for the algebraic solution of the equation $x^p = 1$, for all primes p within those limits. [Kummer 1851, 453]

And indeed, already in his dissertation he had devoted intensive efforts to preparing such a table [Kummer 1844]. Indeed, Kummer's insights about the possible failure of unique factorization in cyclotomic fields came directly from his actual involvement with such computations. The lowest power for which unique factorization of cyclotomic integers fails is $p = 23$, and the example with which Kummer realized that this is the case required a certain amount of computations. It seems that Kummer initially checked the validity of unique factorization for $p = 5$ and $p = 7$, and then he moved directly to the case $p = 23$. At this point he did not know whether or not it holds for the cases $p = 11$, 13, 17 or 19 [Smith 1965, 95]. It also seems that failure of unique factorization for $p = 23$ was known to Eisenstein (who, like Kummer was also investigating higher reciprocity) some weeks earlier than to Kummer [Edwards 1975].

In his research of cyclotomic fields, Kummer introduced some additional, important concepts that are needed for our discussion below. Notice, first, that $\zeta_p, \zeta_p^2, \zeta_p^3, \ldots, \zeta_p^{p-1}$, are all different primitive p-roots of unity. The norm of a cyclotomic integer $f(\zeta_p)$, $Nf(\zeta_p)$, is defined as the product

$$Nf(\zeta_p) = f(\zeta_p) \cdot f(\zeta_p^2) \cdot f(\zeta_p^3) \cdot \cdots f(\zeta_p^{p-1}). \tag{6}$$

It is easy to prove that $Nf(\zeta_p)$ is itself a cyclotomic integer. If $Nf(\zeta_p) = 1$, then $f(\zeta_p)$ is called a unit. Additionally, Kummer associated to every field $Q(\zeta_p)$ a rational integer h_p, called the "class number" of $Q(\zeta_p)$, which in a way provides a "measure" of

the failure of unique factorization of integers in that domain. Kummer showed that this number can be expressed as a product of two integers h_1, h_2, that are obtained each through a somewhat complex expression (not given here explicitly). These integers are commonly known nowadays as the first and second factors of the class number. Kummer proved that a necessary, but not sufficient condition for h_2 to be divisible by p is that h_1 be divisible by p.

Like with many other numerical concepts he introduced, Kummer meticulously calculated many values of h_1 in order to better understand its properties. He published his results for all prime values of p, with $p \leq 97$. For $p = 3, 5, 7, 11, 13, 17, 19$, he obtained the value $h_1 = 1$. For $p = 97$ he obtained $h_1 = 411322823001 = 3457 \times 118982593$. He indicated that these values grow "extraordinarily fast" and conjectured that they would asymptotically converge to

$$h_{p1} = \frac{p^{(p+3)/4}}{2^{(p-3)/2} \cdot \pi^{(p-1)/2}}. \tag{7}$$

He promised to provide a proof for this later on [Kummer 1851, 473], but apparently he never published such a proof.[4]

A much more important insight arising from the computations associated with the class number and its two factors was that for $p \leq 97$ only three cases satisfy the property that p divides h_p. These are 37, 59, and 67. Kummer realized that prime numbers with this property will appear as singularities of general results that could be proved about cyclotomic fields, and that they would need to be treated separately. He thus suggested a new task for research: to find all prime numbers p for which the class number h_p is divisible by p. Such primes are known nowadays as irregular prime numbers (a notation I will continue to use hereafter, even though it does not appear until much later). It is rather curious, in my view, that in spite of all the effort devoted to investigating them and their properties, Kummer did not designate them with any special name.

The first step to deal with this task is to find a more directly operational criterion for identifying any given prime as regular or irregular. Here Kummer's computational abilities brought up the surprising, and now well-known connection between regular primes and the so-called "Bernoulli numbers". To define these numbers we consider the coefficients b_i in the expansion

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{b_n x^n}{n!}. \tag{8}$$

[4] The first known proof of an approximate value for this formula appears in [Ankeny & Chowla 1949]. A more recent result appears in [Murty & Petridis 2001].

The first few values of these coefficients b_i are:

$$
\begin{aligned}
b_0 &= 1 \\
b_1 &= -1/2 \\
b_2 &= 1/6 \\
b_3 &= 0 \\
b_4 &= -1/30 \\
b_5 &= 0 \\
b_6 &= 1/42 \\
b_7 &= 0 \\
b_8 &= -1/30
\end{aligned}
$$

It is easily seen that for all odd indexes n greater than 1, $b_n = 0$, and that for even indexes, the signs alternate. Usually the b_n's are themselves defined as the Bernoulli numbers, but in this article, since the work I discuss in greater detail is that of Vandiver, I will follow a simplifying convention adopted by him (and not only by him. See, e.g., [Davis 1935, 181]) to consider only even indexes, and to define $B_n = (-1)^{n-1} b_{2n}$. In these terms, the first few values of B_n are:

$$
\begin{aligned}
B_1 &= 1/6 \\
B_2 &= -1/30 \\
B_3 &= 1/42 \\
B_4 &= -1/30 \\
B_5 &= 5/66 \\
B_6 &= -691/273
\end{aligned}
$$

Thus stated, Kummer showed that a prime p is regular *iff* it does not divide the numerators of any of the Bernoulli numbers $B_0, B_2, \ldots, B_{(p-3)/2}$. Already in the lower cases one sees that $B_6 = -691/2730$, which shows directly that 691 is an irregular prime. The history of the computations associated with Bernoulli numbers are of direct relevance for our story here, and I will return to it below. At this point I will just mention that the values that Kummer most likely used in his own computations were those published in 1842 by Martin Ohm (1792–1872) [Ohm 1840]. Ohm had calculated values up to B_{31} and these appeared in Crelles' *Journal* so that they were surely known to Kummer at the time of his research.

Kummer invested great efforts in identifying regular and irregular primes with the help of computations related with Bernoulli numbers, and in investigating further properties of the primes and the class numbers of the respective cyclotomic fields. Initially, he used the values of B_n known at the time to investigate each prime number up to 43. The only irregular prime found in this range is 37, as it divides the numera-

tor of B_{16} (i.e., 7709321041217) [Kummer 1850]. In later investigations he extended his computations to show that the only non-regular primes under 164 are 37, 59, 67, 101, 103, 131, 149, and 157. After 164, the computations became prohibitively complex. Kummer's computations also showed that for $p = 157$, the class number h_p is divisible by 157^2 but not by 157^3 . For all the other irregular primes under 157, the class number was divisible by p only. Also $p = 157$ had the special property that it divides both the numerators of B_{31} and of B_{55}. This gives rise to the concept of "irregularity index" (not specifically used by Kummer), whose value in the case of 157 is 2.

With his theory of ideal complex numbers at hand, Kummer had conjectured in 1848 a very general law of reciprocity for higher congruences [Kummer 1850], but it was only in 1859 that gave a more or less general proof, albeit one which was not yet valid for certain primes [Kummer 1859].[5] All the while, however, Kummer was also aware of the relevance of his ideas to a possible proof of FLT. In his 1847 letter to Liouville Kummer stated, indeed, that the application of the theory of ideal complex numbers to the proof of FTL had occupied him for some time now. On the other hand, he clearly stated his opinion that FLT was "a curiosity in number theory, rather than a major item." That year he announced to Dirichlet a proof that FLT is valid for all regular primes [Kummer 1847a, 1850a]. The question thus remained open for irregular primes, and in the following years Kummer attempted to address this question as well.

In 1857 Kummer published a famous article that broke new ground both conceptually and in terms of specific computations [Kummer 1857]. Kummer introduced three criteria that, if satisfied by an exponent p, implied the validity of FLT for that exponent. I formulate here the criteria in terms that are more modern than those actually used by Kummer, as follows:

(K-1) h_1 is divisible by p but not by p^2.
(K-2) If $B_n \equiv 0 \pmod{p}$, $n < (p-1)/2$, then there exists an ideal (of the ring of integers) in $Q(\zeta_p)$ with respect to which the unit

$$E_n = \prod_{i=1}^{(p-3)/2} \varepsilon\left(\zeta_p^{r^i}\right)^{r-2in}$$

is not congruent to a pth power of an integer in $Q(\zeta_p)$.
[In this formula $\varepsilon\left(\zeta_p^{r^j}\right) = \left(\frac{(1-\zeta_p^{r^{i+1}})(1-\zeta_p^{-r^{i+1}})}{(1-\zeta_p^{r^i})(1-\zeta_p^{-r^i})}\right)^{1/2}$, and r is a primitive root of p.]
(K-3) The Bernoulli number B_n is not divisible by p^3.

Kummer proved that each of the cases smaller than 100, namely, 37, 59 and 67, satisfied these assumptions. He thus achieved the very impressive result that FLT is valid for all exponents under 100. We will see below that Vandiver showed in 1920 that Kummer's proof contained some relatively minor inaccuracies. Nevertheless, by all

[5] The published, fully consistent application of ideal factors to prove reciprocity laws appears in [Eisenstein 1850].

accounts this result and the techniques implied in it remained a major milestone in the history of FLT.

Kummer asserted that it would not be difficult, though perhaps somewhat tedious in cases of large Bernoulli numbers, to prove that these criteria hold for individual irregular primes. Criterion (K-1) is relatively easy to check, whereas criteria (K-2) and (K-3) required very intensive computations. Kummer assisted himself with some existing data appearing in a very important collection of mathematical tables published by Jacobi in 1839, the *Canon Arithmeticus*, and about which more is said below. But beyond that he did not show his computations nor explained the formula on which these computations were based. Higher values of Bernoulli numbers were calculated, he said, using special tricks, "that would be too long to explain here in detail". Still he stressed that his methods comprised either some self-checking mechanisms or computations in two different ways, so that "the correctness of the results can be guaranteed" [Kummer 1857, 74].

Apparently Kummer thought at first that there exist infinitely many regular primes, but he soon realized that proving this would not be easy. It is less clear what his estimation was about the irregular numbers and about the number of cases not covered by his general proof of 1847. Kummer most likely expected this number to be relatively small, and he may have even perhaps thought that there is some way to cover them all by arguments similar to those he used now in 1857.[6]

Given Kummer's willingness to undertake such extensive and detailed computations, and given his full domain of the theoretical aspects of the problem at hand, his results on FLT, on irregular primes, and on Bernoulli numbers, can be taken to indicate the material limit to which this approach could lead as a way to proving FLT by 1860. At the same time, with these results and methods at hand, a clearly defined avenue of research had been opened for a possible, continued investigation of FLT. In principle, at least, all that was needed now was to continue the search for irregular primes, and then separate proofs could be worked out for each of them, according to Kummer's criteria. In addition, Kummer's criteria could be refined and further elaborated, with a view to finding more efficient tests for the validity of FLT for given irregular exponents. Working out as many additional, specific cases as possible would in turn add new insights about the overall behavior of prime exponents in this context and perhaps suggest new ideas for general proofs of FLT. As it happened, however, this possible way was followed by very few number theorists—if at all—until Vandiver appeared on the scene. One reason for this was the difficulty of the calculations involved. Another reason was that FLT was not high on the agenda of most leading number theorists, starting from Kummer himself. This in itself should not necessarily imply that further investigations into the Bernoulli numbers or into regular and irregular primes would be pursued only at a very limited pace. And yet this actually turned out to be the case. Relatively few new Bernoulli numbers were computed in the decades to come and

[6] It should be pointed out that Cauchy and Liouville raised several objections concerning Kummer's use of the ideal prime factors in his first proof. [Kummer 1857] (submitted on June 1856) responded to all those objections. In this article, however, Kummer did not mention explicitly either the objections or the problems actually arising in his first proof. For a contemporary account (1860) of Kummer's proof see [Smith 1965, 134–137]. More recent accounts appear in [Edwards 1975, 225–231; 1977a.]

when they were, the motivation never came—before Vandiver and his collaborators—from number theoretical concerns (certainly not from attempts to deal with FLT). This situation was mainly a consequence of the limited role accorded in the second half of the nineteenth-century within number theory (at least by some of its most prominent practitioners) to specific computations with particular cases. In the following section I elaborate this important point, before taking again the thread of progress done on FLT by the turn of the twentieth century.

3 Number theory and number crunching (1860–1910)

As explained in the introduction, Kummer's ideas on ideal complex numbers led to seminal developments in number theory over the following few decades, especially in Germany. The other side of Kummer's mathematical personality, the willingness to undertake massive computations as a main tool in number theoretical research receded into the background, and yet it would be wrong to think that it was not continued at all. As a matter of fact, the story of the development of number theory in the second part of the nineteenth century is a rather complex one in this regard. On the one hand, there are the important achievements of long-standing impact such as embodied in the works of Dedekind and Kronecker, or such as those derived from the use of analytic approaches originally introduced in the work of Dirichlet. On the other hand, actual interest in the field on the side of broader audiences of mathematicians (and especially of prominent mathematicians) was definitely reduced for rather lengthy periods of time. It is well know, for instance, that Dedekind's theory of ideals was hardly read at the time of its publication, both in its German original and then in its French translation of 1876–1877 [Goldstein & Schappacher 2007, 68–70]. At the same time, actual research was being done in number theory during that period, but in directions different to those that would be become prominent in the early twentieth century. The field of number theoretical research in the second half of the nineteenth century can be described as being organized around several clusters of interest. These clusters grouped mathematicians, who shared common interests within number theory, used similar techniques and pursued similar objectives. They published in similar journals and quoted each other. As a rule, they represented self-contained communities that hardly intercommunicated with each other [Goldstein 1994; 2007a, 71–74].

Some of these clusters eventually turned into two main trends of number theoretical research at the turn of the century, e.g., the "algebraic" and the "analytic" ones. But during this period, the cluster where most of the actual activity in number theory (quantitatively considered) took place was a different one. This cluster focused on question directly connected with some of the basic topics discussed in Gauss's *Disquisitiones*, such as reciprocity, and cyclotomic and Diophantine equations. It explicitly avoided the use of techniques involving complex numbers and analysis. Contributors to this cluster included in a visible way not only mathematicians, but also engineers, high-school teachers and university professors from other disciplines. They came from various countries including places without well-developed research traditions in the field. Remarkably, very few Germans were among them. More than any other cluster or sub-discipline in number theory, works belonging to this cluster as a rule did not

involve highly sophisticate mathematical knowledge. Still, some of them comprised very ingenious and innovative ideas, appearing mostly in the work of the more prominent mathematicians that contributed here. The latter included James Joseph Sylvester (1814–1897), Angelo Gennochi (1817–1889), and Edouard Lucas (1842–1891). This cluster did not evolve into a full-fledged, school of mathematical research that trained students and was systematically taught. Incidentally, most research on FLT during this period can be easily associated with this cluster of activity in number theory, and indeed, even here it counted as a rather marginal trend in terms of attention devoted to it. Still, this cluster interests us in the present account not because of whatever direct contribution it may have yield in relation with FLT, but rather because of the broader issue of computation with specific cases as a focus of interest in number theory, that was part of it.[7]

Indeed, the fact that so little progress was made in relation with the apparently simple question of finding additional irregular primes, beyond those calculated by Kummer himself, is directly connected with the overall processes undergone by the discipline. One way to realize the rather reduced attention devoted to the question of irregular primes is by looking at the terminology associated with it, as it was not until quite late before the terms "regular" and "irregular" were introduced, and certainly before it was widely adopted, to denote the meaning that eventually became standard. As already mentioned, Kummer himself introduced no specific term to denote the primes that satisfied the condition "prime numbers p for which the class number h_p is divisible by p". Smith's famous *Report on the Theory of Numbers* of 1859–1866 speaks only of "exceptional primes" (for the irregulars [Smith 1965, 134]), a term that was still in use in a few research articles still at the beginning of the century [Mirimanoff 1904]. No specific term continues to be the case for systematic presentations of Kummer's work, and this is the case both for the best known of them [Bachmann 1910, 458–476] as well as for the more esoteric [Schoenbaum 1908]. Around 1910 there is a boom in publications on FLT, on the wake of the creation of the Wolfskehl prize. At this time we find an article that uses the term "irregular primes" in its title but not in its text [Hecke 1910], and somewhat later it gradually appears in more and more texts. It will still take several year before the term becomes standard, and this can be taken as a good indication of the little attention devoted to the questions in which these numbers play a central role, such as FLT.

A further indication is provided by actual results proved about irregular primes after Kummer. Kummer had initially assumed that in proving FLT for regular primes, he was proving it for an infinite number of cases. Nowadays, there are heuristic arguments to support such an assumption, but no definite proof of it.[8] In spite of the fact that some questions of this kind arise naturally when following the line of attack derived from Kummer, the fact is that not until 1915 someone devoted some systematic thought to it. This was done by an unknown student, the Danish Kaj Løchte Jensen (not to be mistaken for the better known Johan Ludvig Jensen (1859–1925)), whose teacher

[7] [Goldstein 1994; 2007a, 71–74] and [Goldstein & Schappacher 2007] analyze this topic in detail.

[8] Indeed, there is an estimate that about 61% of the primes should be regular. See [Siegel 1964], [Washington 1997, 63]

happened at the time to be looking at Bernoulli numbers. And Jensen proved a result about irregular primes, rather than about the regular ones.

As a matter of fact, very little is known about Jensen. Apparently he was a student of Niels Nielsen (1865–1931), a versatile mathematician who after 1904 became interested in Bernoulli numbers, and published a series of research articles and later on a textbook on the topic [Nielsen 1923]. Still as a student in 1915 Jensen published in a remote Danish journal a proof of the existence of infinitely many irregular primes of the form $4k + 3$ [Jensen 1915]. His proof was rather straightforward and did not require any special idea or technique that was not known to number theorists since the time of Kummer. Jensen asserted that the result he had proved was then commonly assumed. This may have indeed been the case, and this is in any case what Jensen heard from his teachers. Still I have found no written, direct evidence of discussions pertaining to the question at the time. At any rate, Jensen did connect it, but only in passing, with FLT. He wrote:

> That there exist infinitely many irregular primes has been conjectured for a long time but as far as I know it has not been proved. It is well known that it has a certain importance for the evaluation of Kummer's investigations of Fermat's last theorem.

Jensen's result remained unknown for several years even to mathematicians involved with the relevant kind of questions. Thus, for instance, it is not even mentioned in the authoritative *History of the Theory of Numbers*, published in 1919–1920 by Leonard Eugene Dickson (1874–1954). We find it for the first time in a follow-up of the *History* published several years later [Vandiver & Wahlin 1928, 182]. Vandiver published Jensen's argument in English for the first time only in 1954 [Vandiver 1954], and he stressed that by that time it was not yet well-known. One year earlier, Leonard Carlitz (1932–1977) proved a similar, but more general result without the limitation $4k + 3$ [Carlitz 1954].

But even if anyone would try to perform additional computations in order to identify new cases of regular or irregular primes and thus extend Kummer's results on FLT, a basic limitation still existed concerning the known values of Bernoulli numbers. And as Bernoulli numbers are related to broader contexts than just FLT, a look (even if partial) at mathematical activities related with calculating new values of B_n is very instructive about the place of computations within number theory.

Previous to its surprising application by Kummer in the context of regular primes and cyclotomic fields, Jacob Bernoulli was the first to call attention to the possible usefulness of the numbers B_n. His ideas on this matter were published posthumously in 1713 as part of the *Ars Conjectandi*. The question at stake was to find a general formula for power sums of the kind

$$S_n = 1^k + 2^k + 3^k + \cdots + n^k. \tag{9}$$

Bernoulli devised a recursive method involving the numbers b_n, with the help of which he calculated in "less than half of a quarter of an hour" the sum of the tenth powers of the first hundred numbers, obtaining the result 91 409 924 241 424 243 424 241 924 242 500. He stressed that his work showed "how useless was the work of Ismael

Bullialdus (1605–1694) spent on the compilation of his voluminous *Arithmetica Infinitorum* in which he did nothing more than compute with immense labor the sums of the first six powers, which is only a part of what we have accomplished in the space of a single page" [Bernoulli 1713, 90]. Bullialdus (or Boulliau) was a Frech astronomer whose book *Opus novum ad arithmeticam infinitorum* [Bullialdus 1862] had attempted to clarify Wallis' proto-calculus method involving sums of powers [Nellen 1994].

Bernoulli's formula can be rendered in more modern terms (here for the case of fourth powers) as follows:

$$1^4 + 2^4 + 3^4 + \cdots + n^4 = \frac{1}{5}\left(\binom{5}{0} b_0 n^5 + \binom{5}{1} b_1 n^4 + \binom{5}{2} b_2 n^3 + \binom{5}{3} b_3 n^2 + \binom{5}{4} b_4 n\right). \quad (10)$$

There are various recursion formulas that allow calculating coefficients b_i. For the sake of simplicity I will mention here only,

$$\sum_{j=0}^{m} \binom{m+1}{j} b_j = 0 \quad \text{or alternatively} \quad (b+1)^k = b_k, \quad (11)$$

where after expanding the polynomial, b^i is taken to mean b_i.

Leonhard Euler was the first to indicate the connection of Bernoulli numbers with the power expansion (8) above. He computed values of b_n up until $n = 30, b_{30} = 8615841276005/14322$, and used them for summations of certain slow converging series [Havil 2003, 81–85]. The next to calculate additional values was Ohm in 1842 and, as already indicated, Kummer used Ohm's results that comprised values up to B_{31}. Ohm stressed that the efforts to calculate such numbers were fully justified because of the many contexts in which they were used, but did not specify what context he had in mind. After Ohm, the next significant step taken in the computations related to these numbers came in 1878 with the publication of the following 31 values by John Coach Adams (1819–1892). Adams had calculated values of B_n several years prior to publication and at some point decided that the right place for them to appear would be in the same venue where Ohm had published earlier on [Adams 1878]. The bibliography of works devoted to the theoretical and computational aspects of the theory of numbers was already considerably lengthy by this time [Ely 1882] and at any rate, we are already speaking here about large numbers, as the numerator of B_{62} comprises 110 digits. Adams was followed by further computations by Sergey Serebrennikov [Serebrennikov 1907], who reached values up to B_{92}. Much later, in 1935, tables published by Harold T. Davis (1892–1974), were based on an improved algorithm he had devised on his own [Davis 1935]. All of these computations were pursued with the explicit aim of assisting astronomical research, rather than number theoretical one. This was also the case with more general results obtained throughout the years in order to improve the existing computational methods. The most important among the latter was the so-called von Staudt-Clausen theorem [von Staudt 1840; Clausen 1840], consistently used by all those who prepared the above mentioned

tables. It thus happened, as will be seen below, that some mathematicians who thereafter undertook number theoretical research where values of Bernoulli numbers were necessary (such as in the case of FLT), did so by establishing a kind of somewhat unusual professional contact with astronomers.

A more detailed account of how Bernoulli numbers were computed and used in various contexts is beyond the scope of the present article. But their example suggests the need to look more closely at an important part of mathematical practice that only recently started to attract the attention of historian of mathematics, namely the elaboration, dissemination and use of mathematical tables of various kinds [Campbell-Kelly et al (eds.) 2003]. In the case of mathematical tables related to number theory even less has been done. It is nevertheless clear that one cannot speak about the computational side of the discipline without devoting some attention to the peculiar role that table making has played in it. For considerations of space, I will do this only briefly here while directing the readers to existing secondary literature.

In the first place, I stress once again the importance of specific computations for Kummer and the efforts he devoted to this activity. He carefully tabulated much of his computations so that he could examine them carefully and try to ponder their significance [Edwards 2007]. Kummer himself never published these tables, but a table of primes in cyclotomic number fields that was written on the basis of Kummer's theory of ideal complex numbers was published in 1875 by a rather forgotten figure, Carl Gustav Reuschle (1812–1875) [Folkerts & Neumann (eds.) 2006]. Reuschle was a high-school teacher of mathematics, physics and geography at Stuttgart who corresponded with Kummer on mathematical topics after 1850. It is not clear to what extent his book of tables, *Tafeln complexer Primzahlen aus Wurzeln der Einheit gebildet* [Reuschle 1875] was used among number theorists, but it seems that at least Vandiver knew it and saw in it a valuable source for anyone involved in research in cyclotomic fields.[9]

Previous to Kummer we could also mention other prominent mathematicians for whom number-theoretical tables were an essential work-tool, remarkably so Gauss and Jacobi. For instance, Gauss's thorough inspection and computing of additional values for existing tables of logarithms and of prime numbers was essential in leading to his conjecture about the distribution of the latter [Tschinkel 2006]. Jacobi in turn considered tables of indices for prime numbers (i.e., the analog of tables of logarithms for the multiplication mod p of numbers not divisible by p). His *Canon Arithmeticus* [Jacobi 1893] contained—among other things—tables of such indices for primes less than 1,000. These indices were of direct use for Kummer in his own detailed computations related with the reciprocity law. They continued to be used until well into the twentieth century.[10]

What for prominent mathematicians like Gauss, Jacobi, and Kummer was a useful tool leading to inspired theoretical work was a main focus of activity for others, like the

[9] See below footnote 29.

[10] It is indeed remarkable that the book continued to be in use without changes and additions until quite late. [Brandt & Patz 1956] added tables for computations of sums and differences of indexes. Indexes of primes and powers of primes less than 2000 were added in [Andree 1962] with computations carried out with an IBM 650–653.

already mentioned Reuschle and Adams. Indeed, mathematical table-making received a renovated impetus in the second half of the nineteenth century with the introduction of novel mechanizing processes of various kinds. It is important to stress from the beginning, that mechanization involved not only improvements in the precision, speed and complexity of the computations themselves. Rather, there were other tasks related with table making that were sensibly improved, such as transcription, typesetting, proof reading, printing, binding and distribution. In this broader context, mechanization could be seen a possible tool to alleviate the main concern of table-makers throughout history, namely, the avoidance of error. It is remarkable, though, that at least in the early stages, there was no consensus that mechanization will solve the problem, possibly because of the various human interfaces mediating among the successive phases of the process. Indeed, as will be seen now, it was not before the mid-1930s that mechanized computation became the standard procedure for table making, but even at this time we find clear evidence that the concern for error avoidance continued to haunt those involved in this activity. This concern is nicely summarized in the introduction to a book of mathematical tables first published in 1935 and reprinted as late as 1963, a time when interest in tables definitely started to decline:

> In the publication of a work on mathematical tables the greatest struggle must be waged against error. One is particularly amazed at the many ingresses available to this incubus of the computer.[11] This is particularly true in a project which embraces the computation of so many diverse functions, computations which are being made simultaneously by different computers. First the basic formulas must be carefully prepared and auxiliary table computed and checked. After the tabular values have been found, these must be checked by some device independently of the one employed in the original calculation. Duplicate computation is resorted to only when other methods appear too laborious or impractical. ... Differencing, the best check, although a tedious process with available statistical machinery, is employed in most instances. Finally, after the tables have been completed and checked, they must be transferred to copy sheets for the printer and then proofread for the original notebooks. This latter is, perhaps, the most exacting task of all and may be the most fruitful source of errors unless it is warily undertaken. [Davis 1935, *xii–xiii*]

In the early history of attempts to mechanize table making a main figure was, of course, Charles Babbage (1792–1871). The central motivation came from his involvement with astronomy and the concern for possible errors found in existing tables. As Babbage's ideas on mechanized computation evolved, a much broader agenda developed and table making remained one of the underlying preoccupations behind the drive for mechanization though not always a central one [Swade 2003, 159]. And yet, the increased mechanization of table-making activities made more evident than ever their institutional dimensions, and more patent their separation from the kind of work with which most creative mathematicians wanted to see themselves identified. Evidently, a separation between "mathematicians" and "computers" was nothing new in

[11] Of course, "computer" means here a "human computer". See [Grier 2005].

itself. Leibniz in 1685 wrote that "it is unworthy of excellent men to loose hours like slaves in the labor of computations which could be done by any peasant with the aid of a machine" [Swade 2003, 150]. But the more this became an activity involving the coordinated interaction of groups of people working according to established rules, the sharper the separation became. The parallel intrinsic developments in number theory towards sweeping conceptual approaches such as promoted by Hilbert and Minkowski only added to this trend.

The need for new and more accurate tabulated values of special functions became increasingly pressing for astronomers, engineers and physicists by the last third of the nineteenth century. Several initiatives were undertaken in order to cope with these, and a significant part of the efforts were devoted to create infrastructures that would allow for routine work that would produce the tables and check the results. One of the most salient examples of institutionalizing table making in order to deal with such pressing needs came with the creation of the British Mathematical Tables Committee. The committee brought together leading mathematicians such as Arthur Cayley (1821–1895) and Henry J.S. Smith (1826–1883), with the two leading British mathematical physicists such as Sir William Thomson (1824–1907) and Sir George Stokes (1819–1903). But the main active force behind its activities was James W.L. Glaisher (1848–1928) [Croarken 2003], who had himself made important contributions to the theory of Bernoulli numbers [Forsyth 1929].

The activities of the Committee started with a broad survey and classification of existing tables, the results of which were published in 1893 as a catalogue that became a classic for years to come and has remained an authoritative bibliographical guide on the topic. To this catalogue, Cayley added two years later a similar one devoted only to existing tables in number theory. Glaisher then started to design the computational standards and to supervise the computations to be carried out in the forthcoming years by trained (human) computers. Corresponding to the main motivations behind the creation of the Committee, most were devoted to functions that were relevant to applied mathematical concerns, such as elliptic functions, Legendrian functions and Bessel functions. Computations related with the latter class of functions were conducted mainly by Alfred Lodge (1854–1937), who joined the Committee later on. He assisted himself with two volunteers, and in 1889 he was the first to use a machine to check the printed tables. This was the circular calculating machine, designed and patented by Joseph Edmondson in 1883 [Edmondson 1885].

But from very early on, the infrastructures and abilities of the Committee and its associated members and workers were also used for computations related with number theory. The first such undertaking related factor tables, a topic on which Glaisher also published a broad historical account [Glaisher 1878]. By 1873 such tables covered numbers up to three millions and then from six to nine millions. The Committee undertook filling the gap with the help of two hired computers and the results were published in three volumes in 1879, 1880 and 1883.

An additional number theoretic effort related with the activities of the Committee was conducted under the initiative of an interesting figure, Lt. Colonel Allan Joseph Cunningham (1842–1928). Born in Delhi, he was a military engineer who retired from the army in 1891 and devoted the rest of his life to computations related with the theory of numbers, particularly in relation to residues of powers, as well as quadratic and

higher reciprocity [Western 1928]. In 1895 he suggested to the Committee to publish a table of residues of powers of 2, which would be useful for testing divisibility, for factorizations, and for solving congruences to base 2. He had started calculating such tables by himself and now he asked for the support of the Committee. Support was indeed granted and the project was completed in 1899 [Cunningham 1899]. Additionally, he published other detailed number theoretical tables related with quadratic partitions (x and y satisfying $x^2 + dy^2 = p$, for various values of d) [Cunningham 1904], Haupt exponents (the smallest exponent e for which $b^e \equiv 1 \pmod{n}$, for given b and n) [Cunningham 1905], residue indices (values of n for given y in $y^n \equiv 1 \pmod{p}$), and successive primes [Cunningham & Woodall 1904].

Upon his death, Cunningham bequeathed a moderate legacy to the Committee to be used in the production of new number theory tables. The money was also used to purchase calculating machines for the committee's current activities and to publish, with a delay of more than thirty years, additional number theoretical tables (divisor and power tables) that had been prepared by Glaisher but had remained unpublished theretofore. All of this happened in a period when the secretary of the Committee was the dynamic Leslie John Comrie (1893–150). Comrie joined in 1915 the Nautical Almanac Office and by 1928 he had completely mechanized its processes for table making. He brought with him many technical, conceptual and organizational innovations to the Committee's activities. His unique approach to minimizing the incidence of errors in the tables comprised not only original and improved calculational techniques. It also signified a clear understanding of the typographical aspects of printing and the influence of the latter on human communication. Thus, he systematically introduced the use of figures with heads (e.g., for 6 and 8) and tails (e.g., for 3, 5 and 7) as opposed to equal height figures, and he also employed extra white spaces instead of lines to divide across lines and columns. The layouts of the tables were no doubt much more effective for the reader than any other ones available at the time [Croarken & Campbell-Kelly 2000, 50–52]. Below we will see this approach reflected in the work of the Lehmers.

Some of Cunningham's work was also published posthumously, by Alfred E. Western (1873–1961), another curious figure in this context. A Cambridge 7th Wrangler of 1895, Western spent most of his professional life working as a solicitor, but kept his active interest in mathematics alive. He published research, among others, on quadratic fields, on reciprocity laws, on primes of the form $n^2 + 1$, on expressing numbers as a sum of 4 or 5 cubes, and on Fermat and Mersenne numbers. But above all, he had a great interest in numerical computations [Miller 1963]. In this spirit, he undertook the responsibility for the publication of Cunningham's work, which culminated in his *Table of Indices and Primitive Roots* [Western & Miller 1968]. In 1943, Western announced that some interesting, unpublished manuscripts of Cunningham, housed in the library of University College, London, had been "destroyed by an enemy air raid."[12] Cunningham and Western will reappear below in my account of attempts to prove FLT.

Another mathematician enthusiastic about table making who is relevant to this story is Derrick Norman Lehmer (1867–1938). Lehmer was a professor of mathematics at

[12] See *Mathematical Tables and Other Aids to Computation* 1, 1943, 92–96.

Berkeley with a great interest in computations and aids to computations. It will suffice to mention here that in 1909 he published a *Factor table for the first ten millions* [Lehmer DN 1909] and in 1914 a *List of prime numbers from* 1 *to* 10006721 [Lehmer DN 1914]. Later on, in 1929 he also prepared *Factor Stencils* that gave a method of factorizing any number using cards with holes punched in them [Lehmer DN 1939]. He had very strong opinions on the experimental character of mathematical research, and accorded a central role to tables in general. In the introduction to one of his books he stated such views as follows:

> In spite of the contention of certain eminent scientists that mathematics is a science that has nothing to do with observation and experiment, the history of the Theory of Numbers has been chiefly made by those who followed methods closely allied to those of the student of the natural science. Gauss himself, the most successful investigator of the field, was an indefatigable computer, as may be seen by consulting the long list of table in his collected works. Jacobi was also a tireless maker of tables. It is hardly likely, indeed, that any theoem of importance in the Theory of Numbers was ever discovered which was not found in the first place by observation of listed results. [Lehmer DN 1914, *vi*]

Hardly other, contemporary number-theorist would stress this part of the work of Gauss and Jacobi as Lehmer did. But then, hardly other number theorist would be involved in constructing analog devices for specific tasks such as primality testing like Lehmer and his son, Derrick Henry (Dick), did for many years. Below I will return to Dick's important collaboration with Vandiver on FLT, but at this point it is relevant to conclude this section, by adding some brief comments about the slow adoption of mechanized computation in various fields of mathematics in the early twentieth century.

If we look at the development of the activities of the British Mathematical Tables Committee then we notice that, in spite of Babbage's initial impetus and their enthusiastic adoption in statistical and related contexts, the use of desktop calculating devices as a main tool for numerical calculation in mathematics was slower than one can imagine. Desk calculator machines such as the Brunsviga–Dupla, Nova Brunsviga, and the already mentioned Emerson, to name but a few, were available to scientists and engineers at the beginning of the century, but human computers that were well trained and efficient on using other aids, such as tables and slide rules, continued for a while to be central to these activities.

The Nautical Almanac Office, for instance, was one of the main institutions where large scale computations were performed. These computations were used for tasks such as navigation, ephemerides computations, statistics and astronomy. Up to 1926 they continued to be performed with the help of logarithmic tables. The people who did some of the more demanding computations were retired members of the staff, their methods worked well and they were familiar with their jobs. When desktop calculators first became available it did not seem convenient to make any changes. In the early 1900 the available machines were quite expensive in comparison with books of tables, and they were large and cumbersome to use. In addition, computations with them required natural rather than logarithmic values of the trigonometric, exponential and hyperbolic functions, which were the main tools used in places like the Nautical Office.

Since the time of Napier such computations had been done using logarithms and they were the standard. In 1918 at least five new such tables were produced. Only by the early 1930s desk machines had replaced 4- 5- 6- and 7-figure logarithms as the most common method of large scale computations by both individuals and organizations [Croarken 1990, 16–19].

As we will see now, much of the work done on FLT at the turn of the twentieth century and in the following decades was based on number theoretical tables of the kind just described. It is remarkable, however, that the main tools (conceptual, mechanical, institutional) needed for the creation, production and distribution of such tables were developed with very specific concerns in mind, all of them directly related with applied mathematics and all foreign to number theory itself. It seems evident that only concerns of this kind would have elicited the enormous human efforts and material resources necessary for the huge tasks at play here. Number theory benefitted from these developments only at a later stage, when some of the persons involved, for whom this field was an additional focus of interest, made a wise use of the infrastructure that had been created with a very different purpose in mind.

After this overview of computations, computers and tables in the period following Kummer's work, we can return now to the main thread of our story.

4 Progress on Case I (1898–1941)

Before Kummer's road was retaken in the work of Vandiver, as will be seen below, some further attempts were made to prove FLT for ever larger classes of specific exponents. In this context case I was and remained much easier to handle than case II. Thus, for instance, Germain's and Legendre's results for case I had been successively extended at the turn of the twentieth century. Edmond Maillet proved in 1897 that case I is valid for $p < 223$ [Maillet 1897]. Dimitry Mirimanoff (1861–1945) extended this in 1904 to $p < 257$. He did some intensive computations in order to achieve this result, but this was not a straightforward extension of what had been previously done. Rather he provided a new, useful criterion along the lines of Kummer's earlier work, as he proved that Eq. (1) is impossible in integer solutions when the numerator of at least one of four Bernoulli numbers $B_{\frac{(l-3)}{2}}$, $B_{\frac{(l-5)}{2}}$, $B_{\frac{(l-7)}{2}}$, $B_{\frac{(l-9)}{2}}$ is *not* divisible by p [Mirimanoff 1904]. In two articles of 1908, Dickson proved the validity of case I for every prime exponent $p < 7000$, except 6857 [Dickson 1908, 1908a, Dickson 1909]. Interestingly, Dickson's results make no use of Kummer's methods, but rather are directly built on refinements of Germain's original computations. His articles make an interesting reading since they feature an eclectic attempt to use every possible tool available in order to reach the highest possible exponent. Likewise, we see how Dickson calculates value after value, assisting himself with existing tables of various kinds. Jacobi's *Canon* was obviously a main tool which he used intensively, but also the assistance of Cunningham and of Mr. E.B. Escott is repeatedly mentioned in his articles.[13] For example, in one case his proof required verifying, with the help

[13] As a matter of fact, Dickson was the author of one of the volumes on number theoretical tables published with the funds provided by Cunningham's legacy. See [Dickson 1933].

of a certain lemma about numbers of the form 1 + 128*k, the primality of

$$E = 42116007041 = 1 + 128 * 329031305.$$

On completing the proof Dickson remarked that testing a similar number for values close to 400 millions would require fifteen minutes, and for 800 millions about 25 minutes [Dickson 1908a, 42]. The exponent $p = 6857$ required a considerable amount of additional computations, but Dickson did not "take the trouble" to do so, since this exponent was too close to 7000, a value up to which he had proved the validity of the theorem in case I for all other prime exponents.

Mirimanoff's result of 1904 led to a most important new direction that was opened in 1909 by Arthur Wieferich (1884–1954). Using Mirimanoff's article, Wieferich proved that if three integers x, y, z relatively prime to p actually did satisfy $x^p + y^p = z^p$, then the congruence $2^{p-1} \equiv 1 \pmod{p^2}$ holds [Wieferich 1909]. Mirimanoff then simplified Wieferich's somewhat involved argument and extended this result by proving that the same p would satisfy $3^{p-1} \equiv 1 \pmod{p^2}$. Mirimanoff pointed out that his result could be combined with Wieferich's to state that case I of FLT is impossible for exponents p, where p is a prime of the form $2^\alpha 3^\beta = \pm 1$ [Mirimanoff 1910].

For the sake of simplicity I use in what follows the notation

$$q(m) = \frac{m^{p-1} - 1}{p}, \tag{12}$$

and $W(m)$ to be the statement that, whenever $x^p + y^p = z^p$ is satisfied by three integers x, y, z relatively prime to p, then $q(m) \equiv 0 \pmod{p}$. In these terms, Wieferich proved $W(2)$ and Mirimanoff $W(3)$. $W(m)$ was proved for higher values of m in a series of later works: in 1914 Vandiver proved $W(5)$ [Vandiver 1914], and Georg Ferdinand Frobenius (1849–1917) proved $W(11)$ and $W(17)$. Frobenius also proved $W(m)$ for $m = 7, 13$, and for $m = 19$ whenever $p = 6n - 1$ [Frobenius 1914]. In 1917 Felix Pollaczek (1892–1981), then a student of Frobenius in Berlin proved $W(31)$ [Pollaczek 1917]. Later on, in 1931, Taro Morishima (1903–1969) used the methods of Frobenius to provide a new proof for $m = 31$, in a way that he claimed to have establish the validity of $W(m)$ (for all but a finite number of values) in case $m = 37, 41, 43$ [Morishima 1931]. In his doctoral dissertation at Cornell, Norman G. Gunderson raised objections to Morishima's proof and succeeded in correcting some of the existing mistakes [Gunderson 1948], but as late as 1988 problems with Morishima' calculations were still found [Granville & Monagan 1988, 331].

A more systematic approach to this line of attack was also introduced earlier on by Philip Furtwängler (1869–1940) who proved the following [Furtwängler 1912]:

Theorem 2 *If case I of FLT is satisfied by three integers x, y, z for a prime exponent p, then 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).*

These were all significant results since they helped calculate a lower bound for the value of integers for which Eq. (1) could be satisfied. Moreover, they did so only

by considering p, and irrespective of the values of x, y, z that may satisfy the equation. Thus for instance, Furtwängler's result led in 1913 to an interesting and very specific result achieved by Waldemar Meissner. Meissner combined Furtwängler's general theorem with recent results obtained by arduous computations with residues modulo prime number p [Meissner 1913]. He referred to a rather obscure, recent Russian textbook on number theory, written by a certain Ukranian mathematician, Dmitri Grawe (1863–1939), who was involved mainly in questions of applied mathematics and differential equations.[14] Grawe tabulated for all prime numbers $p < 1000$ the residues modulo p of the ratios $2^{p-1} - 1/p$, and stated his belief that it might be possible to prove that Wieferich's congruence never holds. "Had he continued to the next 1000", Meissner remarked, "he would have found that the prime number $p = 1093$ does satisfy the congruence. Indeed, this is the highest number under 2000 to satisfy the congruence." The next related result came only in 1925 when N.G.W.H. Beeger (1884–1965) proved that between 2000 and 14000, the only exponent p that satisfies the Wieferich congruence is 3511. It was readily showed, however, that neither 1093 nor 3511 satisfied the Mirimanoff congruence [Beeger 1925].

Beeger explained the method of his computations and of his checking and why his method "makes an error almost impossible". Moreover, he disclosed, unlike Meissner that he "constantly used W.J. Odhner's 'Bunsviga' calculating machine" [Beeger 1925, 18]. So, this is the first mechanical computer that we explicitly know of as being used for attaining a result directly related with FLT. Both Meissner and Beeger used the Cunningham tables of 1905 on Haupt exponents, containing, for all prime and prime powers $p^k < 10000$, those exponents t for which $2^t \equiv 1 \pmod{p^k}$. Beeger returned to this problem in 1939 and, using Dickson's result of 1908, he proved that case I of FLT is valid for exponents up to 16,000 [Beeger 1939].

Another interesting thread of computations was conducted, somewhat later, by J. Barkley Rosser (1931–1989). Rosser, a student of Alonzo Church, is mainly remembered for his contributions to logic and foundations. He also did some important research in analytic number theory and applied mathematics, being later involved in the Apollo project as well. His incursion into FLT in 1939–1940 is a rather unknown facet of his mathematical activity. What is peculiar in his approach is that he applied analytic methods to the above described situations and used these methods to allow further computations of specific values with the help of some mechanical or possibly electro-mechanical calculators. This he did as follows [Rosser 1939]: If p is a prime for which equation $x^p + y^p = z^p$ is satisfied by three integers x, y, z relatively prime to p, Rosser called p, an improper prime. Call now n an A_n number if it is divisible by no prime which is greater than the nth prime, p_n. Rosser showed that while $q(x) \equiv 0 \pmod{x}$ is satisfied at most by $(p-1)/2$ integers x, with $x < p^2/2$, (with $q(x)$ as defined in Eq. (12) above) every A_n number is a solution of $q(x) \equiv 0 \pmod{x}$, provided $W(m)$ has been established for all prime values up to p_n. Thus, if we define the function $\phi_n(x)$, to be the number of A_n numbers not greater than x, we can state

[14] Some information on Grawe appears in http://www.cultinfo.ru/fulltext/1/001/008/012/539.htm and http://kspu.kaluga.ru/mathematik/mat/name/grave.htm.

that

$$2\phi_n(p^2/2) \leq p - 1. \tag{13}$$

The basic idea of Rosser's proof was to show that (13) cannot hold for small p's if the A_n numbers are sufficiently dense. Thus, using analytical methods, he found a lower bound for $\phi_n(x)$. He defined by recursion a sequence of polynomials $f_k(x)$, as follows

$$f_1(x) = \frac{x}{\log 2}, \quad f_{n+1}(x) = \frac{1}{\log p_{n+1}} \int_0^x f_n(y)\mathrm{d}y + \frac{1}{2} f_n(x). \tag{14}$$

He then proved by induction that

$$\text{if } x \geq 1, \quad \text{then } \phi_n(x) > f_{n+1}(log x). \tag{15}$$

Initially, Rosser used the available result of Morisihima for $p = 31$, which corresponds to p_{11}. Thus, he computed successively the values of $f_1(x)$, $f_2(x)$, ... and obtained an explicit expression for $f_{11}(x)$, as follows:

$$\begin{aligned} f_{11}(x) = {} & 0.00000005447197741x^{11} + 0.0000003295918757x^{10} \\ & +0.00008081950130x^9 + 0.001046349948x^8 + 0.007817038320x^7 \\ & +0.03463081936x^6 + 0.09016427288x^5 + 0.1322851609x^4 \\ & +0.1003412456x^3 + 0.03325580732x^2 + 0.00324407042x \end{aligned}$$

At the same time $f_{11}(x)$ could be computed following a different approach, namely,

$$\begin{aligned} f_n(x) = {} & \frac{1}{n!(\log 2)\Sigma_{n-1}} \left(x^n + \frac{n\Sigma_1}{2} x^{n-1} + \frac{n(n-1)\Sigma_2}{2^2} x^{n-2} \right. \\ & \left. + \cdots + \frac{n(n-1)\cdots(2)\Sigma_{n-1}}{2^{n-1}} x \right), \end{aligned} \tag{16}$$

where Σ_n denotes the elementary symmetric function of log 3, log 5, ... log p_n. A comparison of both values of $f_{11}(x)$ thus obtained provides a fair check of the computed values, and these values are calculated using some "ten place machine" (of a type not specified by Rosser), with the tenth place being rounded off. Rosser pointed out that errors in the tenth significant figure unavoidably occur in this case. However, the largest discrepancy which occurred between the two computed values of $f_{11}(x)$ was five units in the tenth significant figure, which indicated that the results were reliable.

The proof was completed by a combined application of straightforward (if involved) computations with integers methods such as applied by Meissner and Beeger, on the one hand, and analytical considerations concerning $f_{11}(\log(x^2/2))$ and its derivative, on the other hand. From the former, Rosser could deduced that if p is an improper

prime, then $2\phi_{11}(p^2/2) > 411{,}815.08$, and hence $p \geq 411,817$. From the analytical considerations, and using the fact that $p \leq 411.817$, Rosser further deduced that $p - 1 > 8{,}332{,}366.22$, from which, $p \geq 8{,}332{,}403$ (i.e., the next prime after that number).

Rosser presented his first paper in April 1939. Five moths later he presented a second one [Rosser 1940], where he extended the result of Morishima to $m = 37$ and 41. Interestingly, this was done by using a fact obtained in the earlier article, namely that if p is an improper prime, then $p > 8{,}000{,}000$. Then, with the values $m = 37$ and $m = 41$, applying the same analytical methods as before, Rosser deduced that an improper prime p is actually greater than 41,000,000. He also made the interesting observation that although it would seem certain that higher values for a lower bound of p can be found, "it seems unlikely that an indefinitely high lower bound can be so deduced." Thus for instance, it was clear to Rosser that there will be no difficulty to prove $W(43)$, even from the same value $p > 8{,}000{,}000$. Indeed, soon thereafter, Rosser did prove $W(43)$, in a third article, but he did so without using analytical methods [Rosser 1941].

The reason why Rosser thought the method to have inherent limitations was related to the use of two quantities, called the "eliminants", that had been central to all proofs of results mentioned above, starting from Dickson's 1908 article, and up until Rosser's own ones. The "eliminants" are two quantities, $x^{m-1} - 1$ and $(x+1)^{m-1} - 1$ that are used in various ways in proving congruences of the kind $q(m) \equiv 0 \pmod{p}$. Rosser used them here in his article for the cases $m = 37, m = 41$. Using considerations taken from Landau's analytical theory of the distribution of primes, Rosser established a suggestive connection between the order of size of the eliminants used in each case and the lower bound attained. This connection, Rosser asserted, is what made the method work. But it turned out that as larger and larger primes would be involved in the proof this specific connection could not be preserved, and hence the method would not work. More interestingly, Rosser raised a possible counter-argument that could be adduced against his own reasoning, namely, that what counts in his explanation is not the size of the eliminants involved, but rather the size of their largest prime factor (and this because of the way in which the eliminants enter the proof). The immediate answer to this counter-argument was that "after one passes the limits of factor tables, it becomes impracticable to deal with the factors of the eliminant rather than the eliminant" [Rosser 1941, 304]. In other words, the existence of improved methods of computation would perhaps allow the method suggested here, after all, to be used for higher values than Rosser estimated (and perhaps even unlimited values).

Rosser's result was soon extended by Emma and Derrick Henry Lehmer in 1941, for values of up to $p < 253{,}747{,}889$. The Lehmers referred in their article to a recent unpublished manuscript by Alfred Western that contained a further kind of related computations. Western had communicated his result to the Lehmers in private correspondence. He had called attention to the properties of A_n numbers, indicating that as a consequence of a theorem of Landau [Landau 1913], if $q(m) \equiv 0 \pmod{m}$ is valid for all values of m up to p_n, then case I of FLT is true for any exponent p which is the sum or difference of two A_n numbers. However, since all the numbers less that p_{n+1} are A_n numbers, it follows that case I of FLT is true for primes in a region where the A_n numbers are so dense that they do not differ by more than $2p_{n+1}$. Based on this

result – the Lehmers reported – Western had proved in 1938 that case I of FLT is true for $16{,}000 < p < 100{,}000$.

It is not clear from the Lehmers' text, whether or not Rosser was aware of Western's result when he developed his own proof using the idea of the density of the A_n numbers. He did not adopt Western's term, "A_n numbers", and he used the notation "F numbers" to denote integer solutions of $q(x) \equiv 0 \pmod{m}$, relative to a given p. He probably took this from a recent short article on FLT by a rather unknown mathematician from Breslau, Eugen Gottschalk [Gottschalk 1938]. Gottschalk also spoke of "N numbers", to designate those that do not satisfy $q(x) \equiv 0 \pmod{m}$ and are not divisible by p. He proved a series of results similar to those attributed by Lehmers to Western, and involving F and N numbers. Based on these results he proved the case $p = 6875$, that had not been covered by Dickson's proof of 1908, thus closing an existing lacuna that was seldom mentioned. Gottschalk believed that his method would allow proving infinite numbers of cases.

The Lehmers undertook to streamline Rosser's method and to find higher values of p for which case I of FLT is valid. Their idea was to separate the solutions of $q(x) \equiv 0 (\mathrm{mod}\, m)$ into classes that might be more easily scrutinized. Thus, for instance, by considering separately odd and even solutions and by using $\phi_n^*(x)$ to denote the number of $odd\, A_n$ numbers not greater than x, it is easily seen that

$$\phi_n(p^2/3) + \phi_n^*(p^2/3) \leq (p-1)/2. \tag{17}$$

The Lehmers stressed an important point that was not explicitly mentioned by Rosser, namely, that the use of analytical approaches for calculating lower bounds for the discrete functions involved here was necessary *because of the limitations of the existing tables*. Indeed, Cunningham's *Quadratic and Linear Tables* would not cover the cases beyond $n = 5$ [Cunningham 1927, 162–170]. Western, they added, had been recently preparing additional tables, but apparently these did not go much beyond Cunningham. The Lehmers' ability to improve on Rosser's result relied on their recent involvement with Bernoulli numbers. The context of this involvement was much broader than just the attempt to deal with FLT and it is described in some detail below. Here I will just mention how it extended Rosser's result for case I of FLT.

Based on their recent research, the Lehmers defined two kinds of polynomials P_n, Q_n of degree n that provide, respectively, a lower and an upper bound for $\phi_n(10^x)$, and yet another kind, P_{n-1}^*, of degree $n-1$, for a lower bound for $\phi_n^*(10^x)$. As Rosser had already proved $W(41)$, the index to work with now was $n = 13$. The Lehmers calculated the relevant (rather daunting) values of the coefficients of P_{13}, Q_{13}, P_{12}^*, some of which comprised up to twenty decimal digits. They used them for calculating the desired lower bounds of (13) and (17). Thus for instance, using:

$$P_{13}(\log p^2/2) \leq (p-1)/2, \tag{18}$$

and calculating with the explicit expression of the polynomial, one sees that the equation holds only for values $p \leq 93{,}785{,}629$. It follows that case I of FLT is valid for $p < 93{,}785{,}629$ (compared to Rosser's best value of 41,000,000). On the other hand, the equation

$$Q_{13}(\log p^2/2) \leq (p-1)/2, \tag{19}$$

holds only for $p > 141{,}000{,}000$ and hence, even if we knew the exact value of $\phi_n(x)$, for $n = 13$, we could not get a better result than this. Finally,

$$P_{13}(\log p^2/3) + P^*_{12}(\log p^2/3) \leq (p-1)/2, \tag{20}$$

holds only for $p > 102{,}108{,}200$. This establishes case I of FLT for exponents p up to that value. However, before the article was published, Rosser informed the Lehmers of his recent result for $W(43)$. Recalculating with the same techniques all the necessary polynomials and bounds for the case $n = 14$, the final result was achieved that case I of FLT is valid for $p < 253{,}747{,}889$. This was added in proof, on March 1, 1941 [Lehmer & Lehmer 1941].

The value computed by the Lehmers remained, for many years to come, the highest individual result of this kind. But parallel to this, some other results were obtained concerning case I, mainly by Vandiver. Vandiver's results arose from ideas developed in his attempts to deal with case II, as well as from directly extending previous results of Sophie Germain. Thus, using Furtwängler's (Theorem 2) and Germain's (Theorem 1) he proved in 1926 the following two theorems [Vandiver 1926]:

Theorem 3 *If there exists an odd prime p such that congruence* (2) *has no set of integral solutions, each not divisible by l, and such that l is not congruent to 1 module p^2, then Eq.* (1) *has no solutions, each prime to p.*

Theorem 4 *If congruence* (2) *has no set of integral solutions, each not divisible by l, where $l = 1 + mp$, and $m < 10p$, then Eq.* (1) *has no solutions, each prime to p.*

Then, in an important paper published in 1934, Vandiver summarized several results and techniques introduced in previous works by giving a concise formulation and a sketch of the proof of the following theorem:

Theorem 5 *If Eq.* (1) *is satisfied for p with x, y, z relative prime to p, then h_2 is divisible by p.*

He added an interesting comment to the effect that much of his "work concerning FLT is tending toward the possible conclusion that if the second factor of the class number" h_2 of $Q(\zeta_p)$ is prime to p, "then FLT is true" [Vandiver 1934, 122]. This is the so-called "Vandiver conjecture" about which he had begun to speculate much earlier.[15]

The survey of results presented in this section shows that the considerable progress achieved on case I of FLT between 1897 and 1934, whereby its validity was established for prime exponents up to p, $p < 253{,}747{,}889$, proceeded in a rather haphazard way, supported above all by intense calculations of many kinds. The increasingly higher

[15] The importance of this conjecture for algebraic number theory in general gradually gained recognition over the years, albeit in somewhat modified versions. See, for instance, [Iwasawa & Sims 1965]. [Lang 1978, 142] pointed out that the conjecture had originally been formulated by Kummer [Coll. Vol. 1, 85]. Lang indicated that "Vandiver never came out in print with the statement: "I conjecture etc. . . .", but "the terminology 'Vandiver conjecture' seemed appropriate to me. I any case I believe it".

values of exponents for which the result was proved to be valid were calculated on the basis of previous results, creating a complex network of interrelated but not clearly structured results, that was far from transparent and in which certain lacunae could easily pass unnoticed. Some degree of theoretical progress did accompany all these calculations, but it was of relatively limited impact.

5 Vandiver and Case II (1919–1932)

Whereas significant progress had been achieved for case I, as we have seen above, very little was done for case II which proved much more difficult to deal with. One isolated attempt, which however turned out to be unsuccessful, appeared in an article of 1910 by Felix Bernstein (1878–1956) [Bernstein 1910]. The very fact that Bernstein came to publish an article on FLT was no doubt related to the recent establishment of the Wolfskehl prize and the temporary boost it brought to attempted proofs. Indeed, he completed a *Habilitation* thesis under Hilbert on class field theory and published two short articles related to this [Bernstein 1903, 1904]. But thereafter, in his highly productive career, Bernstein published important works on set theory and on statistics and the only time he ever returned to number theory was in 1910, when he published this article. Bernstein's article was close to Hecke's already mentioned one and used its results. Like Hecke's it was very conceptual rather than computational. Bernstein first presented certain conditions related with p and with the second factor of h_p, h_2, that were formulated in terms of class fields and ideals, under which case I is valid. To this he then added certain, somewhat similar conditions for the validity of case II: case II is valid whenever h_p is divisible by p, but not by p^2, or, equivalently, whenever $Q(\zeta_p)$ contains no class whose p^2 power (but no lower power than that) is a principal class, and the second factor of h_p, h_2, is prime relative to p.

Bernstein's article produced no visible follow-up in the form of further attempts to prove FLT. The first to mention it later again was Vandiver, as part of his own incursion into case II – the only truly significant one to address this part of the problem ever since Kummer's 1857 article. After his 1914 proof of $W(5)$ Vandiver had proved some additional, relatively minor results related with FLT. Thus, for instance, in [Vandiver 1919] he provided a general argument from both Kummer criteria and Furtwängler's 1912 result could be derived. Much more important contributions came in 1920, when he identified some lacunae and accuracies in Kummer's arguments of 1857 [Vandiver 1920, 1920a]. Vandiver's painstaking review of each of Kummer's assumptions and derivations, as well as of Bernstein's more recent ones that depended on the former, indicated that existing proofs for the irregular primes under 100 were not valid.[16] As [Mirimanoff 1893] contained a separate proof of case $p = 37$, it turned out that at this point FLT was proved for all prime exponents p, $p < 100$, except for the two values 59 and 67. On the other hand, Vandiver's objections did not invalidate Kummer's proof for regular primes. Thus in the range of prime exponents p, $100 < p < 167$, the only cases not covered by the proof were 101, 103, 131, 149, and 157.

[16] Based on a different kind of consideration, also [Pollaczek 1924] showed that Bernstein's result did not imply the validity of FLT for 37, 59 and 67.

Over the following years, Vandiver worked on formulating a correct version of Kummer's argument, and on applying this modified version to obtaining further results related with FLT, both of general character and for specific cases of p. For example, in [Vandiver 1925] he developed a different kind of criterion for case I, namely, one based on properties of Euler numbers. He also proved [Vandiver 1925a] that if case I is true for p, then h_1 is divisible by p^8. But the really significant contributions, which implied a real breakthrough and led to considerable new advances for case II, appeared in a series of papers published beginning in 1926. Vandiver summarized his results in a detailed article published in 1929 in the *Transactions of the AMS* [Vandiver 1929]. For this article he was awarded the first Cole prize, established by the AMS in 1931 for outstanding work in number theory. The computational approach presented here deserves some detailed discussion.

As already said, for the irregular prime $p = 157$, the first factor of the class number of $Q(\zeta_p)$ is divisible by 157^2, and therefore (K-1) does not apply to this exponent. One of Vandiver's immediate tasks was to develop criteria that would yield a proof for this case. This he did by way of four different theorems, each of which implied separately that FLT is valid for $p = 157$. It turned out that that this validity can be further extended up to $p = 211$. In fact, even before the 1929 article appeared in print, Vandiver had realized that his arguments extended the validity of FLT to all exponents p, $p < 269$. Following Kummer, these four theorems used numbers x, y, z that are integers in the field defined by $(\zeta_p + \zeta_p^{-1})$ and which are prime to each other. An important result that Kummer had proved states that h_2 equals the class number of this field. Vandiver also added a fifth theorem that made explicit use of the somewhat restrictive fact that x, y, z are rational integers. He was fully conversant with recent progress in both number theory and abstract algebra, and he included in his work all the necessary results and techniques that were now available. In order to formulate the theorems, let p be any odd prime number and let B^p be the set of Bernoulli numbers $B_i, i = 1, \ldots, (p-3)/2$. Then the four theorems are as follows:

Theorem 6 *Case II of FLT is true for l, if the following two assumptions are satisfied:*

(6.1) *h_2 is prime relative to p,*
(6.2) *none of the Bernoulli numbers in the set B^p is divisible by p^3.*

The proof of this theorem is essentially an extension of Kummer's 1857 proof.

Theorem 7 *FLT is true for p, if the following two assumptions are satisfied:*

(7.1) *there is only one index n for which a Bernoulli number B_n in B^p is divisible by p,*
(7.2) *for that n and for p, the Bernoulli number B_{np} is not divisible by p^3.*

Also the proof of this theorem is essentially an extension of Kummer's 1857 proof.

Theorem 8 *FLT is true for p, if the following two assumptions are satisfied:*

(8.1) *$p \equiv 1$ (mod 4),*
(8.2) *all Bernoulli numbers in B^p which are divisible by p have even indexes.*

At variance with the previous ones, the proof of this theorem relied on more recent results, namely, a technique developed in [Mirimanoff 1893].

Theorem 9 *Case II of FLT is true for l, if the following assumption is satisfied:*

(9.1) *None of the units* $E_a, a = a_1, a_2, \ldots, a_s$, *is congruent (mod L) to the* pth *power of an integer in the field* $Q(\zeta_p)$.

Here we have: (i) L is a prime ideal divisor of l; (ii) l is a prime number, $l < (p^2 - p), l \equiv 1 \pmod{p}$; (iii) $a_1, a_2, \ldots a_s$ are the subscripts of the Bernoulli numbers in B^p which are divisible by p; (iv) E_a is defined as in (K - 2) above.

Theorem 10 *FLT is true for p, if the following two assumptions are satisfied:*

(10.1) *there exists a rational prime l, such that the congruence*

$$u^p + v^p + w^p \equiv 0 \,(mod\ l)$$

has no solution u, v, w, *all rational integers prime to l, and l is not congruent with 1 (mod* p^2*)*

(10.2) *the relation* $\left\{\frac{E_a}{L}\right\} \neq 1$ *holds, where a ranges over the values* $a_1, a_2, \ldots, a_s$, *these integers being the indexes of Bernoulli numbers in* B^p *which are divisible by p, and L is a prime ideal divisor of l.*

Here the expression $\left\{\frac{E_a}{L}\right\}$ denotes the pth power character as defined, for instance, in Hilbert's *Zahlbericht*, §113 [Hilbert 1998, 199]. Thus, condition (10.2) is closely related to condition (9.1) since, as Hilbert had shown, the relation $\left\{\frac{E_a}{L}\right\} \neq 1$ indicates that E_a is not congruent (mod L) to the pth power of an integer in the field $Q(\zeta_p)$ [Hilbert 1998, 200, Theorem 139].

This theorem was of particular importance for Vandiver since it was "apparently the first time criteria of this kind have been obtained for the second case of Fermat's last theorem" [Vandiver 1929, 637]. In his 1934 article, already mentioned above, Vandiver commented that it is not conclusive that any of the methods used so far absolutely depend on the fact that x, y, and z in Eq. (1) are rational integers. For example, the proof of theorem (Theorem 10) does rely on the fact that x, y, z are rational integers, but it is not shown that a similar argument does not work when x, y, z are interges in the field $Q(\zeta + \zeta^{-1})$. This point had apparently been raised in a conversation with Rudolf Fueter (1880–1950) a leading German number theorist and former student of Hilbert. "Perhaps FLT is true for rational integers – Vandiver concluded – but not for integers in $Q(\zeta + \zeta^{-1})$."

Because of (Theorem 5), and given that for h_2 to be divisible by p it is necessary that h_1 be divisible by p, it followed that (Theorem 6) was true for case I, so that it was necessary to prove only case II, which Vandiver did through a series of complicate lemmas of the kind that Kummer had used back in the 1850s (or of elaborations thereof).

Having these theorems at hand, the time came for computations. For this purpose, Vandiver also developed a series of formulae related with Bernoulli numbers that

became the basis for dealing separately with the various particular cases. Since all the irregular prime numbers under 157 (37, 59, 67, 101, 103, 131, 149) divided the numerator of only one Bernoulli number, B_n, in their respective relevant ranges, Vandiver used (Theorem 7) to prove the validity of FLT in those cases. This necessitated proving separately for each exponent p, that for the relevant n mentioned in the theorem, the Bernoulli number B_{np} is not divisible by p^3. In order to so, Vandiver introduced two auxiliary quantities, defined as follow:

If a is any integer, $1 < a < (p-1)/2$, and p is a prime integer > 5, then

$$B'_{ap} = \frac{(-1)^{a-1} B_{ap}(2^{2ap}-1)}{2ap}; \quad A_a = \frac{(-1)^a B_{ap}(2^{2ap}-1)}{2^{2ap} ap} \tag{21}$$

(Vandiver's A_a's should not be confused with Western's "A_n numbers" mentioned above).

The following two congruences can be now proved:

$$B'_{ap} \equiv 1^{2ap-1} + 3^{2ap-1} + 5^{2ap-1} + \cdots + (l-2)^{2ap-1} \pmod{p^2} \tag{22}$$

$$A_a \equiv 1^{2ap-1} + 2^{2ap-1} + \cdots + \left(\frac{p-1}{2}\right)^{2ap-1} \pmod{p^2} \tag{23}$$

In proving these formulae, Vandiver relied on well-known results, such as the von Staudt-Clausen Theorem, and added some shortcuts to make the computations with the B''s and A's easier. He stressed that these computations do not give as much information as Kummer obtained when he computed the actual values of h_1 for each value of p. Still, he regarded them as a sufficient check on Kummer's results [Vandiver 1929, 615–616].

The computations involved here were by all means long and tedious, and Vandiver relied on the help of colleagues and students among whom he distributed different ranges to be investigated. Thus, Mrs. A.C.S. Williams, a graduate student, checked all cases $p < 100$. This was important in order to check with and compare against Kummer's existing results. Thus for instance, for $p = 37$, she used $a = 16$, and found: $B'_{16\cdot 37} \equiv 42\cdot 37 \pmod{37^2}$. Kummer had previously calculated that $B_{16\cdot 37}/37 \equiv 35\cdot 37 \pmod{37^2}$. The current calculation thus agreed with the older one. In addition, she also obtained:

$$B'_{22\cdot 59} \equiv 59 \cdot 17 (\mathrm{mod}\ 59^2)$$
$$B'_{29\cdot 67} \equiv 67 \cdot 13 (\mathrm{mod}\ 67^2)$$

This later case, Vandiver stressed, implied that $B_{29\cdot 67} \equiv 67^2 \cdot 41 \pmod{67^2}$, where Kummer had written $B_{29\cdot 67} \equiv 67^2 \cdot 49 \pmod{67^3}$. Vandiver thus deduced that this had been a misprint.[17] Vandiver wrote that these results were obtained "directly", by which he probably meant that no machine was used.

[17] But incidentally Vandiver himself had a misprint here, as he wrote: $B'_{9\cdot 67} \equiv 67 \cdot 13 \pmod{67^2}$.

Samuel Wilks (1906–1964) was another graduate student whom Vandiver recruited to the work. Eventually, after completing his MA at Austin, Wilks went on to study mathematical statistics at Iowa and from there he continued to Princeton, where he became one of the leading statisticians of the country, and a leading mathematical educator [Mosteller 1964]. For Vandiver, he performed computations related with the A_a's in the cases $100 < p < 211$. This he did "using Monroe and Marchant electrical computing machines" [Vandiver 1929, 641]. His results included:

$$A_{34} \equiv 96 \cdot 101 (\mathrm{mod} 101^2)$$
$$A_{12} \equiv 10 \cdot 103 (\mathrm{mod} 103^2)$$
$$A_{11} \equiv 103 \cdot 131 (\mathrm{mod} 131^2)$$
$$A_{65} \equiv 133 \cdot 149 (\mathrm{mod} 133^2)$$

The case 157 was of course more important, as here $B_{31} \equiv B_{55} \equiv 0 \pmod{157}$. The computations for this case showed:
$A_{31} \equiv 39 \cdot 157 \pmod{157^2}$ and $A_{55} \equiv 156 \cdot 157 \pmod{157^2}$.

With these results at hand, Theorem II implied the validity of FLT for all cases $p < 211$, except 157. On the other hand, the only primes p for which the two conditions of Theorem III are satisfied simultaneously are 37 and 101. As for Theorem IV, Vandiver and his collaborators calculated $\left\{\frac{E_a}{L}\right\}$ for all relevant values of p and a. Thus for instance, for $p = 37$, the relevant values are $a = 16, l = 149, \zeta \equiv 17 \pmod{L}$. In order to test whether or not the symbol equals 1, Vandiver reduced $E_{16}(17)$ mod 149, and obtained the index modulo 149 by looking at tables of indices for all prime numbers less than 200, published in the second volume of Eugene Cahen's *Theorie de Nombres* [Cahen 1925, 38–54]. Vandiver reassured the readers that these tables had been checked independently by comparing their companion tables against each other.

The relevant computations for all irregular primes in this range (except 157) were performed by Elizabeth Stafford (1902–2002), who was just about to receive her PhD degree from Wisconsin. For instance, in the case $l = 37$, the said index, ind $E_{16}(17) \equiv 24 \pmod{137}$ and this agrees with Kummer's results of 1857. Only the case $p = 157$ was calculated by Vandiver himself. Here two cases arise $a = 31$ and $a = 55$. The relevant values are:
$a = 31, p = 1571, r = 139, \zeta \equiv 1024 (\mathrm{mod}\ P)$. Thus: ind $E_{31}(1024) \equiv 150 \pmod{157}$
$a = 55, p = 1571, r = 139, \zeta \equiv 1024 \pmod{P}$. Thus: ind $\mathrm{E}_{55}(1024) \equiv 39 \pmod{157}$

Vandiver also explained why these computations implied two results, namely:

- in all cases of irregular primes p considered here, h_2 is prime to p,
- Theorem 6 had been tested for all irregular primes.

He summarized all his results by stating that FLT is valid for all powers $n < 211$, and by announcing in a footnote that, after the article was submitted and before its publication, the upper bound had been raised to 269.

For details about many of the computations mentioned here, especially concerning Bernoulli numbers, Vandiver directed the readers to a joint article with Stafford

[Stafford & Vandiver 1930]. Here the discussion was oriented towards questions related with cyclotomic fields, but the computations involved were of course relevant to those needed for FLT. Vandiver and Stafford provided the following two definitions: A cyclotomic field is called irregular if $h_p \equiv 0 \pmod{p}$; it is called a properly irregular cyclotomic field if h_1 is divisible by p but h_2 is prime relative to p. They proved here that all irregular fields determined by primes $p < 211$ were also properly irregular.

It is particularly interesting to see at this point, how – somewhat like we saw above for case I – an increasingly complex network of reciprocal reliance across books and articles starts to be used as evidence for the validity of the results, and it is not always straightforward to determine what the actual source for the overall reliability of the final results is. Some kind of institutional authority had to be infused into the system in order to reassure the readers. Thus, for instance, like in Vandiver's article, also here use was made of Cahen's *Tables*, and to this information was added from Jacobi's *Canon*. But in addition, some further values that are not treated in those tables had to be calculated. Stafford "made all her computations", we are told, "in two different ways". Vandiver's computations for $p = 157$ were checked by "Mr. S.S. Wilks, tutor in mathematics, University of Texas". Vandiver himself went "through the computations concerning the second factor of the class number as a pattern of his work" on the case $p = 157$, and in doing so, he "checked again the computations of Kummer and Mrs. Stafford for $p = 37$". Stafford's computations were further supported by the fact that in the cases $p = 37, 59, 67$, they coincided with Kummer's. And, in addition to all of this, the authors promised that "the paper containing all the above-mentioned computations are now in the possession of Mr. Vandiver at the University of Texas; ultimately they will be deposited in some University library" [Stafford & Vandiver 1930, 149]. This implicitly offered the opportunity to check the results to every reader who might be potentially interested in doing so.

In subsequent papers, Vandiver continued to develop the main topics of his work on FLT, cyclotomic fields and Bernoulli numbers. In the first place, as already said, he extended the upper bound of his result on FLT to $p < 269$. In order to do so, he and his collaborators first found the irregular primes in this range: 233, 257, 263. Then, they found that for each of them only one Bernoulli number satisfies the divisibility test: $B_{42} \equiv 0 \pmod{233}$, $B_{82} \equiv 0 \pmod{257}$, and $B_{50} \equiv 0 \pmod{263}$. This was double-checked by using the values appearing in the Adams tables of 1878. These computations were performed by another graduate student, Elizabeth Badger, who included them in her MA thesis. The next step was to apply (Theorem 6) to the irregular primes. Another graduate student, J.A. Clack, found the following values: $A_{42} \equiv 26 \cdot 233 \pmod{233^2}$, $A_{18} \equiv 186 \cdot 257 \pmod{257^2}$, and $A_{50} \equiv 162 \cdot 263 \pmod{263^2}$. Vandiver did not say if the computations were machine-aided but, this result established the validity of FLT for exponents $p < 269$. Computations were already underway for extending the theorem up to $p < 300$ [Vandiver 1930].

Parallel to this, the results obtained in the joint paper with Stafford on cyclotomic fields were also extended with further computations [Vandiver 1930a]. The results were extended by Badger to primes $p, 210 < p < 269$, and by another graduate student, Mr. M.M. Abernathy, for primes $p, 268 < p < 307$. He found, first of all, that all primes in the range are regular except 271, 283 and 293. Then it was proved that the cyclotomic fields generated by all irregular primes between 210 and 307

were in fact properly irregular. All of this involved considerable amounts of computation, and Vandiver devised further methods to ease and speed up the procedures and also to allow for double-checking. Thus, for instance, he had proved that in a properly irregular cyclotomic field none of the units E_n are pth powers of units in $Q(\zeta_p)$. This result was used here for the exponents in question. Vandiver devised a method that allowed checking if E_n can possibly satisfy the said property for indexes n of Bernoulli numbers B_n that are divisible by p in each case. This was based on the use of Jacobi's tables for indexes of primes, and a rather complex table of relevant values was constructed for all the cases under investigation. Likewise, Vandiver devised a test for double-checking his results. Besides the already mentioned graduate students, also M.E. Tittle and Miss B. Bennett participated in the lengthy computations. Vandiver went on to use his results on irregular cyclotomic fields to extending his results on FLT. Thus, for instance, Clack calculated that $A_{10} \equiv 283 \cdot 71 \pmod{283^2}$. Using various computations of this kind, and the five theorems proved in 1929, Vandiver could prove all the cases involving irregular primes less than 307, and for some cases he even had more than one different proof (for $p = 149$, 257 and 293, he actually had four different proofs). He concluded by stating that FLT had been fully established for all exponents < 307. In these two articles of 1930, Vandiver did not mention any mechanical or electric machine used for his computations, but one may assume that at least something similar to what was used in 1929 was at play here. Additional relations involving Bernoulli numbers and irregular primes appeared in [Vandiver 1932].

6 The Lehmers, FLT and Bernoulli numbers (1939–1946)

The most important collaboration in which Vandiver was involved in relation with his research on FLT is that with the young couple Emma and Dick Lehmer. Elsewhere I have provided a broader background of the mathematical personalities of Vandiver and of the Lehmers, and discussed the interesting details of how their collaboration started and developed. Here I will only repeat as much as needed for the purposes of the present account, while directing the readers to [Corry 2007] and [Corry 2007a] for further details.

Vandiver's life-long quest to deal with FLT was not guided by an attempt to develop new concepts or overarching theories that would afford completely novel perspectives. Rather, he approached this problem as a meticulous technician who is willing to explore and exhaust the unexploited potential of existing theories, while refining them where necessary. As we have already seen, and will further see now, Vandiver was undaunted by even the most demanding computations, aiding himself with any available tools and persons. He was a poor lecturer and formally he only directed five doctoral students. At the same time, however, he had the ability to deeply engage in collaborative work and meaningful interchanges of ideas, as well as to activate groups of younger people willing to undertake heavy calculation projects under his direction. The previous section already mentioned examples of this, and now we will see some additional, and more important ones (including with the Lehmers).

Dick Lehmer was greatly influenced by the work of his father, Derrick Norman (DNL). Numerical tables and devices for automatic computations were always a topic of great interest for Dick, as they were for his father, and they occupied him for his entire life. Thus, for instance, as an undergraduate, he 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 DNL 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 the 1930s he devised the famous Lucas-Lehmer primality test for Mersenne numbers [Williams 1998, 180–201]. In 1932 he constructed a highly ingenious photoelectric number sieve [Lehmer DH 1933].

It was also through his father that Dick came to know his future wife and mathematical partner of a lifetime, Emma Trotskaia. This happened when she was an undergraduate student at Berkeley attending DNL's class. The couple married the year Emma graduated and moved to Brown University. In 1930 Dick completed there his Ph.D. under Jacob D. Tamarkin while Emma was awarded her M.Sc. Emma never completed a PhD or had a permanent teaching position, but this was only due to technical circumstances, such as the fact that university rules prevented at various places a husband and wife teaching in the same department. This fact, however, never prevented her from actively pursuing her mathematical interests both alone and in collaboration with Dick, and of being a leading member of the USA number theory community. Indeed she was completely satisfied with this institutional situation and was able to make the best of it, as she argued in a delightful essay called "On the advantages of not having a Ph.D." [Brillhart 1992].

The main focus of both Emma's and Dick's mathematical work was in number theory, and they approached it (separately and in collaboration) in a rather eclectic way, that included algebraic, analytic and computational methods. It was always some specific problem and the desire to crack it that stood at the focus of their attention. Conceptual and mechanical tools were always sought or developed as ancillary to such pursuits. As pioneers of the use of electronic computers (in particular, but not only, on number theory) they were keenly aware of basic question that a good programmer must face, such as a correct use of computational resources and streamlined coding. As part of their overall interest in computations related with number-theoretical problems, the Lehmers were well aware of current work on FLT, and in particular of the current work of Vandiver. I already mentioned the 1941 article where the couple extended the known results on case I of FLT up to $p < 253{,}747{,}889$. In fact, it was much earlier that they started to publish results related with the problem.

In 1932 Dick published a short note improving on a result of Vandiver [Lehmer DH 1932]. As mentioned above, Vandiver had proved in 1925 that if case I is true for p, then h_1 is divisble by p^8. This result had been recently improved in [Morishima 1932], who showed that p^8 can be replaced by p^{12} provided p does not divide 75571.20579903. Lehmer now proved that the proviso is actually not necessary, since $x^p + y^p + z^p = 0$ is not satisfied by the prime factors of $75571 \cdot 20579903$. This proof was within the thread—described above—that stemmed from Wieferich's work, rather than computations related with Kummer's criteria and irregular primes. But the Lehmers would soon move into this latter kind of work, following their interest in Bernoulli numbers and related topics.

The link between Vandiver and the young Lehmers came through the mediation of Derrick Norman Lehmer. Vandiver and DNL were part of the relatively small USA number theory community and were in a friendly relationship from the early 1920s. It was through his father that Vandiver contacted Dick and asked the couple to join him in his FLT project aroud 1932. Vandiver arranged for a scholarship of the American Philosophical Society that would pay for the rent of an electric Monroe machine for conducting the computations. It also paid partly for Dick's work, then at Lehigh, whereas Emma contributed large amounts of time and effort of her own. An immediate concern of Vandiver was the need for improved methods for calculating Bernoulli numbers. Dick and Emma were natural candidates for such a task, and they got quickly into work. In 1935, Dick published an article containing improved recurrence formulae for calculating Bernoulli and Euler numbers. Referring to previous tables such as those prepared by the "intrepid calculators", "Adams and Cerbrenikoff [sic]", Dick felt a distinct need to justify the calculation of further values, and his arguments are very telling about current attitudes of mainstream mathematicians to this kind of mathematical pursuit. He thus wrote [Lehmer DH 1935, 637]:

> The reader may question the utility of tabulating more than 93 Bernoulli numbers, and hence the need of giving formulas for extending their computations. 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 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.

Dick considered four classes of numbers that have important similarities and interrelations. These are the Bernoulli numbers (b), the Euler numbers (E), the Lucas numbers (R), and the Gennochi numbers (G). They may be defined, respectively, by the following four basic recurrence formulas:

$$\begin{array}{llll} b_0 = 1, & b_1 = -1/2, & (b+1)^n - b^n = 0 \ (n > 1) & \\ E_0 = 1, & E_1 = 0, & (E+1)^n + (E-1)^n = 0 & (n > 1) \\ R_0 = 1/2, & R_1 = 0, & (R+1)^n - (R-1)^n = 0 & (n > 1) \\ G_0 = 0, & G_1 = 1, & (G+1)^n + G^n = 0 \ (n > 1) & \end{array}$$

Here the expressions like $(b+1)^n$ should be read as operational symbols, which after expansion must be turned again into subscripts.[18] The known analytical expressions for the four kinds are also similar:

[18] In his paper Lehmer used the letter B rather than b, for the Bernoulli numbers, but for the sake of consistency with the rest of the article I will keep B here for its use as with Vandiver and with the Lehmers in their collaboration with Vandiver.

$$e^{bx} = \frac{x}{e^x - 1} \quad e^{Ex} = \frac{2e^x}{e^{2x} + 1},$$
$$e^{Rx} = \frac{2e^x}{e^{2x} - 1} \quad e^{Gx} = \frac{2x}{e^x + 1}.$$

The similarity between the four families of numbers is further enhanced by the fact that they vanish for odd values of the indexes, and the even-indexed values have alternating signs. Dick developed a "lacunary" kind of recurrence formulae that do not use all preceding numbers for the calculation of any individual one, but rather leave some gaps. b_n is computed from a set of previous b's whose indexes are congruent to n modulo m, where m represents the length of each gap. He showed how the recurrence formulae could be used for calculating these, and other kinds of numbers.

Typical of his very pragmatic approach, in applying these kinds of formulae, Dick was interested not only in the results they yield, but also in their algorithmic behavior and efficiency, ease of storage, communications and reproduction of results, etc. Such concerns are clearly reflected in an article written the following year where he applied his lacunary formulae to the methods for proving new cases of FLT [Lehmer DH 1936]. The most common ways to calculate Bernoulli numbers at the time were based in the recursive formula $(b+1)^n = b^n$. This was also the case even in recent tables, such as that published in 1935 by Davis. Lehmer called this a "fundamental though inefficient" algorithm. Other existing recurrence formulae were more efficient, but then the calculation of the coefficients soon increased in complexity. Dick suggested that a good compromise could be found in the use of Gennochi numbers, for which the following conversion formula was known:

$$G_n = 2(1 - 2^n)b_n. \tag{24}$$

Moreover, the following recurrence formula was available for calculating them:

$$4G_{2n} + 3\sum_{\lambda=1}^{[n/3]} \binom{2n}{6\lambda} G_{2n-6\lambda} = \begin{cases} 2n, & if\ n = 3k-1, \\ & otherwise. \end{cases} \tag{25}$$

Dick thus suggested an improvement of this formula that would be better suited for actual computations. In order to present this formula, one first defines

$$g(n,\lambda) = \binom{2n}{6\lambda} |G_{2n-6\lambda}|. \tag{26}$$

Thus, the recursion above becomes

$$100\,|G_{2n}| = 75\sum_{\lambda=1}^{[n/3]} (-1)^{\lambda-1} g(n,\lambda) + \begin{cases} 50n\cdot(-1)^n, & if\ n = 3k-1, \\ 100n\cdot(-1)^{n-1}, & otherwise. \end{cases} \tag{27}$$

For $\lambda > 0$, $g(n, \lambda)$ can be obtained as

$$g(n, \lambda) = g(n - 3, \lambda - 1).f(n, \lambda), \tag{28}$$

where

$$f(n, \lambda) = \frac{2n\,(2n-1)\ldots(2n-5)}{6\lambda\,(6\lambda-1)\ldots(6\lambda-5)}. \tag{29}$$

Now since $g(n, \lambda)$ is integer, the denominator of $f(n, \lambda)$ (in lowest terms) must divide $g(n - 3, \lambda - 1)$. This property provides a good way to check the computations for $g(n, \lambda)$.

The numbers G_n are quite large but they offer two important advantages for the computation of b_n:

- The G's are integers and therefore, no additional work in eliminating fractions is needed
- If we write $|b_{2n}| = N_n/D_n$ then $N_n = G_{2n}/d_n$, where d_n is the integer $2(4^n - 1)/D_n$.

In this way, N_n is obtained as the quotient of an exact long division. For $n = 100$, for instance, G_{220} has 313 digits, while d_{10} has 63 digits. This provides a good checking method.

Following this approach, Dick first checked all the results of Serebrennikov and Adams. Adams, as already stated, had calculated the first 62 non-zero values and Serebrennikov the first 92. Here he calculated all values up to B_{196}, which would be of course important for handling FLT for cases with higher exponents.

For the sake of clarity in presentation, Dick arranged and printed the numerators of the B numbers in a novel way, possibly under the influence of Comrie's style of typographic improvements. Previously, it had been customary to write these numerators as strings of digits in a long line, and here Lehmer suggested printing them in columns of 9 digits. Thus for instance, for B_{110} he got: $D_{110} = 7590$, whereas N_{110} he wrote as:

$$\left.\begin{array}{r} 8717064 \\ 809960074 \\ \vdots \\ 768306053 \end{array}\right] \quad 28 \text{ lines of } 9 \text{ digits each.}$$

Printing the results in this way, he stressed, will be very effective, especially "with standard computing machinery" [Lehmer DH 1936, 461].

The results attained by Dick Lehmer in these articles were immediately used by Vandiver–as will be seen right below–for achieving additional results on FLT, via calculation of irregular primes and application of his own extension of Kummer's criteria. But Dick published additional results on Bernoulli numbers that could be applied in different ways to FLT, as we saw above in relation with Rosser's papers. These results appeared in two papers of 1940–41. The Lehmers' improvement over Rosser was

based on the use of certain polynomials P_n, Q_n that provided lower and upper bounds for the function $\phi_n(x)$, and yet another kind, P^*_{n-1}, of degree $n-1$, for a lower bound for $\phi^*_n(x)$. These polynomials arise, also as lower and upper bounds, $P_n(\lambda)$ and $Q_n(\lambda)$, in the attempt to estimate the value of a function $N_n(\lambda) = N_n(\lambda|\omega_1, \omega_2, \ldots, \omega_n)$, representing the number of n-tuples of integers $(x_1, x_2, \ldots, x_n)$, that satisfy the equation $\omega_1 x_1 + \omega_2 x_2 + \cdots + \omega_n x_n \leq \lambda$. Such n-tuples constitute the lattice points inside, or on the boundary of, the n-dimensional tetrahedron bounded by the hyperplanes $x_1 = 0, x_2 = 0, \ldots, x_n = 0$, and the hyperplane $\omega_1 x_1 + \omega_2 x_2 + \cdots + x_n = \lambda$, where ω_i are positive real numbers and λ is a non-negative parameter [Lehmer DH 1940a]. Lehmer asserted that the best way to calculate these bounds was to obtain them recursively, as successive solutions of difference equations involving Bernoulli polynomials, namely expressions of the type:

$$b_\nu(x) = (b + x)^\nu = \sum_{k=0}^{\nu} \binom{\nu}{k} x^{\nu-k} b_k \tag{30}$$

where $(b+1)^\nu$ is taken to mean b_ν, so that $b_0(x) = 1, b_1(x) = x - 1/2$; $b_2 = x^2 - x + 1/6$. These Bernoulli polynomials have the convenient property that

$$b'_n(x) = n b_{n-1}(x). \tag{31}$$

An earlier article [Lehmer DH 1940] presented convenient estimates for maxima and minima of Bernoulli polynomials in the unit interval, $0 \leq x \leq 1$, and these were used here for calculating specific values of P_n, Q_n. In order to grasp the correct context in which all of these computations took place, however, it must be pointed out that one source of direct motivation for calculating these maxima and minima arose in a conversation of Lehmer with a seismologist, and Lehmer believed that they may also have important applications in statistics and interpolation theory. The need for such extreme values arises in connection with the equation

$$n \sum_{1 \leqslant \lambda \leqslant t} (t - \lambda)^{n-1} = b_n(t) - b_n(t - [t]), \tag{32}$$

in which $b_n(t)$ appears as approximating the sum on the right hand side up to an error that depends on the said extreme value. Lehmer expressed his surprise about the fact that the problem of maxima and minima had not been treated in the rather extensive, existing literature on Bernoulli numbers (including the recent tables by Davis).[19]

In addition, it is remarkable that while Lehmer would use the values of P_n, Q_n in order to improve on the computations of Rosser for case I of FLT, he in turn, in calculating the values of $N_n(\lambda)$ used the values of the functions f_n that Rosser had calculated in his previous article. Thus, the network of interconnected results on which the Lehmers' analytic estimation that case I of FLT up to $p < 253,747,889$ was based was a rather complex, and far from transparent one.

[19] For a comprehensive overview of the literature on Bernoulli numbers see http://www.mathstat.dal.ca/~dilcher/bernoulli.html.

The extant correspondence from this time contains many interesting information about the Lehmers' approach to the main problems involved in correctly implementing algorithms for automated computations. This was the kind of task in which their mathematical abilities were most clearly manifest. But the question that more recurrently comes up in the letters concerns the expected publication of their results: what exactly should be published and who would want to publish it? What tables? How many results for each case? The Lehmers clearly understood that coming up with new values of Bernoulli numbers was not the kind of result that the mainstream mathematical community would hold in highest professional esteem. In a letter of February 10, 1936, 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.

And indeed, the results of their collaboration were eventually published in the then new *Duke Mathematical Journal* as well as in the *Proceedings of the National Academy of Science* (*PNAS*), rather than in mainstream mathematical journals of the time. One is not surprised to see that in 1943 Lehmer was among the founders of the new journal, *Mathematical Tables and Other Aids to Computation*, originally published by the National Research Council. In 1960 the name of the journal was changed to *Mathematics of Computation* and it was only in 1962 that the AMS became associated with its publication. This process, together with the prominence that this journal eventually attained, attests for the deep transformation that affected some of basic mathematical values ingrained in the practice of number theory for generations, starting right after Kummer. Vandiver and the Lehmers played a significant, active role in bringing about this transformation.

The results of their joint work appeared in 1937 in an article entitled "On Bernoulli Numbers and Fermat's Last Theorem." Vandiver's name appeared as sole author, but the active collaboration of the Lehmers, as well as that of Abernathy and Tittle, was explicitly acknowledged. The article comprises first of all the identification of new values of irregular primes. Various sources were used for this purpose, including Jacobi's *Canon*, and the Lehmers' recent computations of B_n up to $n = 110$. Vandiver used algorithms that were a refinement of those used in 1919. Based on these, the Lehmers checked the validity of FLT for all irregular primes p below 601, and all primes p of the form, $p = 4n + 3, 601 \leq p < 619$. Vandiver stressed that arithmetical machines had not been used "except in connection with addition." He explained that tables of indices had been carefully constructed that allowed for identifying the smallest residue of any integer raised to a power modulo l. For any given integer n the tables were used to find what power λ is congruent to n modulo l, where λ is a primitive root of l for all primes l below 211. The tables were computed for each l selected in connection with each regular prime p. Vandiver further claimed that tables of indices for primes beyond 1000, if prepared in the future, would be very useful for many other questions in number theory. The values of l used in this connection were: 1187, 1229, 1543, 1579, 1627, 1637, 1699,1733,1867, 2083, 2309, 2767, 2803, 3209, 3343, 3643, 4211, 4549, 4943, 5231, 5471, 5557, 9739. Rather than publishing the tables

used, Vandiver indicated that they "will be ultimately deposited in the library of the American Mathematical Society" [Vandiver 1937, 583].

Using the data discussed in the article, it was shown that FLT is true for all prime exponents $p, 2 < p < 617$, except possibly for 587. As a matter of fact, FLT was proved for various other prime exponents below 700. The case 587 raised some computational difficulties which were nevertheless overcome very soon, while the result was extended to cover also the prime $p = 617$. This case was especially interesting, Vandiver pointed out, since 617 is the first instance of an irregular prime with irregularity index of 3 [Vandiver 1939]. By 1937, then FLT had been proved to be valid for all exponents less than 619. It was also clear by this time, however, that above 619 the computations became prohibitively long and laborious for being carried out with a desktop calculator.

In 1946, the editors of the *American Mathematical Monthly* asked Vandiver to prepare a detailed exposition of the state of the art in research on Fermat's problem [Vandiver 1946]. Vandiver was the acknowledged, world leading expert on the topic. FLT was a problem that many mathematicians were curious to hear about but, at the same time, very few were aware of recent progress in it. So both the problem and the author were natural choices. And indeed, the report is thorough, clearly written and authoritative, and it is small wonder that it remained a classical source of reference for decades to come. Vandiver's expository abilities came to full expression here, as he was able to present a rather systematic picture of a field of research that evolved in a rather haphazard way and actually retained that spirit.

One of the most interesting features of Vandiver's article is his current opinion about the possible, general validity of the conjecture, a question about which he was frequently asked. In this regard, Vandiver drew a clear distinction between the two classical cases. He was convinced of the validity of case I, but not merely because it had been proved for very high values. Rather, his confidence stemmed from some important, related theorems he had proved along the way on trinomial congruences and cyclotomic fields. Case II involved a much more complex situation; thus, while he believed it would ultimately be proven, he did not think he had any compelling evidence to support it. Indeed, it seems that Vandiver had been skeptical about the general validity of case II of FLT, as we realize from a letter written to him by Eric Temple Bell in 1929:

> If I remember rightly, you once said that you would not be surprised if the second case turn out to be false. . . . You give the limit five hundred for exponents to be tried. I have no idea of the actual amount of computation required for such an undertaking, but I should think it would be terrific. There is no doubt in my mind that anyone who knows anything about the Theory of Numbers would say that this work ought to be done while there is a man not only able to do it, but also willing. If in one of these exponents the computations should give a negative result, you will set a problem to exasperate generations of arithmeticians. I rather hope that it does turn out that way.[20]

[20] Bell to Vandiver: January 15, 1929. All letters cited in this article are kept in the Vandiver Collection, Archives of American Mathematics, Center for American History, The University of Texas at Austin. They are quoted with permission of the CAH.

By 1964 Vandiver had already surpassed the limit of five hundred and more was to come, but it was not the high values checked that could dispel his doubts. Also concerning the validity of the Vandiver conjecture, he felt now less sure than he was in 1934, precisely because of its close relationship with and possible dependence on the validity of FLT. Commenting on the frequency with which apparently promising conjectures in number theory are eventually abandoned, he wrote:

> When I visited Furtwängler in Vienna in 1928 he mentioned that he had conjectured the same thing before I had brought up any such topic with him. As he had probably more experience with algebraic numbers than any mathematician of his generation, I felt little more confident. (p. 576)

And, he added:

> However it would probably be best if I were wrong about this. I can think of nothing more interesting from the standpoint of the development of number theory, than to have it turn out the Fermat relation has solutions, for a finite number > 0, of primes l.

At this point in his career, Vandiver had already been investigating FLT for more than thirty years and, as already said, he was the world-leading expert on the question. He had well-formed opinions about the theorem and of what could be expected in terms of proofs for ever higher values of the exponent p. And yet, he could not imagine the completely new stage into which research on this, as well as on other number-theoretical questions, would enter in a few years from now with the advent of electronic digital computers. The then unimagined capabilities for fast-speed number crunching that these computers would provide was not really of much relevance to the kind of conceptual, structural research that had developed as a main trend in number theory under the influence of Dedekind and Hilbert. But for the kind of computation-intensive approach of which Vandiver was a main representative they would be of real interest, and would open a trend of research that started in a limited way and within a few decades became a most active a fruitful thread in number theory at large.

7 FLT and SWAC (1950–1960)

If Vandiver was a natural choice for writing an expository article on FLT for the *Monthly*, it turned out in retrospect that also the timing for its publication was perfect. The advent of electronic computers in the post-war era would also bring significant changes to work on FLT, so that in many senses 1946 was a good time for summarizing work done so far. On the other hand, the forthcoming changes would not bring about dramatic conceptual changes in the way it was approached. Rather, the changes would consist mainly in harnessing the enormous power of this new tool on behalf of an old approach. As we will see, the basic algorithms and calculation methods were refined but they were not superseded by completely innovative ones. Initially it was basically more of the same, though with truly powerful tools for making the computations.

Nor was it at all an obvious matter that the new tool would be indeed used for this particular problem, certainly not so soon. 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 in order 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 [Reitwiesner 1950]. The problem of Mersenne Primes, $M_n = 2^n - 1$, and the Riemann Conjecture also attracted attention from very early on. Alan Turing (1912-1954) addressed both problems at Manchester in 1951–1952. The Lehmers were of course natural candidates to pursue these kinds of problems with electronic computers. In 1952 they joined forces with Raphael Robinson (1911–1995), and found with the help of an electronic computer that M_{521} was prime. Soon, the additional results for M_{607}, M_{1279}, M_{2203}, and M_{2281}, were also achieved. Robinson was 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" [Robinson 1954, 844].

To a large extent, the fact that precious processing time of an electronic computer was devoted to FLT already in the early 1950s was the consequence of a series of fortuities. In 1945 Dick was invited to work at the ENIAC project at the Aberdeen Proving Ground. 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 for Emma and Dick in the use of electronic computers. Some years later, during the McCarthy era, Dick refused to take the loyalty oath, and he lost his position at Berkeley for a while. This did not become as acute a problem for him as it was for some others, since he became director of the Institute for Numerical Analysis (INA) at the National Bureau of Standards [Todd 1990]. In particular, Emma and Dick had here the opportunity to work with SWAC, the Standards Western Automatic Computer at the NBS. Particularly Emma, who was not officially employed at NBS, "had the good fortune to do quite a bit of the actual drudgery of coding and therefore enjoy the thrill of seeing the SWAC, so to speak, 'dance to my tune,' often after many false starts and blind alleys" [Lehmer E 1956]. Given their past collaboration on FTL, using now the power of SWAC to carry on with this work could be seen as a natural path to follow.

SWAC was one of the early stored program computers and the first to be built on the West Coast. In 1950, when it became active, it was the fastest computer in the world. It featured some of the most innovative technologies known at the time, such as the Williams tube memory, as well as an auxiliary magnetic drum memory of 256 words and a punched card I/O system. A main innovation of SWAC derived from the unique design of its command structure that considerably saved programs space and made program writing more concise. Also the magnetic drum memory was by that

time a well-known technology, but the way it was implemented in SWAC constituted an important innovation that brought it close to what is known nowadays as direct memory access. Its designer was Harry Huskey (1916–), who had previously worked with Alan Turing in England, and had been involved in previous computer projects in the USA, such as EDVAC and SEAC. SWAC was used primarily by the INA, but also by local aircraft companies. At the institutional level, SWAC demonstrated that a computer could be built by smaller establishments and with less intimidating amounts of money [Huskey 1997, Huskey et al 1997, Rutland 1995].

From the extant correspondence and testimonies one gets the clear impression that Emma was the driving force behind the use of SWAC for number-theoretic problems. Emma found that certain technical features of SWAC were especially well suited to this field of enquiry. SWAC worked with a word size that allowed for 36 binary (or 11 decimal) digits. The binary approach was found useful for expressing two-valued number-theoretical properties such as residuacy and primality. SWAC could perform 1,600 additions and 2,600 multiplications per second, which was way beyond anything that mathematician, even like the Lehmers, have ever come across or thought about. Given their prior experience, the Lehmers soon addressed the problem of how to program an all-purpose computer so as to turn it into a number sieve. They realized that they could process at the rate of 100,000 numbers per minute. The first number-theoretical problem they addressed was to find solutions for the Diophantine equation $x^3 + D = y^2$ for $-100 < D < 100$. They found no solutions for x less than one million [Lehmer DH 1953].

The idea of using SWAC for possible results connected with FTL was rather offhandedly suggested sometime during 1952. When news reached Vandiver of the success achieved with the Mersenne primes he hastily wrote to the Lehmers to congratulate them for the achievement:

> Wotinel do you and Dick mean by not wiring me as soon as you discovered those new Mersenne primes? ... Too bad the number theorists can't all get together and properly celebrate the Mersenne discoveries.[21]

Emma answered immediately suggesting that SWAC could be used for other number theoretical questions, but even these mathematicians that had devoted their efforts to FLT seemed not to think of this problem as a natural candidate for that. Thus Emma wrote:

> The Mersenne chase was exciting and is in fact still going on. Robinson coded it up to about $p = 2300$ and it has not quite reached the 2000 mark yet. They are running it off and on at odd times. The Robinsons [Raphael and Julia] came down and stayed with us between terms and we put in some long night vigils, but nothing new showed up after the first memorable night of Jan. 30^{th} . I am taking a class in coding now, so 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. The machine seems to be performing quite well lately.[22]

[21] Vandiver to Emma Lehmer: March 4, 1952.

[22] Emma Lehmer to Vandiver: March 7, 1952.

And Vandiver's answer about three months later does not leave room for interpretation. Vandiver simply did not think that it might be interesting to use SWAC for looking into FLT:

> Have you found any new Mersenne primes? At the moment no particularly numerical problem occurs to me that may be handled by the machine; but if one does, I'll let you know.[23]

The first extant letter in which we find FLT explicitly mentioned is on June 1st, 1953. Emma wrote to Vandiver the following:

> In connection with FLT we thought it may be fun to try finding some more irregular primes on the SWAC. We have just finished coding up a program for it. It looks like we should be able to do a prime of the order of 1000 in about 3 minutes. The question is where should we start? Would you feel happier if we went back to Kummer's 167 as the first try. That would probably take 5 or 10 sec. Have you gone beyond 607? Have you published a list of the irregular primes indicating which Bernoulli numbers they divide, and if so where? . . . How about coming out and watching SWAC knock out the irregulars. Let us know what you think of the project.[24]

And nine days later:

> We rather plan to run it first for all primes, except the obvious ones like 257 which will give too many exceptions. As soon as we get our things sent back to Berkeley next week we will move into a little beach house near here, where there will be practically no housekeeping for me to do, I will get busy and code up the more elaborate formula you mention in your letter using the drum, which has just been put into operation on the SWAC. This will be an interesting experience, as I have not tried to use the drum before and should give us plenty of room so that fairly large primes could be run, time permitting.
> Unfortunately due to the new administration's economy measures the Institute's budget has been curtailed very drastically so that all we can offer is some free time on the SWAC these days. Even that is hard to come by sometimes. We have hopes that after July 1*st* when several of the current problems are supposed to be finished we will be able to get in a few innings.[25]

From Emma's letter we learn that devoting machine time to a problem like FLT was not precisely a first priority, and that without the personal interest by the Lehmers and their friendship with Vandiver, no effort would have been devoted to this at the time. And as already indicated, even Vandiver did not think at the beginning of suggesting FLT as a possible project to undertake with the help of the Lehmers at SWAC. Now, in June 1953, it seems that he had already started to work out the improved algorithms

[23] Vandiver to Emma Lehmer: April 3, 1952.

[24] Emma Lehmer to Vandiver: June 1, 1953. Actually the year 1953 is not typed as part of the date in this letter, but there are several contextual matters that make it clear that this is the year of the letter.

[25] Emma Lehmer to Vandiver: June 10, 1953.

that would be used, and that are described below. On June 16, 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.[26]

Work was now under way, and it looked as a natural continuation of the earlier collaboration of 1935–40, only with a new and much more powerful technology at hand. The results of this joint research were published in 1954. Work was done in two parts: (a) identifying all the irregular primes < 2000; and (b) checking that each irregular prime thus found satisfies necessary criteria for ensuring that FLT is valid in that case. The criteria introduced by Vandiver in 1929, and that improved on Kummer's, were not easily turned into programmable algorithms. Thus, Vandiver was required to modify them accordingly, which he did very successfully.

The first step is to look at the set B^p of Bernoulli numbers B_i, $i = 1, \ldots, (p-3)/2$, and to find the indexes a_i of B_{ai} within that set that are divisible by p. In the case of regular primes, there are no such indexes. In the case of irregular primes, the existing criteria would be checked for those indexes. One way to find the indexes was to use any of several known congruences that allowed expressing Bernoulli numbers as sums of like powers. Vandiver himself had developed various such congruences in his previous work on FLT. Among these, the one involving the least number of terms is:

$$S_a = \sum_{p/6 < s < p/4} s^{2a-1} \equiv (-1)^a f_a B_a/4a, \pmod{p} \quad (p > 7,\ 2a < p-1) \tag{33}$$

where $f_a = (2^{p-2a} - 1)(3^{p-2a} - 2^{p-2a} - 1)$. This formula has the advantage that if for all a, S_a is not divisible by p, then p is regular. On the other hand, for some a's the factor f_a may itself be divisible by p and thus, the divisibility of B_a may sometimes remain doubtful and may require further checking. In these terms, the algorithm that SWAC was programmed to perform was the following:

(SW-1) Calculate $S_a \pmod{p}$ for $a = 1, 2, \ldots, (p-3)/2$. Write into punched cards all the values of p and a for which $S_a \equiv 0 \pmod{p}$. In addition, accumulate the value of

$$S = \sum_{a=1}^{(l-1)/2} S_a \pmod{p}. \tag{34}$$

This was used as a check before moving to the next step, since it should yield $S \equiv 0 \pmod{p}$.

(SW-2) If it turned out that S was not congruent with $0 \pmod{p}$, then SWAC would stop. (This never happened, however.)

[26] Lehmer to Vandiver (Cable), June 16, 1953. This document is found at the Emma & Dick Lehmer's Archive, UC Berkeley, and is quoted with permission.

(SW-3) With the relevant values of p and a, calculate $f_a \pmod p$. Write into a punched card all values for which the result was not divisible by p, together with an indication that p was irregular with index a.

(SW-4) For values for which $f_a \equiv 0 \pmod p$ it was necessary to further check to see if this was not a false alarm. This was done with the help of yet another known congruence:

$$S_a = \sum_{p/6 < s < p/5} s^{2a-1} + \sum_{p/3 < s < 2\,p/5} s^{2a-1} \equiv (-1)^a f'_a B_a/4a \pmod p \quad (p > 5,\ 2a < p-1). \tag{35}$$

where $f'_a = (6^{p-2a} - 5^{p-2a} - 2^{p-2a} + 1)$. We start with the case: f'_a is not divisible by p. In this case S'_a contains $[p/10]$ terms. Now, if S'_a is not divisible by p, neither is B_a, and thus this was actually a false alarm caused by the divisibility of f_a.

(SW-5) Now, if $S'_a \equiv 0 \pmod p$ (and still f'_a is not divisible by p), then p is irregular with index a, and this is recorded on a punched card as in step (SW-3).

(SW-6) If, however, $f'_a \equiv 0 \pmod p$, and since at the same time $f_a \equiv 0 \pmod p$, then it is not yet certain that B_a is divisible by p. In this case yet a third congruence is used, which dispels any remaining uncertainty but is much longer than the previous two, since it comprises $[p/2]$ terms:

$$S''_a = \sum_{r=1}^{(p-1)/2} (p-2r)^{2a} \equiv (-1)^{a-1} 2^{p-2a} l B_a \pmod{p^3}.^{27} \tag{36}$$

The actual congruence here is mod p^3 but it was considered sufficient to check mod p^2. For each case it was first checked if $S''_a \equiv 0 \pmod p$ and if it this was the case, then every time that $S''_a \equiv 0 \pmod{p^2}$ the card was punched indicating that p was irregular with index a.

At this point, SWAC had produced its output of punched cards indicating all irregular primes with their indexes or "degrees of irregularity". The largest index found was three. For values of $p < 619$ the results could be were checked against those obtained back in 1937 by Vandiver and the Lehmers. 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.

The second part of the procedure involved applying any of various existing criteria for checking that FLT is valid for each of the irregular primes identified in the first part. The criteria formulated by Vandiver in his earlier work were not easy to code as a program for SWAC. Thus, the need arose to formulate a modified version of (Theorem 9), as follows:

Theorem 11 *Case II of FLT is true for l, if the following assumption is satisfied:*

[27] This was based on an idea of Mirimanoff and then developed in [Stafford & Vandiver 1930].

(11.1) *None of the units* E_a, $a = a_1, a_2, \ldots, a_s$, *is congruent to the* pth *power of an integer in the field* $Q(\zeta_p)$ *mod* L.

Here we have: (i) L is a prime ideal divisor of l; (ii) l is a prime number, $l < (p^2 - p), l \equiv 1 \pmod{p}$; (iii) $a_1, a_2, \ldots a_s$ are the subscripts of the Bernoulli numbers in B^p which are divisible by p.

Some additional definitions were needed here. Let t be any integer such that t^k is not congruent with 1 (mod l), where l is a prime, $l = kp + 1, l < p^2 - p$. Let $\mu = (p-1)/2$. Let $d = 1^{p-2a} + 2^{p-2a} + \ldots + \mu^{p-2a}$. Define Q_a as follows:

$$Q_a = t^{-kd/2} \prod_{b=1}^{\mu} (t^{kb} - 1)^{b^{p-1-2a}}. \tag{37}$$

The following lemma holds: the unit E_a is congruent to the pth power of an integer in the field $Q(\zeta_p)$ modulo a prime ideal L that divides l, if and only if $Q_a^k \equiv 1 \pmod{l}$. Let Q_a be defined as above, and let $B_{a1}, B_{a2}, \ldots, B_{as}$, the list of Bernoulli numbers, with indexes less than $(p-1)/2$, which are divisible by p. Then, FLT is valid for p, if for $i = 1, 2, \ldots, s$, it is not the case that $Q_{ai}^k \equiv 1 \pmod{l}$. Let now p be an irregular prime with index a, as appearing in the output of the first part of the procedure. The following algorithm was programmed in SWAC in order to check if FLT is valid for p:

(SWI-1) Calculate the least prime l, of the form $kp + 1$.

(SWI-2) Find out whether $2^k \equiv 1 \pmod{l}$. If it is: find out whether $3^k \equiv 1 \pmod{l}$, etc., until a negative answer is found. The basis thus obtained will be used as the t in (37). As it happened, all cases checked give a negative answer for 2, so that in all cases $t = 2$ was used.

(SWI-3) Calculate d. This was done modulo p, without loss of generality. Calculate $2^{-kd/2} \pmod{l}$. Iteratively multiply this by each of the successive factors in (+), and, after each iteration, reduce the product mod l. This yields the value of $Q_a \pmod{l}$.

(SWI-4) Raise $Q_a \pmod{l}$ to the k-th power, and compare to 1.

It should be noticed that if the test had failed for a given value of l, it might yet be possible that it would succeed with a different l. The algorithm worked by trying first the smallest possible l, and it turned out that in all cases the test worked already with that l. Moreover, all these values of l satisfied the required condition $l < p^2 - p$. A recent article by the he Finnish mathematician Kusta Inkeri (1908–1997) [Inkeri 1947], however, showed that the criteria would still be valid if $l < \frac{3}{2}(p^2 - p)$.

The correspondence indicates that the summer of 1953 was the most intense period of activity in computing with SWAC, and on checking on the side of Vandiver and his collaborators. For instance, on August 3, Emma wrote to Vandiver:

> You will be glad to know that the drum is rolling over at a good clip. On the last 25 minutes it has shown that 1693 and 1697 are regular. We hope to be able to push this to 2000 while we are here. This will take 10 SWAC hours. Then run the Kummer criterion again and get a new listing to 2000 which we hope will agree with the old one to 1669. Meanwhile I think we will all feel better if you

> let your computer do $p = 389$, $2a = 200$ the SWAC way and check us step by step.[28]

In Vandiver's various letters we read about the progress of checking of all values sent to him. This he did with the help of various collaborators, an electric machine, and Jacobi's *Canon*. It seems that by the end of the month of August, most of the results were already essentially at hand. The new algorithms were indeed quite complicate, but they yield clear results when applied to the various new values of irregular primes found. The outcome was unambiguous and the double checking confirmed it: the criteria were satisfied by all irregular prime exponents under 2000 and thus FLT was valid for all exponents less than that value.

The distribution of regular and irregular primes between 1 and 2000 was indeed a very interesting and even surprising fact to ponder about. If the primes are grouped into sets of 250 the following table is obtained:

	1–250	251–500	501–750	751–1000	1001–1250	1251–1500	1501–1750	1751–2000	Total
No. of irregular primes	9	19	20	16	11	14	11	18	**118**
No. of primes	52	42	37	36	36	35	33	31	**302**
% of irregular primes	17	45	54	44	31	40	33	58	**39**

The high percentage of irregular primes within the primes under 2000 was rather surprising for Vandiver. While Jensen had proved in 1915 the infinity of the irregular primes, Vandiver did not find in this table a suggestion that there may be only a finite number of regular primes. This could be an important result ("a permanent addition") not only in this particular context but also in the theory of cyclotomic fields, where, as Vandiver explained, several theorems were known which do not appear to extend to irregular fields. The information provided by this table, he said, "will greatly simplify and facilitate the study of the units and ideals in such fields as defined for any $p < 2000$" [Vandiver, Lehmer & Lehmer 1954, 33].

As the overall picture started to consolidate, Vandiver was evidently in an upbeat mood and he wrote a long letter to the Lehmers that brought together many of the topics in which he alone, and the three together, had been working for years. The letter deserves being quoted *in extenso*. Vandiver thus wrote:

> In your letter of the 14th you say, "What is your feeling about publishing the SWAC output? Where, when, and how much, etc." . . . I hope that after a couple of years you will be able to announce that result that F.L.T. is true for all primes less than, say, 20,000 with possibly a few exceptions which will be doubtful. You will then have a mass of information not only about Fermat's Last Theorem but the theory of cyclotomic fields which will amount, in effect, to a considerable addition to Reuschle's book.[29] Your work with the SWAC so far increases greatly, in my opinion, the theory of properly irregular cyclotomic fields. On the other hand, if you find a case where $Q^K \equiv 1 \pmod{l}$ for a number of values of l

[28] Emma Lehmer to Vandiver: August 3, 1953. In this an other letters quoted I make slight notational changes so as to make them fit the text of the article.

[29] See above footnote 9.

(say for example 10), I would begin to suspect that the second factor of the class number is divisible by p in that case. Such a possible eventuality reminds me of a statement that Bell made in a letter to me dated 1929.[30] ... I am inclined to agree, based on my experience with it, that the problem of the divisibility of the second factor of the class number by p is just as difficult as Bell thinks. You will probably recall that we defined a properly irregular cyclotomic field defined by a pth root of unity as properly irregular if the first factor of its class number is divisible by p, but the second is not. So far, your work holds open the possibility that cyclcotomic fields are either regular (that is, defined by regular primes) or properly irregular. Maybe the dreams of Mirimanoff, Furtwängler and myself will come true! If there exists any improperly irregular cyclotomic field, we can at the present time say very little about the properties of its units and ideals (belonging to powers of p). On the other hand, the properties of the properly irregular cyclotomic fields are much simpler than what you might expect in advance, and I regard some of them as quite beautiful.[31]

And another letter that deserves being quoted at length was written exactly one month later. Vandiver makes patent and explicit his views about the primacy of question related to cyclotomic fields over those of FLT. Thus he wrote:

I should like to state in detail what I think of the significance of the work you have so far done on the SWAC concerning F.L.T. So fart in the work for exponents < 2000 several of the things that have stood out which I do not think any specialist in algebraic number theory would have predicted are: First, the persistence of the regular primes. If there is only a finite number of these, I should be more than surprised considering the way they have been turning up. Now this is quite significant. In case there are an infinite number, then a lot of Kummer's theory assumes much more importance than, I think, mathematicians have attached to it, since, in particular, Furtwängler discovered his law of reciprocity. The fact is, the latter's law of reciprocity does not generalize Kummer's law and the latter was restricted to regular fields. I have heard several number theorists state in the past that they thought the number of regular primes was finite. As you know, the cyclotomic fields considered are regular or properly irregular either. So this points up to the possibility that if there are any improperly regular cyclotomic fields, that list would appear to form quite a restricted class. To me this is an astonishing situation. You may recall that when I talked to you in L.A. several times, I expressed some doubt about continuing a project of testing Bernoulli numbers for regularity alone. At that time I had not studied your tables up to 2000 in detail, and I imagined that because the irregular primes appeared so dense in the 600's, that the regular primes would fade out later. Also, when I left you in L.A., I thought it quite probable that before you carried your computations much further [than] that what would appear to be an improperly irregular cyclotomic

[30] See above footnote 20.

[31] Vandiver to Emma and D.H. Lehmer: August 22, 1953.

> field would turn up. You will recall that we discussed at some length the ideas as to what to do if our criteria broke down consistently.
> Fortunately, I spent some years studying the property of the properly irregular cyclotomic fields and the results in the main turn out to be simpler than I had ever expected them to be. I do not think this work ever attracted very much attention, as the readers would imagine that because of the assumptions I made that this work was of a very special nature. Well, it certainly doesn't appear to be so special!
> *Another point, someone may prove Fermat's Last Theorem tomorrow, but unless his proof contains a demonstration that the second factor of the class number of a cyclotomic field defined by* $e^{2i\pi/p}$ *with p an odd prime is prime to p, I certainly would not recommend that the F.L.T. work be stopped. The main point is that every prime we test throws more light on this key problem of cyclotomic fields, that it, the possible divisibility of the second factor by p.*[32]

Interesting also in this regard are Vandiver's comments on current interest in cyclotomic integers and what he saw as problematic in the current interest in more abstract approaches to algebra:

> I forgot how unfashionable the theory [of cyclotomic fields] is at the present time. The tendency seems to be nowadays to take the viewpoint of abstract algebra and strive always for generality and immerse the cyclotomic field in some more general system. Thus, for example, some recent writer stated a result of this kind and observed that it was known previously "merely" for the special case of the cyclotomic field. Such birds are not consistent, however. No doubt the same man made a great fuss about the work of Erdös and Selberg on the prime number theorem. This would be curious from the first viewpoint I mentioned, as the rational field would be only a special case of the cyclotomic.
> At the present time I can only think of a handful of living mathematicians who ever paid any attention to the cyclotomic field in itself aside from myself. There are F. Pollaczek, Morishima, Inkeri, and Denes. So, anyone interested in cyclotomic fields must be a very exclusive group, and you or anybody else could not be criticized for not belonging to it.[33]
>
> In terms of the right strategy for writing the paper where the results of the SWAC computations were to be presented, this meant for Vandiver that it would be better to "avoid as much of the theory of cyclotomic fields as possible at the beginning of the paper."

One matter that proved to be really stimulating for Vandiver and the Lehmers was the rather efficient way in which SWAC, with a proper codification of the algorithms, made all computations: for the largest prime tested it took SWAC to run for three minutes. Emma Lehmer was quick to understand the significance of the new situation created in number theory by the use of high-speed computers. Because of her involvement with actual coding, on the one hand, and with detailed theoretical research in

[32] Vandiver to Emma and D.H. Lehmer: September 22, 1953. Emphasis in the original.

[33] Vandiver to Emma and D.H. Lehmer: October 7, 1953.

number theory, on the other hand, she was perhaps among the first to call attention to some broader implications of the use of computers that nowadays may seem obvious to many. Speaking soon after the publication of the article to an audience of applied mathematicians, she said [Lehmer E 1956, 104]:

> I have found coding an exacting science as well as an intriguing art. Not only does one learn a new language, but one has to speak it perfectly to be understood at all. The proverbial mathematician, whom Professor Pólya likes to describe, who thinks that something is A, says that it is B, writes down C, while it sould have been D, would get rapidly nowhere as a coder. The machine is a very exacting taskmaster. It acts dumb and fails to understand what you are trying to say until you are forced to say it just right. In this process it is not the machine but the coder who gets a liberal education in the art of straight thinking and invincible logic. All Sunday supplements to the contrary, machines do not think and machines do not learn; but in spite of this, they are exacting and relentless teachers having no sympathy or understanding for human foibles and frailties.

Vandiver published two additional articles where this line of attack was further pursued. This meant both further refinements of the Kummer-like criteria and, of course, additional computations with SWAC. First, with SWAC coded and operated by John Selfridge, Vandiver computed the relevant values for checking that FLT is valid for prime exponents p, $2000 < p < 2521$. Selfridge was at that time a graduate student at UCLA, and had been assisting Vandiver and the Lehmers from 1953.[34] At this point it was clear that about 40% of the primes were irregular and that no irregular prime existed with irregularity index greater than 2 [Vandiver 1954]. In a follow-up article published in 1955 in collaboration with Selfridge and Charles Nicol (Vandiver's doctoral student). Work with SWAC was supervised by Charles Brown Tompkins (1912–1971), then director of the INA. This time, the values of p examined were in the range $2520 < p < 4002$, and about hundred hours of machine time were employed in the computations. As in the pervious range the percentage of irregular primes found here was around 40%. On the other hand, it was pointed out, "if we take a comparatively short range and examine the number of irregular primes therein, percentages differ widely" [Vandiver, Selfridge & Nicol 1955, 971]. Also, only one prime number had been found with irregularity index 3 (this is 491, but this is not explicitly said in the article). In addition, all irregular primes thus far discovered were properly irregular.

8 Computers and FLT after SWAC

The situation created in the aftermath of the early application of electronic computers to FLT was similar in various respects to that existing close to hundred years earlier, after Kummer's proof of FLT for all exponents under 100. Like then, now in 1955 lower bounds for the validity of FLT were known separately for case I and case II (4003 being the lower bound for case II and hence for FLT at large). Much computation had been done in the meantime, and several significant conceptual advances

[34] See Vandiver to E. and D.H. Lehmer: September 1, 1953.

had been achieved, but no real conceptual breakthrough was reached. Kummer's criteria for the validity of FLT for exponents that are irregular prime numbers had been refined. The technical limitations in computing values of irregular primes and checking the various criteria for those cases were overcome by various techniques. First it was division of labor among human computers, then the help of mechanical devices, and finally with electronic digital computers. The accelerated pace of development in the processing and memory capacities of these latter devices in the decades to come could not even be imagined at this time. But from the point of view of the mainstream research in number theory the kind of results provided by the work of Vandiver and his associates was not properly at the center of attention, except to the extent that it satisfied the natural curiosity of any mathematician to be updated about current developments related to FLT. Thus, it did not become a main topic of research and it was left for a relatively small group of researchers that continued to deal with it.

And yet, unlike immediately after Kummer, a much shorter time was need now before a series of new papers started to appear where extended computations were actively pursued. Of course, this was closely connected to the more general phenomenon whereby intensive computations with electronic devices became increasingly common also in a field like number theory. Thus, in 1964 Selfridge and Pollack announced their computations indicating that FLT was true for any exponent up to 25,000 [Selfridge & Pollack, 1964]. Several additional computations were performed in the early 1970s with third-generation, minicomputers. In 1975, using a DEC PDP-10, Wells Johnson determined all irregular primes p less than 30,000 and showed that FLT is true for these primes. In his work, however, Johnson had broader aims than just FLT, and he also computed new values of Iwasawa invariants as well other properties of Bernoulli numbers [Johnson 1975].

A significant leap forward in this thread came the following year when Samuel Wagstaff announced the proof, mentioned at the beginning of this article, that FLT is true for $p < 100,000$ [Wagstaff 1978]. This proof was soon improved to reach values of $p < 125,000$. Wagstaff's computations identified all irregular primes up to that limit, 125,000, and led to many additional, illuminating results. In Wagstaff's opinion the most exciting one of this was the discovery of two primes with irregularity index 5: 78233 and 94693. Selfridge and Pollack had found in their work two primes with index 4, and to these Wagstaff added now another fourteen. On the other hand, no primes with index greater than 5 were found. The computations were all carried on four IBM 360/75 computers, the standard powerful computer at the time. They took about 80 min to complete for each prime near 125,000. The programs were written partly in 360 assembler language and partly in FORTRAN [Wagstaff 1978].

Wagstaff's work was followed by many other highly intensive computational efforts, some of which deserve being mentioned here. These works displayed an increasingly sophisticated use of algorithms and criteria taken from a broad spectrum of different number-theoretical works, an increasing understanding of problems related with the computational complexity of the algorithms implemented, and the use of ever more powerful machines. In 1988 Granville and Monagan used a generalized version of Wieferich criteria, together with many additional and extensive computations performed in a VAX machine to prove that case I of FLT is true for

prime exponents up to 714,591,416,091,389 [Granville & Monagan 1988]. This was followed by another computation of Wagstaff, in collaboration with Jonathan Tanner, that extended this result to prime exponents up to 156,442,236,847,241,729. This time a personal computer was already used for the calculations, but, for greater accuracy, the results were further checked with a CYBER 205 machine, a super computer produced by Control Data Corporation in 1979 as a truly powerful number-cruncher.

Work on case II also continued, and one interesting result was achieved in 1993, namely, that case II is valid for prime exponents p up to 4,000,000 [Buhler et al. 1993]. The mathematicians involved in this complex calculation dedicated their article to "the computational genius of Derrick Lehmer". They praised the Lehmers and Vandiver for their statement in 1954 that their calculations were relevant not only to FLT, but rather that they constituted "a permanent addition to our knowledge of cyclotomic fields". Indeed, the enduring interest in their calculations was evident for the many publications that came in their sequel over thirty years and in the work of Iwasawa on the structure of cyclotomic class groups. The very intensive computations involved here had been done over the course of several months using idle time of about one hundred NeXT workstations. They estimated that about 10^{15} arithmetic operations were involved, which is the equivalent of what a single such workstation could calculate in 10 years time. Of course, the question of the reliability of calculations needed to be addressed, and the authors expressed their reasons to believe in the accuracy of the results achieved, especially because "several entirely different programs written at different times by different programmers were used to check the data" (p. 153). Although the attempt to find ever higher values for the validity of FLT is still mentioned in an article like this, it is obvious that the real motivations for the effort invested here went well beyond this very circumscribed problem. This is clear, among other things, from the simple observation that these efforts continued in various ways even after Wiles' general proof of FLT. The same group of mathematicians sent their new results in 1996 (but they were corrected in 1999 and published only in 2001) reaching to values of irregular primes and cyclotomic invariants up to 12 millions. The computers involved and the algorithms implemented here reached a truly high degree of sophistication and power. In this latter article, FLT was not even mentioned [Buhler et al. 2001].

Developments related with work on FLT after SWAC, however, were not limited to calculations of this kind and included further results that connected with many of the ideas already mentioned here. One very important result in the mid-1980s, for instance, developed directly from ideas of Sophie Germain. It appeared in the joint contributions of Len Adleman, Roger Heath-Brown and Étienne Fouvry, which implied that there exist infinitely many primes for which case I of Fermat's last theorem holds [Fouvry 1985; Adleman & Heath-Brown 1985]. If we recall the quotation of Edwards at the beginning of this article, we realize that this result dispelled the main concern expressed there about the status of research in1977, and that all existing calculations, even those of Wagstaff, did not remove, namely that "one cannot rule out the possibility that the Theorem is false for all primes beyond some large bound."

9 Summary and concluding remarks

Considering the history of FLT from the point of view of the role and nature of the related calculations on individual cases offers interesting vistas on the development of the problem and of its place within the discipline of number theory. The relationship between number crunching and theory development changed over the years, as did the relationship between number crunchers and number theoreticians (sometimes, but not frequently, both roles appearing in one and the same person).

An early milestone discussed above touched upon the work of Kummer. As was seen, this mathematician performed intensive calculations and set up tables for himself as part of his efforts to gain direct insights on the inner workings of the new kinds of domains of numbers he undertook to investigate. This provided a solid basis that helped formulate his theory of ideal complex numbers in order to address the problem of higher reciprocity which was at the center of his agenda. As a side benefit, it also provided new tools to deal with FLT, and Kummer pursued this direction with some interest, but only inasmuch as the calculations involved required a reasonable amount of effort. Proving FLT for prime exponents up to one hundred was definitely a respectable result, but Kummer did not see any point in performing further calculations that had already become considerably complex. Nor did most of his successors. On the one hand, the most significant progress in number theory in the following generations, especially in Germany, focused on the development of abstract, general theories along the lines of both Dedekind and Kronecker. These developments neither encouraged the pursuit of computations for particular cases nor elicited any kind of particular attention towards FLT. Hilbert, while extolling the great achievements of Kummer, called to pursue research in number theory while avoiding calculations wherever possible. As for FLT, since Kummer's way was the only one open at the time to attack the problem, almost no efforts were devoted to deal with it beyond Kummer's own results.

Over the nineteenth century, mathematical table-making became an activity to which significant efforts were devoted at both the individual and the institutional levels. At some point, mechanization became central to this activity. Number theory received some degree of attention as part of these efforts, but much less than other, more applied pursuits that were the main motivation behind all these efforts. New work related to individual cases of FLT would eventually benefit from the values of Bernoulli numbers calculated in this framework, but these calculations were themselves in no way related to FLT nor motivated but this problem.

At the turn of the twentieth century a new avenue for research on FLT was opened with the results of Wieferich and Mirimanoff. This avenue brought a new motivation for computations with individual cases, as lower bounds for case I could now be calculated. Ever improving theorems that were added along this line over the following decades in the work of Dickson, Morishima and others only helped encourage this thread. Calculating machines were harnessed to these tasks, as were new tables of increased accuracy, including those that had been prepared with different purposes in mind. This line of attack on FLT also led to original work along the analytical tradition, especially by Rosser and the Lehmers, in which other kinds of computations with individual cases were involved. While all of these computations visibly helped

extend the domain of validity of case I, it is easy to see in retrospect that the complex network of mutually cross-referenced results underlying the support for these results was not always clear, and it contained many lacunae that were not always duly clarified.

Vandiver's early contributions to FLT were part of this thread, but he soon opened his own new direction of attack in which Kummer's results were refined and increasingly high values for case II were thus calculated. Vandiver himself was directly involved in these calculations but, since the calculations were long, complex and tedious, he assisted himself with groups of collaborators and with all kinds of devices, from mechanical ones all the way up to electronic computers.

The Lehmers were Vandiver's more important collaborators. Their eclectic mathematical background, their willingness to try all possible ways of attack on a given problem, and their institutional connections, placed them in a unique position to lead FLT into the electronic era. When this happened, it happened in a somewhat incidental way. Calculations related to FLT were for the Lehmers part of a much broader horizon of interests that at some point led to the use of computers for intensive number crunching in number theory in general and in which the art of computing programming became of intrinsic interest in ways that anticipated many questions later to be addressed by computer scientists and programmers.

The work of Vandiver and the Lehmers took place in the pioneering period of the electronic computer. Number theory entered this era somewhat hesitantly, but it gradually embraced computational methods as one of its central threads. With ever more powerful machines and with constantly improving programming techniques available, number-theoretical computations constantly extended the horizon of known results for many interesting open conjectures. This was the case for FLT too. But even by the mid-1980s, with the lower bound of certainty for FLT already well over 100,000 no new real conceptual breakthrough seemed to have been achieved. And then, when it was achieved with the thread that eventually led to Wiles' proof, it came from a completely different direction. In the case of FLT, number theory defeated number crunching, in spite of the very sophisticated methods and tools already available to the latter. And yet, there still seems to be plenty of motivation for number crunchers of the new generation to continue with their pursuits, including in relation with FLT, as material and conceptual tools continue to evolve and reach ever new heights.

References

Adams, John C. (1878), "Table of the values of the first sixty-two numbers of Bernoulli", *Jour. r. ang. Math.* 85 1878 . 269–272.

Adleman, Len and Roger Heath-Brown (1985), "The First Case of Fermat's Last Theorem", *Invent. Math.* 79, 409–416.

Ankeny, Nesmith and Sarvadaman Chowla (1949), "The Class Number of the Cyclotomic Field", *Proc. NAS* 35(9), 529–532.

Andree, Richard V. (1962), *A Table of Indices and Power Residues for all Primes and Prime Powers below 2000* (Introduction by H.S. Vandiver), New York, Norton.

Bachmann, Paul (1910), *Niedere Zahlentheorie,* Vol. 2, Berlin, Teubner.

Beeger, NGWH (1925), "On the Congruence $2^{p-1} \equiv 1 \pmod{p^2}$ and Fermat's Last Theorem", *Math. Messenger* 55, 17–26.

Beeger, NGWH (1939), "On the Congruence $2^{p-1} \equiv 1 \pmod{p^2}$ and Fermat's Last Theorem", *Nieuw. Arch. Wiskunde* 20, 51–54
Bernoulli, Jakob (1731), *Ars Conjecturandi*, Basel. (Fragment reproduced in David E. Smith (ed.), *A Source Book in Mathematics,* Dover Publications, New York, (1959, first edition 1929), Vol. 1, 85–90. Translated from the Latin by Jekuthiel Ginsburg.)
Bernstein, Felix (1903), "Über den Klassenkörper eines algebraischen Zahlkörpers", *Göttingen Nachrichten* 1903, 46–58 & 304–311.
Bernstein, Felix (1904) "Über unverzweigte Abelsche Körper (Klassenkörper) in einem imaginären Grundbereich", *Jahresb.* DMV 13, 116–119.
Bernstein, Felix (1910), "Ueber den letzten Fermat'schen Satz", *Göttingen Nachrichten* 1910, 482–488.
Brandt Heinrich and Wilhelm Patz (1956), *Canon Arithmeticus (K.G.J. Jacobi). Nach Berechnungen von Wilhelm Patz* (In verb. und erweiterter Form neu hrsg. von. Heinrich Brandt), Berlin, Akademie-Verlag.
Brillhart, John (1992), "John Derrick Henry Lehmer", *Acta Arithmetica* 62, 207–213.
Buhler, J.P., R. E. Crandall R. Ernvall, T. Metsänkylä (1993), "Irregular primes and cyclotomic invariants to four million", *Math. Comp.* 61 (1–2), 151–153.
Buhler, J., R. Crandall, R. Ernvall, T. Metsänkylä and M. Shokrollahi (2001), "Irregular primes and cyclotomic invariants to 12 million", *J. Symbolic Comput.* 31, 89–96.
Bullialdus, Ismael (1862), *Opus Novum ad Arithmeticam Infinitorum,* Paris.
Cahen, Eugene (1925), *Théorie des nombres. Cours de la Faculté des sciences de l'Université de Paris, Vol. 2: Le second degré binaire*, Hermann, Paris.
Campbell-Kelly, Martin et al (eds.) (2003), *The History of Mathematical Tables. From Sumer to Spreadsheets,* Oxford, Oxford University Press.
Carlitz, Leonard (1954), "A Note on Irregular Primes", *Proc. AMS* 5, 329–331.
Clausen, Thomas (1840), "Theorem", *Astron. Nach.* 17, 351–352.
Corry, Leo (2004), *Modern Algebra and the Rise of Mathematical Structures,* Basel and Boston, Birkhäuser (Second, revised edition).
Corry, Leo (2007), "Fermat Comes to America: Harry Schultz Vandiver and FLT (1914–1963), *Mathematical. Intelligencer* 29(3)(2007):30–40
Corry, Leo (2007a), "FLT Meets SWAC: Vandiver, the Lehmers, Computers and Number Theory", *IEEE Annals of History of Computing* (Forthcoming).
Corry, Leo (Forthcoming) "On the History of Fermat's Last Theorem: A Down-to-Earth Approach".
Croarken, Mary (1990), *Early Scientific Computing in Britain,* Oxford, Clarendon Press.
Croarken, Mary (2003), "Table Making by Committee; British Table Makers, 1871–1965", in Campbell-Kelly et al (eds.) (2003), 235–263.
Croarken, Mary and Martin Campbell-Kelly (2000), "Beautiful Numbers: The Rise and Decline of the British Association Mathematical Tables Committee. 1871–1965", *IEEE Annals for History of Computing* 22(4), 44–61.
Cunningham, Allan J.C. (1899), *A Binary Canon Showing Residues of Powers of 2 for Divisors under 1000, and Indices to Residues,* London : Taylor and Francis.
Cunningham, Allan J.C. (1904), *Quadratic Partitions,* London, F. Hodgson.
Cunningham, Allan J.C. (1905), "Haupt-exponents of 2", *Quart. Jour. Math.* 42, 241–250.
Cunningham, Allan J.C. (1917), *Quadratic and Linear Tables,* Hodgson, London.
Davis, Harold T. (1935), *Tables of the Mathematical Functions,* San Antonio, The Principia Press (2^{nd} revised edition: 1963).
Del Centina, Andrea (2007), "Unpublished Manuscripts of Sophie Germain and a Reevaluation of her Work on Fermat's Last Theorem", *Arch. History Exact Sci.* (DOI:10.1007/s00407-007-0016-4).
Dickson, Leonard E. (1908), "On the Last Theorem of Fermat", *Quart. Jour. Math.* 40, 27–45.
Dickson, Leonard E. (1908a), "On the Last Theorem of Fermat", *Math. Messenger* 38, 14–32.
Dickson, Leonard E. (1909), "On the Last Theorem of Fermat", *Proceedings ICM Rome* Vol. 2, 172.
Dickson, Leonard E. (1919), *History of the Theory of Numbers*, 3 Vols., New York, Chelsea.
Dickson, Leonard E. (1933), *Minimum Decomposition into Fifth Powers,* Mathematical Tables, British Assoc. for the Advancement of Science, Vol. 3, (Committee for the Calculation of Mathematical Tables), London, Office of the British Association.
Edmondson, Joseph (1885), "Summary of Lecture on Calculating Machines", *Proc. Phys. Soc. London* 7(1), 81–85.
Edwards, Harold M. (1975), "The Background of Kummer's Proof of Fermat's Last Theorem for Regular Primes" *Arch. Hist. Ex. Sci.* 14, 219-236.

Edwards, Harold M. (1977), *Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory,* New York, Springer.
Edwards, Harold M. (1977a), "Postscript to: 'The background of Kummer's proof of Fermat's last theorem for regular primes"', *Arch. His. Ex. Sci.,* 17, 381–394.
Edwards, Harold M. (2007), "About the Cover: Kummer's Tables", *Bull. AMS* 44(1), 133–135
Eisenstein, Ferdinand G. (1850), "Beweis der allgemeinsten Reciprocitätsgesetze zwischen reellen und complexen Zahlen", *Monatsberichte BA,* 189–198.
Ely, G.S. (1882), "Bibliography of Bernoulli Numbers", *Am. J. Math.* 5, 228–235.
Folkerts, Menso and Olaf Neumann (eds.) (2006), *Der Briefwechsel Zwischen Kummer und Reuschle* (Algorismus 50), Augsburg, Dr. Erwin Rauner Verlag.
Forsyth, Andrew R. (1929), "James Whitbread Lee Glaisher", *J. London Math. Soc.* 4, 101–112.
Fouvry, Étienne (1985), "Theorem de Brun-Titchmarsh- application au théorème de Fermat", *Invent. Math.* 79, 383–407.
Frobenius, Ferdinand Georg (1914), "Über den Fermat'schen Satz. III", *Berlin Ber.* (1914), 653–681.
Furtwängler, Philip (1912), "Letzter Fermatscher Satz und Eisensteinsches Reziprozitätsprinzip", *Wien. Ber.* 121, 589–592. (DOI:10.1007/s00407-007-0016-4)
Glaisher, John W. (1878), "On factor Tables . . .", *Proceedings of the Cambridge Philosophical Society* 3, 1878, 99–138.
Goldstein, Catherine (1994), "La théorie des nombres dans les *notes aux Comptes Rendus de l'Academie des Sciences* (1870–1914): un premier examen", *Riv. Stor. Sci.* 2, 137–160.
Goldstein, Catherine and Norbert Schappacher (2007), "Several Disciplines and a Book (1860–1901)", in Goldstein, Catherine, Norbert Schappacher and Joachim Schwermer, (eds.) (2007), *The Shaping of Arithmetic after C.F. Gauss's Disquisitiones Arithmeticae,* New York, Springer.
Gottschalk, Eugen (1938), "Zum Fermatschen Problem", *Math. Ann.* 115, 157–158.
Granville, Andrew & Michael B. Monagan (1988), " The First Case of Fermat's Last Theorem is True for all Prime Exponents up to 714,591,416,091,389", *Trans. AMS* 306, 329–359.
Grier, David A. (2005), *When Computers Were Human,* Princeton, Princeton University Press.
Gunderson, N.G. (1948), *Derivation of criteria for the first case of Fermat's last theorem and the combination of these criteria to produce a new lower bound for the exponent* (PhD Thesis, Cornell University).
Havil, Julian (2003), *Gamma. Exploring Euler's Constant,* Princeton, Princeton University Press.
Hecke, Erich (1910), "Ueber nicht-reguläre Primzahlen und den Fermat'schen Satz", *Göttingen Nachrichten* 1910, 420–424.
Hellegouarch, Yves (1972), *Courbes Elliptiques et Équation de Fermat*, Thèse, Université Besançon.
Hilbert, David (1998), *The Theory of Algebraic Number Fields,* Berlin, Springer. (English translation of the German original by F. Lemmermeyer and N. Schappacher.)
Huskey, Howard D. (1997), "SWAC-Standards Western Automatic Computer", *Annals of the History of Computing* 19, 51–61.
Huskey, Howard D. et al. (1997), "The SWAC Design Features and Operating Experience", *Annals of the History of Computing* 19, 46–50.
Inkeri, Kusta (1947), "Über den Euklidischen Algorithmus in quadratischen Zahlkörpern", *Ann. Acad. Sci. Fennicae Ser. A.* 1. Math.-Phys. 41, 1–35.
Iwasawa, Kenkichi and Charles Sims (1965), "Computation of Invariants in the Theory of Cyclotomic Fields", *J. Math. Soc. Japan* 18, 86–96.
Jacobi, Karl G.J. (1839) *Canon Arithmeticus sive Tabulae quibus exhibentur pro Singulis Numeris Primis vel Primorum Potestatibus infra 1000 Numeri ad Datos Indices et Indices ad Datos Numeros pertinentes,* Berlin, Typis Academicis.
Jensen, Kaj Løchte (1915), "Om talteoretiske Egenskaber ved de Bernoulliske Tal", *Nyt Tidsskrift for Matematik* 26, 73–83.
Johnson, Wells (1975), "Irregular primes and cyclotomic invariants", *Math. Comp.* 29 (Special Issue: A Collection of articles dedicated to Derrick Henry Lehmer on the occasion of his seventieth birthday), 113–120.
Kummer Ernst E. *(Coll), Collected Papers,* 2 Vols., ed. by André Weil, New York, Springer (1975).
Kummer Ernst E. (1844), *De numeris complexis, qui radicibus unitatis et numeris integris realibus constant,* Gratulationschrift der Univ. Breslau zur Jubelfeier der Univ. Königsberg, Reprinted in *Jour. math. p. appl.* 12 (1847), 185–212. (*Coll* Vol. 1, 165–192.)
Kummer Ernst E. (1847), "Zur Theorie der complexen Zahlen", *Jour. r. ang. Math.* 35, 319–326. (*Coll* Vol. 1, 203–210.)

Kummer Ernst E. (1847a), "Beweis des Fermat'schen Satzes ...", *Monatsberichte BA,* 132–141 & 305–319. (*Coll* Vol. 1, 274–297.)
Kummer Ernst E. (1850), "Allgemeine Reciprocitätsgesetze für beliebige höhere Potenzreste", *Monatsberichte BA,* 154–165. (*Coll* Vol. 1, 347–357.)
Kummer Ernst E. (1850a), "Allgemeiner Beweis des Fermat'schen Satzes, ...", *Jour. r. ang. Math.* 40, 130–138. (*Coll*. Vol. 1, 336–344.)
Kummer Ernst E. (1851), "Mémoire sur la théorie des nombres complexes composés de racines de l'unite et de nombres entiers", *Jour. math. p. appl.* 16, 377–498. (*Coll* Vol. 1, 363–484.)
Kummer Ernst E. (1857), "Einige Sätze über die aus den Wurzeln der Gleichung ...", *Abh. BA,* 1857, 41–74. (*Coll* Vol. 1, 639–672.)
Kummer Ernst E. (1859), "Über die allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist", *Abh. BA,* 19–159. (*Coll* Vol.1, 699–839.)
Landau, Edmund (1913), "Une série de réponses", *L'intermediaire des mathematiciens* 20, 206.
Lang, Serge (1978), *Cyclotomic Fields*, New York, Springer.
Laubenbacher, Reinhard and David Pengelley (1999), *Mathematical Expeditions*, *Chronicles by the Explorers*, New York, Springer.
Lehmer, Emma (1956), "Number Theory on the SWAC", *Proc. Symp. Applied Math.* 6, *AMS*, 103–108.
Lehmer, Emma and Derrick H. Lehmer (1941), "On the first case of Fermat's last theorem", *Bull. AMS* 47, 139–142.
Lehmer, Derrick H. (1932), "A note on Fermat's last theorem", *Bull. AMS* 38, 723–24.
Lehmer, Derrick H. (1933), "A photo-electric number-sieve", *Amer. Math. Monthly* 40, 401–406.
Lehmer, Derrick H. (1935), "Lacunary recurrence formulas for the numbers of Bernoulli and Euler", *Ann. Math.* 36, 637–648.
Lehmer, Derrick H. (1936), "An extension of the table of Bernoulli numbers", *Duke Math. J.* 2, 460–464.
Lehmer, Derrick H. (1940), "On the Maxima and Minima of Bernoulli Polynomials", *Am. Math. Mo.* 47(8), 533–538.
Lehmer, Derrick H. (1940a), "The lattice points of an n-dimensional tetrahedron", *Duke Math.* J. 7, 341–353.
Lehmer, Derrick H. (1953), "The sieve problem for all purpose computers", *Math. Tables and Other Aids to Computation* 7, 6–14.
Lehmer, Derrick Norman (1909), *Factor table for the first ten millions, containing the smallest factor of every number not divisible by 2, 3, 5, or 7 between the limits 0 and 10017000,* Washington, Carnegie Institution of Washington.
Lehmer, Derrick Norman (1914), *List of prime numbers from 1 to 10 006 721*, Washington, Carnegie Institution of Washington.
Lehmer, Derrick Norman (1939), Factor Stencils, (Revised and extended by J. D. Elder) Washington, Carnegie Institution of Washington.
Maillet, Edmond (1897), "Sur l'équation indéterminée $ax^{\lambda t} + by^{\lambda t} = cz^{\lambda t}$", *Assoc. Francaise St. Etienne* 26, 156–168.
Meissner, Waldemar (1913), "Über die Teilbarkeit von 2^{p-2} durch das Quadrat der Primzahl $p = 1093$", *Berl. Ber.* 1913, 663–667.
Miller, J.C.P. (1963), "Alfred Edward Western", *J. London Math. Soc.* 38, 278–281.
Minkowski, Hermann (1905), "Peter Gustav Lejeune Dirichlet und seine Bedeutung für die heutige Mathematik", *Jahresb. DMV* 14, 149–163.
Mirimanoff, Dimitry (1893), "Sur l'équation $x^{37} + y^{37} + z^{37} = 0$", *Jour. r. ang. Math.* 111, 26–30.
Mirimanoff, Dimitry (1904), "L'équation indeterminèe $x^l + y^l + z^l = 0$ et le critérium de Kummer", *Jour. r. ang. Math.* 128, 45–68.
Mirimanoff, Dimitry (1910), "Sur le dernier théorème de Fermat", *Comptes Rendus de l'Academie des Sciences* 150, 204–206.
Mosteller, F (1964), "Samuel S. Wilks: Statesman of Statistics", *American Statistician* 18, 11–17.
Morishima, Taro (1931), "Über den Fermatschen Quotienten", *Japanese Journ. of Math.* 8, 159–173.
Morishima, Taro (1932), "Über die Fermatsche Vermutung. VII." *Proc. Imp. Acad. Jap.* 8, 63–66.
Murty, M. Ram and Yiannis N. Petridis (2001), "On Kummer's Conjecture", *J. Number Theory 90 (2), 294–303.*
Nellen, H. J. M. (1994), *Ismaël Boulliau (1605–1694), Astronome, Épistolier, Nouvelliste Et Intermédiaire Scientifique* (Studies of the Pierre Bayle Institute), Amsterdam and Utrecht, APA-Holland University Press.
Nielsen, Niels (1923), *Traité élémentaire des nombres de Bernoulli,* Paris, Gauthier-Villars.

Ohm, Martin (1840), "Etwas über die Bernoulli'schen Zahlen", *Jour. r. ang. Math.* 20, 11–12.
Pollaczek, Felix (1917), "Über den grossen Fermat'schen Satz", *Wien. Ber.* 126, 45–59.
Pollaczek, Felix (1924), "Über die irregulären Kreiskörper der l-ten und l^2-ten Einheitswurzeln", *Math. Z.* 21, 36–38.
Reitwiesner, George W. (1950), "An ENIAC Determination of π and e to more than 2000 Decimal Places", *Mathematical Tables and Other Aids to Computation* 4, 11–15.
Reuschler, Carl G. (1875), *Tafeln complexer Primzahlen aus Wurzeln der Einheit gebildet sind,* Berlin.
Robinson, Raphael (1954), "Mersenne and Fermat Numbers", *Proceedings AMS* 5, 842–846.
Rosser, J. Barkley (1939), "On the first case of Fermat's last theorem", *Bull. AMS* 45, 636–640.
Rosser, J. Barkley (1940), "A new lower bound for the exponent in the first case of Fermat's last theorem", *Bull. AMS* 46, 299–304.
Rosser, J. Barkley (1941), "An additional criterion for the first case of Fermat's last theorem", *Bull. AMS* 47, 109–110.
Rutland, Davis (1995), *Why Computers are Computers. The SWAC and the PC*, Philomath, OR, Wren Publishers.
Schoenbaum, E. (1908), "Ke Kummerovým pracim o Fermatově větě", *Casopis, Prag,* 37, 484–502.
Selfridge, John and B.W. Pollack (1964), "Fermat's last theorem is true for any exponent up to 25,000", *Notices AMS* 11, 97.
Serebrennikov, S. (1907), "Neue Berechnungsmethode der Bernoullischen Zahlen", *St. Pétersb. Mém.* 19 (4), 6.
Siegel, Carl L. (1964), "Zu zwei Bemerkungken Kummers", *Gött. Nachr.* 1964, 51–62.
Smith, Henry J.S. (1965), *Report on the Theory of Numbers* (originally published in six parts as a Report of the British Assn., 1859–1866), Chelsea, New York.
Stafford, Elizabeth and Harry S. Vandiver (1930), "Determination of some properly irregular cyclotomic fields", *Proc. NAS* 16, 139–150.
Staudt, Karl G. C. von (1840), "Beweis eines Lehrsatzes, die Bernoullischen Zahlen betreffend, *Jour. r. ang. Math.* 21, 372–374, 1840;
Swade, Doron (2003), "The 'unerring certainty of mechanical agency': machines and table making in the nineteenth century", in Campbell-Kelly et al (eds.) (2003)" 145–174.
Todd, John (1990), "The prehistory and early history of computation at the NBS", in S.G. Nash (ed.) *A History of Scientific Computing,* New York, Addison-Wesley, pp. 251–268.
Tschinkel, Yuri (2006), "About the cover: On the distribution of primes – Gauss' Tables", *Bull. AMS* 43, 89–91.
Vandiver, Harry S. (1914), "Extensions of the criteria of Wieferich and Mirimanoff in Connection with Fermat's Last Theorem", *Jour. r. ang. Math.* 114, 314–318.
Vandiver, Harry S. (1919), "A property of cyclotomic integers and its relation to Fermat's last theorem", *Ann. Math.* 21, 73–80.
Vandiver, Harry S. (1920), "On Kummer's Memoir of 1857 Concerning Fermat's Last Theorem", *Proc. Nat. Acad. Sci.* 6, 266–269.
Vandiver, Harry S. (1920a), "On the class number of the field Ω ($e^{2i\pi/pn}$) and the second case of Fermat's last theorem", *Proc. Nat. Acad. Sci.* 6, 416–421.
Vandiver, Harry S. (1922), "On Kummer's memoir of 1857, concerning Fermat's last theorem (second paper)", *Bull. AMS* 28, pp. 400–407.
Vandiver, Harry S. (1925), "On a new type of criteria for the first case of Fermat's last theorem", *Ann. Math.* 26, 88–94.
Vandiver, Harry S. (1925a), "A property of cyclotomic integers and its relation to Fermat's last theorem (second paper)", *Ann. Math.* 26, 217–232.
Vandiver, Harry S. (1926), "Transformations of Kummer's criteria in connection with Fermat's last theorem", *Ann. Math.* 27, 94–96.
Vandiver, Harry S. (1929), "On Fermat's Last Theorem", *Trans. AMS* 31, 613–642.
Vandiver, Harry S. (1930), "Summary of results and proofs on Fermat's last theorem (fifth paper)", *Proc. NAS* 16, 298–305.
Vandiver, Harry S. (1930a), "Summary of results and proofs on Fermat's last theorem (sixth paper)", *Proc. NAS* 17, 661–673.
Vandiver, Harry S. (1932), "Note on the divisors of the numerators of Bernoulli's numbers", *Proc. NAS* 18, 594–597.

Vandiver, Harry S. (1934), "Fermat's last theorem and the second factor in the cyclotomic class number", *Bull AMS* 40, 118–126.
Vandiver, Harry S. (1937), "On Bernoulli Numbers and Fermat's Last Theorem", *Duke Math. J.* 3, 569–584.
Vandiver, Harry S. (1937a), "On Bernoulli numbers and Fermat's last theorem (second paper)", *Duke Mathematical Journal* 3, 418–427.
Vandiver, Harry S. (1946), "Fermat's Last Theorem", *Am. Math. Mo.* 53 (1946), pp. 555–578.
Vandiver, Harry S. (1954), "Examination of methods of attack on the second case of Fermat's last theorem", *Proc. NAS* 40, 732–735.
Vandiver, Harry S., Derrick H. Lehmer and Emma Lehmer (1954), "An application of high-speed computing to Fermat's last theorem", *Proc. NAS* 40, 25–33
Vandiver, Harry S., John L. Selfridge and Charles A. Nicol (1955), "Proof of Fermat's last theorem for all prime exponents less than 4002", *Proc. NAS* 41, 970–973.
Vandiver, Harry S. and George E. Wahlin (1928), *Algebraic Numbers - II.Report of the Committee on Algebraic Numbers,* Washington, D.C.,National Research Council.
Wagstaff, Samuel S. (1976), "Fermat's Last Theorem is true for any exponent less than 100,000 (abstract)", *Notices AMS* 167, A-53.
Wagstaff, Samuel S. (1978), "The irregular primes to 125000", *Math. Comp.* 32 (142), 583–591.
Washington, Lawrence (1997), An Introduction to Cyclotomic Fields (2nd ed.), New York, Springer-Verlag.
Western, Alfred E. (1928), "Allan Joseph Champneys Cunningham", *J. London Math. Soc.* 1–3, 317–318.
Western, Alfred E. & J.C.P. Miller (1968), *Tables of Indices and Primitive Roots,* (Volume 9 of the Royal Society Mathematical Tables), Cambridge, Cambridge University Press.
Wieferich, Arthur (1909), " Zum letzten Fermat'schen Theorem", *Jour. r. ang. Math.* 136, 293–302.
Williams, Hugh C. (1998), *Édouard Lucas and Primality Testing,* New York, John Wiley and Sons.