Hunting Prime Numbers from Human to Electronic Computers

Leo Corry - Tel Aviv University

Abstract

The present article discusses the changing attitudes of mathematicians towards intensive computations with particular cases as part of the discipline of number theory from the second half of the nineteenth century on. It focuses on the cases of Mersenne primes and irregular primes and discusses factors that shaped these attitudes in various historical contexts. It describes, in particular, the work of Emma and DH Lehmer and the unique approach they followed in their number theoretical investigations. This approach helped them take a leading role in the early incursion of digital computers into number theory. This incursion is described against the background of institutional, ideological and technological aspects of the development of the discipline of number theory in the USA in the period considered. Their cooperation in 1952 with Raphael Robinson in calculating new cases of Mersenne primes with SWAC at UCLA is discussed in some detail.

1. Introduction

Frank Nelson Cole (1861-1921) was among the prominent American mathematicians of his generation. He was long time secretary of the American Mathematical Society and editor-in-chief of its *Bulletin*. He was institutionally immortalized in the late 1920s as two important AMS prizes bearing his name were established, in number theory and in algebra respectively. Cole is also remembered for a legendary achievement that Eric Temple Bell (1883-1960) recounted in his *Mathematics; Queen and Servant of Sciences* as follows [Bell 1951, 228]:

> At the October, 1903, meeting in New York of the American Mathematical Society, Cole had a paper on the program with the modest title *On the factorization of large numbers*. When the chairman called on him for his paper, Cole—who was always a man of few words—walked to the board and, saying nothing, proceeded to chalk up the arithmetic for raising 2 to the sixty-seventh power. Then he carefully subtracted 1. Without a word, he moved over to a clear space on the board and multiplied out, by longhand,
>
> $$193{,}707{,}721 \times 761{,}838{,}257{,}287.$$
>
> The two calculations agreed. … For the first and only time in record, an audience of the American Mathematical Society vigorously applauded the author of a paper delivered before it. Cole took his seat without having uttered a word. Nobody asked him a question.

The number $2^{67} - 1$ is, of course, the Mersenne number M_{67}, and Cole's achievement represented a veritable *tour de force* of patience and computational skills. Bell intended above all to preserve "a small bit of history before all the American mathematicians of the first half of the twentieth century are gone." When he had asked Cole in 1911, he wrote, how long it had taken to crack M_{67}, Cole reportedly answered: "three years of Sundays."

Historians of mathematics tend to distrust the historical reliability of most of Bell's accounts, and in this case there are good reasons to stick to this habitude. For one thing, the *Bulletin of the American Mathematical Society* records the talks presented at its meeting of December 31, 1903, in New York, including Cole's, precisely with the name mentioned by Bell. The text is much more elaborate than simply two arithmetic operations whose results are equated, and it contains some interesting ideas about the importance of the result and about how Cole went about finding the factors involved in his calculation (more on this below). One may certainly agree that Cole deserved the standing ovation, and indeed the ovation may have actually taken place. None of this, however, is mentioned in the *Bulletin*. As for the amount of time spent on the calculation, there seems to be no other source of information about this than Bell. His account, at any rate, became an accepted mathematical urban legend that has been repeated over and over again, often extending the three years of Bell to "twenty years of Sunday afternoons."[1] One way or another, the result is admirable and one may be sure that it was achieved only after much computational effort.

Almost hundred years later, another remarkable factorization of large integers took place, this one involving much bigger numbers. In 1997 a team of computer scientists led by Samuel Wagstaff at Purdue, factorized a 167-digit number, $(3^{349} -1)/2$, into two factors of eighty and eighty-seven digits respectively.

According to Wagstaff's report, the result required about 100,000 computer hours. Wagstaff had previously been involved in many other remarkable computations. For

[1] A recent example appears in [Ruskeepää 1998, 1].

instance, in 1978 he used a digital computer to prove that Fermat's last theorem (FLT) is valid for prime exponents up to 125,000. This required computing values of Bernoulli numbers in order to identify new instances of irregular primes (more on this below). His methods were further developed over the following decades and, combined with new algorithms and symbolic computation techniques, they continue to be applied for very intensive calculations that have showed, e.g., that FLT is valid for prime exponents up to 12,000,000 (Buhler et al 2001).

Factorization results such as Cole's and Wagstaff's will at the very least elicit a smile of approval on the side of anyone with a minimum of sympathy and appreciation for remarkable mathematical results. But when faced with the price tag (in terms of time spent to achieve it), the same sympathetic listener (and by all means the cynical one) will immediately raise the question whether all this awful lot of time was worth spending. Investing valuable resources in the search for ever higher values of exponents for which FLT is valid may appear to be an especially awkward pursuit after 1994, the year when Andrew Wiles gave a general proof that FLT is valid *for any exponent*. As a matter of fact, it is plausible that critical attitudes towards the value of these kinds of mathematical pursuits may come (or came), in the first place, from pure mathematicians and even from leading number theorists. Indeed, if we look at the opinions of some of the most prominent number theorists at the turn of the twentieth century, we may find clear evidence pointing to this direction. A very famous instance of this appears in a passage from the introduction of a well-known book of David Hilbert (1862-1943). The *Zahlbericht* ("Report on numbers") was one of the most influential texts in the discipline

for decades after its publication in 1897. Referring to the recent development of the theory of algebraic number fields, starting with ideas of Ernst Edward Kummer (1810-1893) and then moving to the hands of Richard Dedekind (1831-1916) and Leopold Kronecker (1823-1891), Hilbert said [Hilbert 1998, 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 application in the proof of the higher reciprocity laws. I have tried to avoid Kummer's elaborate computational machinery, so that here ... proof can be completed not by calculations but purely by ideas.

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].

One may assume that both Hilbert and Minkowski could be counted among those who would approve with a smile when faced with Cole's result, but at the same time one can hardly think of either them as devoting so much of their own time (or the time of their students) to a task of that kind, and much less to a mathematical task of the kind undertook by Wagstaff or any of his followers. So, a general historical question arises here concerning the conditions and circumstances under which time-consuming, computational tasks are deemed by mathematicians of being worth their time, efforts, and resources. It is obvious that in a discipline like number theory there is always an ongoing interplay between calculations with specific cases, on the one hand, and the formulation

of powerful theories that should provide general theorems, algorithms and results, on the other hand. Still, there is a question of balance between these two aspects of mathematical activity, and the factors that affect this balance throughout history. It is this question that occupies the main focus of the present article.

In the case of the examples mentioned above, one can immediately notice the different mathematical circumstances in which these tasks involving in their own ways intensive calculations might be justified. Sheer scientific curiosity was of course a main motivation behind both Cole's and Wagstaff's calculations, but Wagstaff's quest could also be justified by external factors that did not apply back at Cole's time. Such factors are explicitly stated in a press release published by Purdue University following the announcement of Wagstaff's factorization result, under the title: "Number crunchers zero in on record-large number".[2] Wagstaff cared to stress for the press the importance of knowing the limits of our abilities to perform such large factorization while arguing that the latter are "essential to developing secure codes and ciphers." Cole did not have to provide any kind of justification for the resources spent on reaching his result (i.e., his time), and not only because they were significantly cheaper than those involved in Wagstaff's result. If called to do so, he could not have put forward an argument similar to Wagstaff's. General perceptions about the need, and the appropriate ways for public scrutiny of science, its tasks and its funding, changed very much in the period of time between 1903 and 1997, and this in itself would be enough to elicit different kinds of reactions to both undertakings. But above all, it was the rise of e-commerce and the need for secure encryption techniques for the Internet that brought about a deep revolution in

[2] See http://homes.cerias.purdue.edu/~ssw/Wnumber.html.

the self-definition of the discipline of number theory in the eyes of many of its practitioners, and in the ways it could be presented to the public. Whereas in the past, this was a discipline that prided itself above all for its detachment from any real application to the affairs of the mundane world, over the last three decades it turned into the showpiece of mathematics as applied to the brave new world of cyberspace security. The application of public-key encryption techniques, such as those based on the RSA cryptosystem, turned the entire field of factorization techniques and primality testing, from an arcane, highly esoteric, purely mathematical pursuit into a most coveted area of intense investigation with immediate practical applications, and expected to yield enormous economic gains to the experts in the field.

Cole, as far as we know, provided no explicit justification for the many hours spent on his pursuit. He was, after all, a man of few words (at least according to Bell). Probably he felt no need to provide such a justification to begin with. But another mathematician who was directly involved in factorizations similar to Cole's in the pre-RSA era of number theory did state clearly his views on these matters, and it is pertinent to quote him here. This is Derrick Henry (Dick) Lehmer (1905-1991) about whom I will say more below. He developed a life- long interest in computing devices, especially as applied to number theory. One of the various machines he was involved with was a photoelectric sieve he built in 1932 for factorizing integers and identifying prime numbers. He used it successfully to find the factors of M_{93} in several minutes work of the "rapidly rotating wheels" of the sieve, this time being spent in trying out a certain formula on ten million candidate numbers. Lehmer compared this short and accurate calculation to that of a man entrusted with performing the same task: each separate trial would take a man at least six

minutes; assuming that the man would work ten hours a day it would take him a hundred thousand years, i.e., three hundred years "if he did not get stale".

Technologically speaking, Lehmer was closer to Wagstaff than to Cole, but his justification discourse was of a completely different kind, presumably adequate for Cole as well. It may come as a surprise to many, he said, "that the most compelling urge to the study of mathematics is not its practical application to the study of every day, bread-and-butter life, but lies in the romance and glamour surrounding its mysterious secrets." Moreover, he thought, it will come as a shock to some, when they are told that there is absolutely no practical application to this "astonishing machine upon which so much thought and care has been expended." He certainly did not see himself as looking for any application, and he was strongly opinionated about it [Lehmer 1932, 235]:

> There is a cowardly and sinking sort of a scientist, no doubt, who is ashamed or afraid to take a walk in the country with the avowed purpose of enjoying the landscape. He must provide himself with a fishing rod or a collecting basket of some sort, so that if one asks him why he is aborad he will be able to point to some "practical application" for his stroll in the hills. He is, no doubt, merely trying to avoid the odium that seems to have attached itself to the poet or to the musician who is hard put to it to procuce a health, bread-and-butter reason for making a sonnet or a symphony. To listen to the apologists for the study of pure mathematics one would get the impression that this study is sustained, not by the Wonder or Beauty of the subject, but by its external utilities. But how little of the vast field of mathematics has to do with the study of the outside world!

Many mathematicians expressed similar opinions before or after Lehmer, the most noted of whom was Hardy in his famous *A Mathematician's Apology* [Hardy 1940]. Here it has a special flavor because of later developments as embodied in works such as Wagstaff's

and the discourse that developed around them. And, in addition, Lehmer ended his text by sounding a prophetic note that enhances the main thrust of his opinions. He thus wrote:

> The subtle and expensive determinations of the bending of a ray of light by a gravitational field, or the careful listing of the binary starts in the heavens, can have little application to the making of two squares where only one grew before. Faraday, playing with wires in his laboratory, wrests from the hands of nature a torch that Edison uses to light the world, and Einstein to light the universe. Who can tell? Perhaps in some far distant century they may say, "Strange that those ingenious investigations into the secrets of the number system had so little conception of the fundamental discoveries that would later develop from them!"

Lehmer passed away precisely at the time when it was becoming clear that the only miscalculation involved in a statement like his was that it would be enough to wait several decades, rather than centuries.

The deep change in the status of time-consuming computational tasks from Cole to Wagstaff, via Lehmer, provides an extreme, most visible example of the more general topic of this article, namely, the changing attitudes of mathematicians towards intensive computations with particular cases as part of the discipline of number theory from the second half of the nineteenth century on. By focusing on the cases of Mersenne primes and irregular primes I will discuss some of the factors that shaped these attitudes in various historical contexts. Section 2 contains an account of the early history of Mersenne primes up to Cole. It provides an overview of the works of mathematicians involved in calculating such numbers and of their scopes of interests, as well as of their main methodological guidelines. Section 3 focuses on work on irregular primes done by Kummer. In spite of their apparent conceptual proximity, these two fields of research in number theory, Mersenne numbers and irregular primes, developed in completely

different ways. This is particularly the case when it comes to the question of massive computations performed in relation with each of them. Section 4 provides a comparative overview of the stories of these two kinds of calculations and in doing so, it directs the focus of attention to the topics to be discussed in the following sections. Section 5 describes the early work of the Lehmers and the unique approach they followed in their number theoretical investigations, making them ideal candidates to taking a leading role in the early incursion of digital computers into number theory. This incursion is described in section 7, after having discussed in section 6 some institutional, ideological and technological aspects of the development of the discipline of number theory in the USA in the period considered, and the main changes that affected it. This discussion provides a broad historical context for understanding the work of the Lehmers and its idiosyncratic character within the discipline. Their unique professional and institutional position facilitated a process that could otherwise have taken much longer to materialize, whereby massive calculations with digital computers were incorporated into number theory, first at the margins and gradually into its mainstream.

2. Mersenne Primes

Cole's computation of the factors of M_{67} is at the peak of a fascinating mathematical story that can be traced back to the Pythagoreans' interest in perfect numbers.[3] These are

[3] In this section I have relied on information provided by three main sources: [Dickson 1920, Vol. 1], [Décaillot 1998], [Williams 1998].

integers n, such as 6 and 28, satisfying the property that n equals the sum of their proper factors (i.e., not including n itself). The arithmetical books of Euclid's *Elements* culminate with Proposition 36 of Book IX, which (in modern terms) states that:

> **(E)** numbers of the form $2^{n-1}(2^n - 1)$ are perfect whenever $(2^n - 1)$ is prime for some n.

Nicomachus of Gerasa (@ 60 -120, AD), who discussed Eratosthenes' sieve method for determining primeness and was aware that 31 and 127 were prime, established that 6, 28, 496, 8128 are perfect numbers (i.e., when in the above formula we use n = 2, 3, 5, 7). Nicomachus advanced many additional claims about the perfect numbers, such as, for example, that they all end alternately in digits 6 and 8, or that the nth perfect number has n digits. Nicomachus and many others after him also assumed that all perfect numbers are even and that, indeed, the perfect numbers yield by Euclid's criterion **(E)** are all the perfect numbers that exist.

Many of these claims turned out to be wrong, and some were later proved to be correct. From the point of view of our account here it is important to stress, above all, that even at this early stage of the history of number theory we see two completely different kinds of emphasis embodied in the respective approaches of Euclid and Nicomachus to the same question: the former formulated the general principle and proved the general theorem, whereas the latter set out to look for specific instances of perfect numbers by calculating with particular cases. This quest for individual instances in the hands of a Pythagorean like Nichomacus finds a clear explanation in his more mystical than purely mathematical motivations. Euclid's general formulation and proof of the criterion pertaining to the

perfect numbers, on the other hand, is in line with the overall spirit of his mathematics, as embodied in the *Elements*.

Although after Nicomachus we find discussions about perfect numbers in various sources, especially in the Islamic world, further instances of perfect numbers were discovered only much later, in fifteenth-century Europe. A main figure in this development was Pietro Cataldi (1552-1626) who by 1603 was aware of the primality of $2^{13} - 1$, $2^{17} - 1$, and $2^{19} - 1$ (but was not the first to add numbers to the list of four numbers known in antiquity). More importantly, he was the first to realize that if $2^n - 1$ is prime, then n has to be prime.

The study of what we call now Mersenne primes started as part of this same thread of ideas. Marin Mersenne (1588 – 1648) was a French Minim friar who became known in the history of mathematics for his role as a clearing house for correspondence between eminent philosophers and scientists – such as Descartes, Pascal and Fermat – as well as for his own enthusiastic interest in questions related with number theory. Like various others with a similar interest before him, Mersenne approached the question of the perfect numbers and of the primality of the factors $2^n - 1$. In a text published in 1644 Mersenne came up with the surprising statement that from the fifty-five primes in the range $n \leq 257$, the perfect numbers of the form $2^{n-1}(2^n - 1)$ are only those that obtain for n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257. Mersenne was perfectly aware of the enormous difficulty involved in testing the primality of large numbers of 15 to 20 digits that appear in this context, and it is obvious that he did not actually check all the factors $2^n - 1$ for the cases appearing in his list. It is thus all the more curious that he was so certain about his guess as expressed in that statement. By looking at a different text of Mersenne, historian

Stillman Drake [Drake 1971] was able to determine the rule by which he apparently produced the list:

(M1) the values of n for which $2^n - 1$ is prime are either of the form $n = 2^k \pm 1$ or of the form $n = 2^{2k} \pm 3$.

Mersenne's list, however, is incorrect. The values $n = 67, 257$ do not yield primes as he claimed, whereas the values $n = 61, 89, 107$ do yield primes but they are missing in the list. Nonetheless the list is an amazing achievement not just because of the many insights it involves and the calculational effort involved in producing it, but also because the very long time that passed before its mistakes were first spotted. Indeed, the first mistake to be identified was that 61 should be in the list even by Mersenne's own rule. This fact was not discovered before 1883. The mistake was sometimes explained as being merely a typographical one in Mersenne's original text [Bateman et al 1989].

Mersenne's interest in these kinds of question was a main topic of discussion in his correspondence in general, and particularly so with Fermat. In his letters to Mersenne, as was his habitude, Fermat raised many interesting ideas, mentioned many general results proved along the way (but usually without revealing his proof) and proposed new problems to be solved. Using some of the general results he had proved, Fermat also addressed questions related with particular cases of Mersenne numbers. In a letter of 1638 he formulated in a precise way, for the first time, the statement that all *even* perfect numbers are such that satisfy Euclid's condition **(E)**. In a different letter, to Frans van Schooten (1615-1660) in 1958, he proposed the challenge of proving or disproving this assertion. He also showed, for example, that 23 was a factor of M_{11} and that 47 a factor of M_{23}.

Among other original ideas mentioned by Fermat in his letters dealing with the Mersenne numbers, a famous one he discussed concerned the question of the possible divisors of numbers $2^m + 1$. In this context he advanced the claim that numbers of the form $F_m = 2^{2^n}+1$ are always prime. Such numbers F_m are called Fermat numbers. Interestingly, in a letter sent in 1659 to another of his correspondents, Pierre de Carcavi (1600-1684), but actually intended for Christian Huygens (1629-1695), Fermat suggested that he had a proof of this conjecture based on the "method of infinite descent" [Fermat *Oeuvres*, Vol. 2, 431-436]. Eventually, however, in 1732 Leonhard Euler (1707-1783) famously showed that F_5 is not a prime.

A series of prominent mathematicians of the following generations undertook to solve problems associated with Fermat's legacy in number theory, a field of mathematical interest that was called then, simply, higher arithmetic. The most distinguished of these included Euler, Joseph Louis Lagrange (1736–1813), Adrién Marie Legendre (1752-1833) and Carl Friedrich Gauss (1777-1855). Among many other things, Euler proved a series of results that allowed him to identify, in many cases, factors of Mersenne numbers. These same results stood behind his proof that F_5 is not prime. At the same time, he also proved that M_{31} is prime, which remained the largest known prime until 1851. A posthumous paper by Euler contains the first proof that Euclid's condition **(E)** does give all possible *even* perfect numbers [Sandifer 2006]. This result also implies that

all even perfect numbers end in either a 6 or 8, but not alternately as stated by Nichomacus.[4]

Legendre further developed some of the new methods introduced by Euler to the discipline and used them to find factors of numbers that were quite large at the time, such as 10,091,401. The factorization techniques he introduced had long lasting influence and they deserve a brief discussion here. Legendre relied on the concept of quadratic residue: a is called a quadratic residue of p if there exists integers x that satisfy the congruence $x^2 \equiv a \pmod{p}$. Otherwise, a is a quadratic nonresidue of p. It is easy to see that if p is an odd prime, then there are exactly $(p-1)/2$ quadratic residues mod p, and $(p-1)/2$ nonresidues. Legendre introduced a useful notation (a/p), the Legendre symbol, to indicate that a is a quadratic residue mod p (in which case $(a/p) = 1$) or a nonresidue (in which case $(a/p) = -1$). Now, let us assume that for a integer N we can write

$$kN = x^2 - ry^2, \qquad (*)$$

for some values of k and r. It can be seen that in such cases, if a prime p divides N, then $(r/p) = 1$. Using some additional, elementary properties of the quadratic residues, this property allows determining forms of primes p that are possible candidates for factors of N. The more representations of N in linear forms of the type (*) that are available, the further the restriction on the prime numbers p, $p < \sqrt{N}$, that are possible candidates for being factors of N. Tables of linear forms for representing any number N as in (*) can be

[4] As for odd perfect numbers, it not yet known if any such exists, but none has been found for values up to 10^{300}. See [Brent *et al.* 1991; Guy 1994, 44-45].

prepared in advance and these provide an extremely useful tool for factorization processes.

Both Legendre and Gauss wrote very influential textbooks that summarized the state of the art in the discipline and that shaped much of its subsequent development. More than Legendre's treatise [Legendre 1798], it was Gauss's monumental *Disquisitiones Arithmeticae* of 1801 that represented the first great codification and systematization of number theory at the beginning of nineteenth century. It presented for the first time in a truly systematic fashion a great amount of results that were theretofore seen (even in Legendre's first edition) as a somewhat haphazard collection of separate problems and diverse techniques. It had a momentous influence over what the discipline of number theory would become over the nineteenth century and beyond, but this influence acted in many, diverging ways [Goldstein & Schappacher 2007a]. Intensive calculations with individual cases were devoted only little attention in Legendre's book and not at all in Gauss's. Subsequent developments on activity related to Mersenne numbers and their possible factors has to be seen against the background of the processes unleashed in number theory by the publication of *Disquisitiones Arithmeticae,* and by the ways in which these processes left only little room for intensive computations as a main task in the discipline (more on this below).

And indeed, the person who appears next in our story, as the main contributor in the last third of the nineteenth century to calculations related with Mersenne numbers was not at the mainstream of academic mathematics of his time. He is Édouard Lucas (1842-1891), whose name continues to be associated to this day with the algorithm for testing the primality of Mersenne numbers, about which more is said below. It was only relatively

recently, however, that more focused attention was devoted to his research as an object of historical interest, as we see in the illuminating accounts of Hugh Williams [1998] and, from a somewhat different perspective, of Anne-Marie Décaillot [1998, 2002].

After graduating from the École normale supérieure Édouard Lucas worked at the Paris observatory, as assistant to Urbain Le Verrier (1811-1887), best known for the calculations that led to the discovery of Neptune. Then he was artillery officer at the Franco-Prussian war of 1870-71, where he distinguished himself in the battlefield. After the war Lucas worked in various French *lyceés*, first in Moulins and then in Paris. Lucas' interests covered various fields of mathematics such as astronomy, geometry, combinatorics and, above all, number theory. He published dozens of articles on these topics, which were mainly short research notes generally appearing in relatively minor journals. Much of his mathematical activities were associated with the *Association française pour l'advancement des sciences* (AFAS), established in 1872 as a way to contribute to the moral recovery of their country after the war. Lucas also published a textbook on the theory of numbers [Lucas 1891] (a rarity in French mathematics at the time) and a four-volume book that became a classic: *Récréations mathématiques*. Among other things, Lucas is well known for the invention of the Tower of Hanoi puzzle [Williams 1998, 57- 65].

His important contributions to questions of factorization and primality testing were developed during a relatively short time he devoted to investigating this field of arithmetic, 1875 to 1880. Curiously, among the original motivations that led Lucas to his interest in number theory and particularly on prime numbers, questions related to industrial fabrics are prominent. He found interesting ways to apply Gauss's theory of

congruences to the construction and classification of fabrics with a rectilinear weaving, by representing the latter as drawings on cross-ruled paper. In fact, Lucas even formulated a new proof of the reciprocity theorem using weaving-related concepts [Lucas 1890]. Lucas took direct inspiration from Fermat's works and, among other things he became interested in what is nowadays called pseudo-primes, i.e., integers that satisfy sufficient criteria of primality but are not themselves prime. For Lucas, the most important such criterion was the one deriving from the so-called Fermat's little theorem, which states that if p is a prime number, then for any number a not divisible by p one has $a^p \equiv a \pmod{p}$. Lucas used a variant formulation of Gauss, which states that:

(G) If p is a prime number which does not divide a and if a^t is the smallest power of a for which $a^t \equiv 1 \pmod{p}$, then t divides p -1.

Lucas was aware of the fact that the converse of this theorem is not generally valid, as he showed in the following example: $2^{37\cdot 73-1} \equiv 1 \pmod{37\cdot 73}$. He then also formulated in 1876 a kind of converse for Fermat's theorem, namely:

(Lu1) If a and p are relatively prime, and if $a^x - 1$ is divisible by p when $x = p$-1 and is not divisible by p when x is any divisor of p-1 other than p-1, then the number p is prime.

Lucas investigated the primality of large numbers by looking at the sequence of Fibonacci numbers, for which he proved several results. Let u_n be the nth number in the sequence of Fibonacci numbers, and d divides u_n; then d is called a proper divisor of u_n if d does not divide u_r, for any r such that $1 < r < n$. From the table of Fibonacci numbers and its divisors Lucas discovered the following two properties:

(Lu2) If $n \equiv \pm 3 \pmod{10}$ and n is a proper divisor of u_{n+1}, then n is prime.

(Lu3) If $n \equiv \pm 1 \pmod{10}$ and n is a proper divisor of u_{n-1}, then n is prime.

He presented various successive proofs of this, each of which turned out to be mistaken in its own way. The result was correctly proved only in 1913 by Robert Daniel Carmichael (1879–1967). At any rate, when Lucas first published it in 1876, he added a very significant comment, namely that a result like this allows determining if a number is prime or composite, "without making use of a table of prime numbers", and indeed, *without having to perform a large number of trial divisions*. In particular, he thought to have proved in this way the primality of $M_{127} = 2^{127} - 1$, a number of the form $10p - 3$. In order to do so, he said, he had verified that u_k is never divisible by numbers $A = 2^n$, except for $n = 127$.

For reasons of space, the details of Lucas interesting calculations cannot be given here. Still, for the purposes of the present account, it is necessary to mention some of the main ideas related with it. Let v_n be defined as $v_n = u_{2n}/u_n$. Lucas proved another, related result as follows:

(Lu4) Let p be an odd prime and suppose $p \mid v_{2^n}$; then $p \equiv \pm 1 \pmod{2^{n+1}}$.

It follows from here that in order to show that M_{127} is prime, it suffices to show that $M_{127} \mid v_{2^{126}}$. Notice again: the primality of M_{127} is determined, not by checking whether or not this number *is divided* by certain factors, but rather by checking whether or not the number itself *divides* another, specified number (which itself is typically very large). This is the core of Lucas innovation. It reduces enormously the amounts of operations to be

performed for testing an individual number, but not the complexity (and length) of the specific computations involved in that case.

If we write now $r_k = v_{2^k}$, what Lucas had to show is that $r_{126} \equiv 0 \pmod{M_{127}}$. Now, M_{127} is a 39-digit number. Lucas needed to perform about 120 squaring operations and about 120 divisions involving numbers of that size. To help performing this exacting task he devised an original approach based on the use of a 127 × 127 chessboard. This approach significantly embodies a combination of Lucas' interest and motivations: a game-like spirit, his previous experience with mathematical analysis of industrial fabrics, and also his knowledge of Sylvester's anallagmatic chess-board, which Lucas had used previously to decompose numbers which are sums of squares [Décaillot 2002]. Lucas represented on the board the numbers investigated, for instance $r_{126} \times r_{126} \pmod{2^{127}}$, by using a binary notation in which a pawn in a square stands for 1, while an empty one stands for 0. The convenience of using this method in the context of Mersenne numbers derives from the fact that in their binary representation, they appear as strings of only 1's. To this binary representation Lucas applied an algorithm that reduces the arithmetic operations on the numbers to removal or addition of pawns and gradual reduction of lines on the chessboard, until only the upper row still contains pawns. Working in this way he performed the test for M_{127} in a time that is estimated between 170 and 300 hours. The last step in his algorithm indicated a result, according to the status of the pawns in the remaining line on the chessboard: M_{127} is prime. But Lucas had no permanent record of the many partial results on the way to this conclusion. Thus, even though he could trust his method in principle, and even though he had trained himself previously with lower values of n, to gain experience with the method, he could not be completely sure not to

have made any mistake in an intermediate step of his long procedure. He performed the entire computation only once, and hence his somewhat hesitant conclusion that "he thought to have proved" the result.

It should be noticed that Lucas's main focus of attention when developing these methods was the properties of primes in general and primality testing in particular, rather than, more specifically, Mersenne numbers as such. As he was looking for numbers for which his method would yield interesting result, M_{127}, turned out to have some desirable properties in terms of the applicability of result **(Lu3)**. Thus, one can look at numbers of the form $N \pm 1 = 2^k$, which would be easy to factor. On the other hand, $N = 2^k + 1$ prime implies that k is a power of 2, as Lucas certainly knew. Thus, $N \equiv 7 \pmod{10}$, and in such cases **(Lu2) - (Lu3)** are not easily used. Thus, it is more convenient to use numbers $N = 2^k - 1$.

This much said, there are various possible reasons to explain why, from all possible Mersenne numbers, Lucas chose precisely to use his method for testing the primality of M_{127}, but there is not enough evidence to decide [Williams 1998, 60-61]. One interesting point is that Lucas became aware of Mersenne's list only much later, after 1876, and that once he became aware of it he attributed an enormous importance to the list and considered it correct, on face value. Indeed, he assumed that Mersenne possessed certain methods that were meanwhile lost. In addition, as already remarked, the first mistake on Mersenne's list was spotted only in 1883. This happened when a Russian priest named Ivan Mikheevich Pervušin (1827-1900) communicated to the Academy of Saint-Peterburg that M_{61} is prime. The same result was independently found in 1886 by Paul Petter Seelhoff (1829-1896) and it was confirmed in 1887 by Jules Hudelot. Interestingly,

Lucas explicitly pointed out that in checking this result Hudelot had spent fifty four hours of calculations [Lucas 1887]. At any rate, Lucas was aware by 1887 of this mistake in Mersenne's list and nevertheless his conviction about the existence of a putative, unknown method possessed by the latter remained unshaken. In different places, Lucas came up with somewhat unclear and even contradictory statements about results (his own as well as other's) pertaining to Mersenne numbers and in particular concerning the primality of M_{67}. To summarize I would like to state that, while Lucas certainly proved correctly at least once the primality of M_{127}, it is possible that he may have proved that of M_{67} as well, but he was hesitant about it and we have no evidence to decide to what extent he did this correctly.

This is, then, the background against which Cole presented his factorization of 2^{67} -1 at the New York meeting of the AMS on October 31, 1903. The *Bulletin* of the AMS reports the names of the attendants to the meeting, and it is safe to assume that they knew very little of this story. The *Bulletin* does not report if, as Bell recounted, this was a silent presentation followed by a standing ovation, but it did publish a short note by Cole with details of his motivation and the method followed for finding the factors [Cole 1903]. Briefly stated, Cole relied on techniques such as introduced by Legendre and used existing tables of quadratic remainders based on representations of the form (*), a method that had been standard for factorizing for decades now. He discussed thoroughly the possible candidates of factors obtained with the help of this technique, together with some specific considerations for the case in point, and gradually focused on a reduced number of candidates which he tried one by one until he found the result. Cole was aware of Lucas' announcement that $2^{67} - 1$ and 2^{89} -1 are composite, and he was also aware of

Seelhof's result of 1886. Most probably, he was not fully aware of Lucas' method and of his hesitations, and certainly not of Lucas' reasons for the latter. But from his description of how he reached his result it is clear that he relied strongly on a wealth of theoretical considerations about the properties of primes of various specific forms and that such considerations led him to reduce to a manageable size the range of possible values to be take into account as possible factors. From all we know, the calculations he did, whether they took three years of Sunday afternoons or not, were done manually and without the aid of any mechanical device. It will be almost fifty years before the next instance of a Mersenne prime would be found. This happened only after digital computers were used to solve number theoretical questions. I will retake this thread below in section 7.

Before concluding this section, however, it is necessary to mention that the search for Mersenne primes and, more generally, for techniques of primality testing, led to the development of mechanical devices specifically conceived for these specific kinds of tasks. Indeed, we have already seen the very algorithmic spirit of Lucas' methods. Several engineers found out that these methods could be embodied in a series of ingenious devices that could turn the necessary calculations into mechanized tasks. The earliest announcement of the ideas of such a machine dates from 1887 when Lucas himself mentioned the work of the engineer and inventor Henri Genaille on an Arithmetical Piano that could be used for finding instances of Mersenne primes. It is quite possible that this machine was never built. For reasons of space I will not describe here the various attempts to construct such devices following the publications of Lucas' methods. Suffice it to say here that when DH Lehmer came up in 1932 with his photoelectric sieve he was just one more link on an interesting chain of inventors that,

working essentially on the margins of the great traditions of research in number theory, undertook to develop mechanized procedures for discovering individual instances of prime numbers in general and of Mersenne primes in particular [Williams 1998, 141-168]. At the same time it is important to stress that some further results were obtained by rude-force calculation. M_{89}, for instance, was found in 1911 to be prime by a railroad employee named R.E. Powers, who used a plain calculating machine. Powers also showed in 1914, using the same method, that M_{107} is prime while M_{103} and M_{109} are composite [Powers 1911; Powers 1914].

3. Irregular Primes

A second perspective from which to consider the question of computations in number theory is the one afforded by "irregular primes".[5] Regular and irregular primes were identified by Kummer in the 1840s in connection with his work on the problem of higher reciprocity and with some attempts to prove FLT. Calculations of individual cases of irregular primes became subsequently associated with the proof of individual cases of the latter conjecture. Indeed, in 1850 Kummer proved that FLT is valid for all regular primes and in 1857 he proved that it is valid for all irregular primes (and hence all powers) under 100. (Curiously, though, Kummer never coined any term to denote this special case of primes.)

[5] This section summarizes material that I have discussed at greater detail in [Corry 2008a].

Kummer's ideas are interestingly related to a discussion held in 1847 at the Paris Academy. Participants in this discussion were several prominent mathematicians, including Gabriel Lamé (1795-1870), Augustin Louis Cauchy (1789-1857) and Joseph Liouville (1809-1882). The discussion turned around a possible proof that had been suggested for FLT, which was based on representing a sum of integers as a product of complex numbers, as follows:

$$x^p + y^p = (x + y)(x + ry)(x + r^2y) \ldots (x+r^{p-1}y) \qquad (**)$$

Here p is an odd prime number, and r is a complex number called a primitive p^{th} root of unity, namely, a number that satisfies the condition: $r^p = 1$ and $r \neq 1$. A domain of complex numbers generated by a p^{th} root of unity is called a "cyclotomic field", $k(\zeta_p)$. The strategy was to start from (**) and to apply the method of "infinite descent" in order to lead to a contradiction that would prove the theorem. Now, a fundamental property of the integers is that when one factorizes an integer number (or an expression involving integers like the left-hand side of (**)) into a product of primes, this can be done in an essentially unique way. An implicit assumption behind this intended proof was that this condition of uniqueness is satisfied also when the numbers in the right-hand side of (**) are "prime integers" (in a well-defined sense) within $k(\zeta_p)$.

Several years prior to that, however, as part of his research on higher reciprocity, Kummer had investigated the behavior of cyclotomic fields and he was aware that this assumption is not generally valid for such domains. On hearing about their intended proof, he wrote to Liouville informing that in 1844 he had already published a counterexample to that assumption. He also wrote that his new theory of "ideal complex numbers" restored a somewhat different kind of unique prime factorization into these

fields. Also the idea of regular primes was associated with his research on cyclotomic fields.

The basic definition of a regular prime is quite complex and of little practical value when it comes to identify individual primes as regular or irregular. It is based on the concept of "class number" h_p of a cyclotomic field $k(\zeta_p)$, a number which provides a "measure" of the failure of unique factorization of integers in that domain. Thus, the prime number p is said to be regular whenever p does not divide h_p. Calculating class numbers may be a difficult task, but fortunately Kummer very soon found a surprising, and much more operational criterion for allowing the identification of regular primes, this one based on the use of so-called "Bernoulli numbers".

The Bernoulli numbers appeared for the first time in 1713 in the pioneering work of Jakob Bernoulli on probabilities, and thereafter in several other contexts. Euler, for instance, realized that they appear as coefficients B_n of the following Taylor expansion:

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

He was also the first to calculate actual values of the coefficients. There are also several, well-know recursion formulas to calculate them. Given that for all odd indexes n greater than 1, $B_n = 0$, I follow in this article a simplifying convention, namely, to consider only even indexes.[6] In these terns, the first few values of B_n are:

$B_1 = 1/6$

[6] This convention was normally used by Vandiver and the Lehmers, whose work I make reference to here.

$B_2 = -1/30$

$B_3 = 1/42$

$B_4 = -1/30$

$B_5 = 5/66$

$B_6 = -691/273$

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.

Kummer developed his ideas on ideal complex numbers and on irregular primes as part of his own involvement with arduous calculations with individual cases of products and factorization with number in cyclotomic fields. Meticulously drafted tables that were preserved in his archives provide clear evidence to this. Thus, for instance, it is known that the lowest case for which unique factorization fails in the cyclotomic fields $k(\zeta_p)$, in cases like (**) above, is $p = 23$. Kummer obviously had made extensive and difficult calculations with numbers of all kinds before coming to realize that a case like this one may arise at all. Using the values of B_n known at the time, he worked out all the computations necessary to see that the only non-regular primes he found below 164 were 37, 59, 67, 101, 103, 131, 149, and 157. He did not go beyond 164, possibly because of the complexity and length of the calculations involved. On the other hand, for all irregular primes under 157, he found that the class number was divisible by p only, whereas for $p = 157$, the class number is divisible by 157^2 and then again not by 157^3. This result had important consequences in his treatment of FLT for powers which are irregular primes.

Kummer initially believed that there would be infinitely many regular primes and that, in turn, only a few primes would be irregular. That this is not exactly the case became clear many decades later, as will be seen below. After he proved FLT for regular primes in 1850, he naturally asked himself how to go about the case of irregular primes. He brilliantly developed three criteria that provided a sufficient condition for the validity of FLT for any given irregular prime p. Checking these criteria for a specific p involves a considerable computational effort, but they do yield clear results. Kummer was by no means the mathematician to be intimidated by the need to make the necessary calculations. And indeed, in 1857 he published a famous article that broke new ground, both conceptually and in terms of specific calculations. It introduced the three said criteria and proved that each of the three irregular prime smaller than 100 satisfies them. He thus achieved the very impressive result that FLT is valid for all exponents under 100.

It is noteworthy that Kummer never published his calculations nor explained any specific formula that perhaps facilitated these calculations. But clearly, the latter were lengthy and demanding. Indeed, Kummer's work turned out to contain some relatively minor inaccuracies, but this was found out for the first time only in 1920 by Harry Schultz Vandiver (1882-1973). It was clear by 1856, at any rate, that Kummer's results might be extended with additional calculations involving Bernoulli numbers. This would require, in the first place, to add new values to the list of known ones, and this is a main point where intensive calculations for table-making enter the story.

It is important to stress, that given Kummer's willingness to undertake extensive and detailed computations, and given his full domain of the theoretical aspects of the problem at hand, his results on FLT can be taken to indicate the material limit to which this

approach could be extended at that time. Relatively few new Bernoulli numbers were computed in the following decades (see next section) and when they were computed, the motivation never came – before Vandiver and his collaborators – from number theoretical concerns (certainly not from attempts to deal with FLT). Very much like in the case of Mersenne numbers, this situation in connection with irregular primes 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.

4. Number Theory and Electronic Computers

Having presented in the two previous sections the early stages of the history of calculations of specific values of Mersenne primes and irregular primes, I jump now directly to the late 1940s, when the first electronic computers made their appearance. Some classical problems in mathematics were soon seen as a challenging test for the computing power of the new machines as well as for the programming skills of those in charge of operating them. A well-known, remarkable early instance of this came as early as 1949, when John von Neumann (1904-1957) suggested that ENIAC might be used to calculate values of π and e up to many decimal places. Von Neumann was interested in questions of randomness and particularly in the developing possible tests for checking randomness, and the decimal expansions of these two numbers seemed to offer useful instances of random sequences of integers where such test could be initially tried [Reitwiesner 1950].

More closely related with the topic of this article is the case of Alan Turing (1912-1954) who in 1950 became involved in the development and early use of the Mark I at Manchester and combined many of his previous mathematical interests as he applied the machine to investigating Mersenne primes and to the Riemann Conjecture [Booker 2006]. In fact, the first to explore the possibility of looking for Mersenne primes with the help of the Mark I was Turing's colleague Maxwell H. Newman (1897-1984), and Turing went on to develop and improve his ideas. No actual result came out of their efforts, however. The first instance of a new prime number identified with the help of an electronic digital computer came in 1951 when Jeff Miller and David Wheeler (1927–2004) used EDSAC at Cambridge to find several primes of the form $k \cdot M_{127} + 1$. Among them was the largest known prime at that time, $180(M_{127})^2 + 1$, a 79-digit number. This result was soon followed by the discovery in 1952 of several new instances of Mersenne primes by Raphael Robinson (1911-1925), about which more is said below.

The application of digital electronic computers to problems in pure mathematics and particular in number theory implied a less straightforward process, however, than it may appear at first glance. In the first place, the new machines were funded with very specific, and more mundane purposes in mind, such as the calculation of ballistic trajectories related with artillery. Obviously, administrators had little direct interest in allowing the use of expensive CPU time for solving esoteric problems with no visible, direct application. But limitations also came from the side of the mathematicians working in mainstream "pure" fields. Very often they showed little interest in exploring the possibilities opened for their disciplines by this new technology. This was the case even when they had themselves been involved in wartime efforts related with electronic

computers. Number theory, in particular, presents a very interesting case of reticence to the adoption of computers as a significant tool in the discipline, precisely because of a more general reticence to calculations with individual cases, as I already commented above. Of course, the very innovation implied in the use of electronic computers in terms of speed, accuracy and the magnitude of values that could be calculated, would gradually affect the attitudes of many and would allow for the incursion of this tool into the discipline. But the point I want to make here is that not only technological questions related with the computer itself and its development affected the pace of this process, but also other factors which I will mention in what follows.

To make the historical picture more concrete at this point, it is convenient to look now at various timetables related to specific calculations with individual instances of primes of various kinds. This provides a schematic summary of the changes in the intensity and attention accorded to mathematical activities of this kind throughout the years, and in particular of the slow adoption of electronic digital computers as a main tool for performing related tasks. Let us consider, first, the table of discoveries of Mersenne primes:

Year	Discoverer	Index
1558	Cataldi	17, 19
1772	Euler	31
1883 / 1886	Pervusin / Seelhof	61
1911 - 1914	Powers	89, 107
1876	Lucas	127
1952	Robinson	521, 607, 1279, 2203, 2281

I did not include in the table information about proofs of non-primality of certain cases or of calculations leading to the discovery of the factors of some specific cases.[7] Nor does the table provide information about many unsuccessful attempts of various kinds. And yet, even with these limitations the table shows an evident lack of linearity in the discovery of new instances, and this cannot be explained simply by the passage of time. The large gap between 1914 and 1952, for instance, is obviously related to the introduction of electronic computers. But the availability of electronic computers does not in itself explain when and how they were adopted, why some other devices of mechanical calculations were not successfully adopted before for the same calculation, and why Mersenne primes, and not other kinds of numbers, were calculated at earlier or later times. That additional explanations are necessary is more clearly manifest when looking at the timetable of calculations related with irregular primes, which appears here:

Year	Discoverer	Result
1850	Kummer	Irregular primes up to 157
1915	Jensen	Infinitness of irregular primes
1930	Vandiver	Irregular primes up to 293
1939	Vandiver, Lehmer, Lehmer	Irregular primes up to 619
1954	Vandiver, Lehmer, Lehmer	Irregular primes up to 2000
1955	Vandiver, Selfridge, Nicol	Irregular primes up to 4002

[7] For some additional information see

http://primes.utm.edu/mersenne/LukeMirror/biblio.htm#lit_012.

Why did no one after Kummer and before Vandiver calculate new values of irregular primes? What led Vandiver and the Lehmers to be involved in such calculations between 1930 and 1939? Why didn't they adopt electronic computers earlier to continue their previous calculations? Why did it take so long before Jensen's result of 1915 and in what circumstances did he pursue the research that led to it? Similar questions will arise when looking at the respective table of Bernoulli numbers:

Year	Discoverer	Result
1840	Ohm	Up to B_{31}
1878	Adams	Up to B_{62}
1907	Serebrenikov	Up to B_{92}
1936	Lehmer	Up to B_{196}
1953	Lehmer, Lehmer	Up to B_{214}

There is a clear relation between Lehmer's work on Bernoulli numbers and on irregular primes for FLT. But as will be seen below, his calculations with Bernoulli numbers were not obviously received as a result that deserves attention. Lehmer was intensively involved in number theoretical calculations from an early stage in his career and, after a short experience with ENIAC, he was among the first to use electronic computers for number theoretical questions. In this sense his work offers an interesting perspective on the issue of the changing attitudes of mathematicians to mass computations with individual cases in number theory. I explore this work in the next section.

5. The Lehmers, Vandiver, and FLT

DH Lehmer 's overall mathematical conceptions and outlook were strongly influenced by those of his father, Derrick Norman Lehmer (1867-1938), who was professor of mathematics at Berkeley and had a great interest in computations and aids to computations. In 1909 DN Lehmer 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]. DN Lehmer had very strong opinions about the experimental character of mathematical research, and accorded a central role to tables in general. He stated such views as follows [Lehmer DN 1914, *vi*]:

> 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.

In 1929 he came up with an innovative method of mechanizing factorization processes based on the use of *Factor Stencils* [Lehmer DN 1929]. The basic idea behind the use of the stencils was to mechanize part of the process involved in Legendre's approach to finding candidates for factors, as explained above. The stencils embodied a 100 × 50 matrix on which quadratic residues of all primes up to 5000 were represented by means of punched holes. Taken together, this allowed for gradual elimination of possible candidates for being factors of a given number *N*, by reference to the stencils representing

its quadratic residues. Technically, the reduction was done by stacking on top of each other the stencils selected for a given *N*. The stencils were provided with a box having a glass cover. An electric light was introduced into the box so that light would shine through the holes, thus revealing the possible candidates for the given *N* [Williams 1998, 142-144].

In developing the stencils projects DN Lehmer was assisted by his son, Dick, as well as by his student Emma Trostakya (1906-2007), who would soon become Dick's wife and mathematical partner of a lifetime. DH Lehmer inherited many of the abilities of his father as well as the latter's interest in number theory and in mechanized computation. In 1932 DH Lehmer constructed, now with his father's help and encouragement, the highly ingenious photoelectric number sieve that was already mentioned above. This was a rather sophisticated improvement of earlier sieve he had built as an undergraduate, based on a set of bicycle chains hanging on sprockets attached to a shaft and turned by an electric motor [DH Lehmer 1933]. The photoelectric sieve required a rather complex setup before it could be used for each new separate case. Thus, in spite of its promise and the interest it aroused even in extra-mathematical circles, it was never really put to use. In building his next sieve in 1936, DH Lehmer paid much more attention to its ease of use as a main guideline for design and implementation. This was a variation of his first sieve, but the bicycle chains were replaced by loops of 16 mm movie film leader. This sieve had many of the desired advantages over the previous models, but nevertheless it did not become a device that was consistently put to use. Starting in 1945, DH Lehmer and Lemma became involved with electronic computers, such as ENIAC and SWAC, and used them, as will be seen below, as arithmetic sieves. And yet, interestingly enough, DH

Lehmer continued to construct special-purpose sieves similar in their basic architecture to his earlier ones. Thus for instance, in 1965 he built a Delay Line Sieve which he continued to use until 1975 for factoring and for studying the properties of certain integer sequences [Williams 1998, 192-195].

Side by side with the construction of these mechanical devices, DH Lehmer also devoted much attention to the theoretical side of his interest in numbers. In 1930 he finished his doctoral dissertation were he improved Lucas' methods. The dissertation presented what became known as the famous Lucas-Lehmer primality test for Mersenne numbers. DH Lehmer obtained his degree at Brown University, under Jacob D. Tamarkin. Emma was awarded there her M.Sc. at roughly the same time. Emma, it is interesting to point out, 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].

Emma and DH Lehmer moved to Lehigh in 1932 and it is there that they started a long-standing collaboration with Vandiver. Vandiver's personal and professional story is an interesting one, as he was the only mathematician in history whose *entire* professional life was devoted to solving FLT [Corry 2007]. He was a high-school dropout and a self-styled autodidact whose choice of problems and research agenda sensibly diverged from

the mainstream of number theory. One should keep in mind that after Kummer's work on FLT it was possible in principle to continue the search for irregular primes. For each new irregular prime found, one might check if Kummer's criteria applied. Also, as it was clear from the beginning that the criteria he developed could not account for all cases, there was also room for refining and further elaborating criteria of this kind, in order to find more efficient tests for proving FLT for a given prime irregular exponent. Nevertheless, very little research was done in this direction in the following decades, thus reflecting the rather marginal status of FLT in the overall panorama of number theory [Corry 2008a]. More concretely, the important result that there are infinitely many irregular primes was proved by Jensen only in 1915. To be sure, the proof of this result did not contain any conceptual innovation and it was published by an unknown student in a remote Danish journal [Jensen 1915]. Moreover, the first report of this result in an English publication appeared only in 1928 [Vandiver and Wahlin 1928]. In choosing FLT as the main focus of his research agenda and in taking up where Kummer had left, Vandiver was following a path that had little in common with the mainstream of the discipline. This unusual choice can be explained, at least partly, by reference to Vandiver's original path in mathematics, and also by the lack of a strong community of number theorists in the USA during the early stages of his career.

Vandiver's first article on Fermat's Last Theorem appeared in 1914 in Crelle's *Journal* [Vandiver 1914]. Over the years, he continued to present short communications on FLT to the AMS containing, among others, improvements and simplifications of Kummer's criteria. In 1931 he was awarded the first Cole prize established by the AMS for outstanding research in number theory. This came in recognition to a series of works on

FLT summarized in a detailed article published in 1929 in the *Transactions of the AMS* [Vandiver 1929]. Up to this stage Vandiver was able to extend Kummer's results to a point where he proved the validity of FLT up to $p = 269$. Besides refining the Kummer-type criteria for proving the theorem in the case of irregular exponents Vandiver also worked on the side of the Bernoulli numbers. He proved several new congruences involving Bernoulli numbers in order to allow more efficient calculations related with the Kummer criteria and improved existing methods for calculating increasingly high instances of Bernoulli numbers. He also coordinated the work of various graduate students who would perform specific calculations for sets of cases that they were assigned. The students assisted themselves with then available electro-mechanical calculators. Vandiver also relied on existing mathematical tables of various kinds, but he systematically reassured the readers that these tables had been re-checked independently by comparing one with the other.

Within the small number theoretical community that worked in the USA at the time, Vandiver and Derrick Norman Lehmer were in close working and personal relationships. It is thus small wonder that when DH Lehmer and Emma had started their professional lives in the early thirties, with jobs scarcely available around, DN Lehmer established a contact between them and Vandiver. Vandiver had just been able to raise some funds with the American Philosophical Society for his FLT project and these were used to pay for the work of DH Lehmer and Emma [Corry 2008b]. An immediate concern addressed by the Lehmers related to the improvement of the recurrence formulae for calculating Bernoulli numbers. DH Lehmer devised a new method based on "lacunary recurrence", namely, one in which only some of the previous values are used for calculating each new

one [Lehmer 1935]. He took as reference existing tables of Bernoulli numbers and applied his newly developed method to check, in the first place, that the results coincided. Then, he went on to calculate values of up to B_{196}.

It is remarkable how early the Lehmers became clearly aware of the requirements that a properly implemented computing procedure should comply with. For example, in their correspondence they continually raise concerns about the degree of efficiency of the methods used for calculations, the estimated timings, the reliability of the results, and, no less than that, the clarity of presentation. In a letter to Vandiver in 1934, for instance, DH Lehmer wrote:[8]

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

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

But it is clear that the most pressing concern that arose in connection with this research pertained to the matter of publication itself: who would want to publish this kind of results and what exactly should be published? What tables? How many results for each

[8] DH Lehmer to Vandiver: November 20, 1934. This and following letters are kept in the Vandiver Collection, Archives of American Mathematics, Center for American History, The University of Texas at Austin (hereafter cited as HSV). They are quoted with permission of the CAH.

case? As a matter of fact, DH Lehmer understood that the very task of calculating new values of Bernoulli numbers was not one that his mathematical colleagues would hold in high esteem. He thus opened his 1935 article by trying to justify the task itself. He thus wrote [Lehmer 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 calculations. It is true that for the ordinary purposes of analysis, for example in the asymptotic series of Euler MacLaurin summation formula, a dozen Bernoulli numbers suffice. There are other problems, however, which depend upon more subtle properties 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.

Still in connection with this issue, it should also be noticed that the actual values he calculated were published in the *Duke Mathematical Journal* [Lehmer 1936], that had then only started to appear. This choice was not accidental and it had to do with the contents of the article and the reactions it elicited. As DH Lehmer wrote to Vandiver:[9]

> 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.

Solomon Lefschetz (1884-1972) was at the time president of the AMS and editor of the prestigious *Annals of Mathematics*. His reported reaction merely hints to the much broader and complex phenomena of the status within the mathematical community (in the

[9] DH Lehmer to Vandiver: February 10, 1936 (HSV).

USA and elsewhere) of mathematical tables, their elaboration and publication (more on this below). Evidently, Vandiver and the Lehmers had their own ideas about matters of this kind.

The first article published by Vandiver and the Lehmers also appeared in *Duke*. It established the validity of FLT for all exponents p, $2 < p < 619$, except possibly for 587. The latter case raised some computational difficulties which were nevertheless overcome very soon [Vandiver 1939]. It was also clear by this time, that above 619 the calculations became prohibitively long and laborious for being carried out with a desktop calculator.

The early collaboration between Vandiver and the Lehmers was interrupted at this point and it would resume only in 1952. There was, of course, a world of difference between the two stages of this collaboration, clearly separated from each other by the war and its aftermath and, in particular, by the introduction of electronic computers. In section 7 the story of this collaboration will reappear as one component of the Lehmer's broader computational activity in number theory. Before reaching that, however, I describe in the next section some significant contemporary processes that shaped the context within which this activity took place in its various stages.

6. Traditions and Institutions in Number Theory

In the foregoing sections, I have pointed out several times that the mathematicians involved in massive calculations with individual cases were mostly working at the margins of the mainstream and away from the leading centers of the discipline. In this section I would like to elaborate on this point, and to explain the importance of this issue

as part of the present story. In doing so, I will also refer to communities of researchers and to academic and governmental institutions and initiatives, as factors that significantly contributed to shaping research agendas in number theory.

I return briefly to the aftermath of the publication of Gauss's *Disquisitiones*, which I defined above as a watershed in the history of the theory of numbers. One of the most salient threads that is clearly discernible in the history of the discipline is the one that led from *Disquisitiones* to the work of Kummer, to the creation of the theory of fields of algebraic numbers with Kronecker and Dedekind, and from there to a significant peak at the turn of the century with Hilbert's *Zahlbericht*. This thread involved a highly abstract and sophisticated approach which, as already stated, attributed very little interest to computations with specific cases. Another thread that developed in parallel is the one in which analytic tools become prominent and that led through the work of Peter Lejeune Dirichlet (1805-1859) to the rise of the analytic tradition in number theory (of which very little is said here).

From a broad historical perspective, the works associated with these two main threads are those that can be more prominently associated with achievements of long-standing impact in the discipline of number theory as it developed from the mid-nineteenth century on. It is important to point out, however, that in their early stages, the ideas related to both the analytic and the algebraic thread in number theory attracted relatively little attention. It is well know, for instance, that Dedekind's theory of ideals was hardly read at the time of its publication, both in its various German versions and then in its French translation of 1876-77. Number theoretical questions did attract the attention of large audiences in the second half of the nineteenth century, but in ways different to those that became

prominent in the discipline under the influence of Hilbert's *Zahlbericht*. The scope of the ideas discussed in *Disquisitiones* was so broad and thoroughgoing that it led to a complete reorganization of the entire field around several clusters of interest and activity with relatively little intercommunication with each other, as Catherine Goldstein has clearly showed in her recent historical research. Based on a detailed analysis of citation networks manifest in the leading German review journal of the nineteenth century, the *Jahrbuch über die Fortschritte der Mathematik*, between 1870 and the First World War, Goldstein identified groups of mathematicians who shared common interests within number theory, used similar techniques in their research, and pursued similar objectives. As a rule, mathematicians associated with each of these clusters published in the same journals and quoted each other, thus giving rise to essentially self-contained areas of research. The algebraic and the analytic threads in number theory evolved from two such clusters but in their early stages they were not as dominant as they later became. Quantitatively speaking, most of the actual activity in number theory during the second half of the nineteenth century was connected to neither of them [Goldstein 1994; Goldstein & Schappacher 2007b, 71-74]. Lucas's works and those closely associated with it were part of a very prolific cluster of activity that, without having evolved later on into a full-fledged school of mathematical research and teaching, attracted many practitioners and produced many remarkable results.

This cluster of activity focused on questions directly connected with some of the basic topics discussed in Gauss's *Disquisitiones*, such as reciprocity, and cyclotomic and Diophantine equations. Massive calculations with individual cases and table making found a natural place here. Its contributors 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. They explicitly avoided the use of techniques involving algebraic and complex numbers or analysis. Still, some of them comprised very ingenuous and innovative ideas, appearing mostly in the work of the more prominent mathematicians that contributed here. The latter included James Joseph Sylvester (1814-1897) and Angelo Gennochi (1817-1889), and also Lucas was one of them. The case of Lucas offers an interesting example, as he can be taken to be a representative figure of arithmetical research in France in the second half of the nineteenth century. As I already suggested above, he was essentially marginalized from the elite French academic milieu. The journals in which he published were not the leading ones, and his topics of interest were mainly neglected by the leading mathematicians of his time. In fact, the case of Lucas is indicative of a more general trait of number theory in the last third of the nineteenth century within French mathematics at large, being a field of activity that received scant attention at the top research institutions before 1910 [Gispert 1991, 86-91 & 158].

A clearly discernible line connects Lucas, as well as other contemporary mathematicians pursuing similar agendas in number theory, with mathematicians like Vandiver and the Lehmers in the early twenty century. This is true in relation with the contents of their research as well as with their methodological preferences (including massive calculations with individual cases). This is also true in relation with their venues of publication,

typically not among the main journals of the profession (at least in part of their careers). Furthermore, this is also true in relation with the kind of professional community to which they belonged (this is also the case for Jensen who, as already mentioned, was a Danish graduate student working far away from the great centers of German and French number theory, who published on a local journal and whose work became known only much later). Vandiver was autodidact and – for that reason among others – strongly independent-mindedly when it came to problem choice. Also the Lehmers had, as already mentioned, very *sui generis* careers, and their horizons of mathematical interests were shaped with little influence of the dominant European centers. More broadly speaking, the number theory community in the USA was, as already hinted, rather small, somewhat apart from the main national centers of the time, and it comprised few prominent names. Besides Cole, Bell, Vandiver and the three Lehmers, the list of American mathematicians with some kind of significant contributions in number theory prior to 1939 is more or less exhausted by adding that of Carmichael (mentioned above), as well as the following: Hans Frederik Blichfeldt (1873-1945), Leonard Eugene Dickson (1874-1954), Aubrey Kempner (1880-1973), and Albert Cooper (1893-1960). Not all of them would identify number theory as their main field of activity.

It is interesting to notice, however, that the situation of the number theory community in the USA changed dramatically after the rise of the Nazis to power in Germany, which brought an enormous influx of mathematicians and in particular a handful of leading number theorists that went on to change the face of the discipline in the country. Claude Chevalley (1909-1984) arrived in 1938 and, following the outbreak of war, he remained at Princeton and later at Columbia until 1957. André Weil (1906-1998) worked for

several years at Chicago and Princeton, and Carl Ludwig Siegel (1896-1991) at Princeton between 1946 and 1951, and their influence was felt for decades to come. Hans Rademacher (1892-1969) created a very active school at Pennsylvania. In 1940, Hermann Weyl (1885-1955) wrote from Princeton to Paul Bernays (1888-1977) that he was "trying to stimulate the dormant interest in number theory" in his new country.[10] Number theory started at this time its dramatic rise in the USA with strong contributions that can be seen as natural continuations of the traditions that had shaped research in the discipline in Germany (and also, though to a lesser extent, in France) after the publication of the *Zahlbericht*.

The more clearly computational approach that Vandiver or the Lehmers had followed for years had only a relatively minor influence on these developments. Still, parallel to these significant changes in the community, the Lehmers continued to carry on their own research agendas and to add new impetus to calculational methods in number theory. It goes without saying that this was strongly related to the appearance on stage of the electronic computer at the end of the war. But it is important to stress that the rise of the new technology does not in itself explain its very fast adoption by the Lehmers (and others) for research in number theory. Rather, additional – and somewhat contingent – historical circumstances were at play here. Indeed, the Lehmers had moved to Berkeley in 1940 as DH Lehmer was finally offered a position there, but in 1945 DH Lehmer was called to work at the ENIAC project at the Aberdeen Proving Ground. Most of Dick's time was devoted then to the task of computing trajectories for ballistics problems, but Emma and he used some of their available time over the weekends to work on questions

[10] Quoted in [Siegmund-Schultze 1998, 247].

related with number theory. Thus, for instance, by June of 1946, they had computed the multiplicative order of 2 mod p, for many primes numbers p, $p < 453871$. Later on they calculated values of so-called Fermat quotients, $(2^{p-1} - 1)/ p \bmod p$, for all primes numbers p, $p < 25000$ [Lehmer 1974]. Obviously, their scientific background provided a unique blend of knowledge in number theory with an inclination and unmatched experience with calculating devices. The presence of Emma was no doubt decisive. She had no formal duties with ENIAC, and had the time, knowledge and availability to think about the possible uses of the new technology in her field of interest. This period of time afforded, above all, the crucial training in programming techniques and in the basic acquaintance with the new technology. But when the time came to return to California, where no similar devices were available at the time, this entire experiment may have been put on hold for an undetermined period of time were it not for a series of initiatives that developed in the postwar era in the West coast on matters related to applied mathematics and which created interesting new opportunities that the Lehmers were quick to become involved with.

The Lehmers' involvement with ENIAC at the end of the war had been but one instance of a much broader process whereby scientists of all specialties, mainly mathematicians, gained experience and interest in electronic computers. This gave a tremendous impulse to a phenomenon that antedated the war, whereby increased demand for facilities of mass data processing was felt at both universities and government institutions. University authorities in institutions like UCLA, Berkeley and Stanford took steps to contact industry leaders, such as IBM's Thomas Watson, to procure for themselves equipment donations and to create local computing centers. The most important of these initiatives

came in April 1946 from the National Bureau of Standards (NBS) as it intended to create a laboratory for mathematical computation in one of the leading universities of the West coast, partly funded by the military. After a somewhat nasty competition and lobbying among the three universities, the decision was reached in July of 1947 to establish at UCLA an Institute for Numerical Analysis (INA), that started it operations by the summer of 1948. A main figure at INA was Harry Huskey, who designed and led the construction of SWAC, the Standards Western Automatic Computer. SWAC became active in 1950, and at that time it was the fastest computer in the world. Huskey had previously worked with Alan Turing in England, and had also 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. Besides its purely technological assets the SWAC project 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].

Personal and political circumstances played now a role in helping materialize the connection between the Lehmers (and hence number theory) and SWAC. In 1949 all university employees at Berkeley were required to sign a new oath of loyalty to attest nonmembership in organizations that advocated the overthrown of the government, particularly in the Communist party. This requirement, which was part of a broader phenomena commonly associated with the McCarthy era, gave rise to a passionate controversy and to the dismissal, in August of 1950, of twenty-four faculty members who refused to sign. They were only reinstated by the end of 1952 after the California Supreme Court declared the oath unconstitutional [Moore 2007, 119-136]. DH Lehmer

initially refused to take the loyalty oath, and he finally signed under duress. But he took leave of absence and it was quite clear that he would not return unless the controversy would be settled satisfactorily. But contrary to other members of the faculty, losing his position at Berkeley would not become as acute a problem for him as it was for many others. Indeed, at the very early stages of the negotiations for creating INA, DH Lehmer had been contacted as a possible candidate for directing it, and now, in 1951 he was invited to become director [Moore 2007, 107-116]. In this capacity he was able to devote significant computer resources of SWAC to problems in number theory, as will be described in the following section.

A last, related point I would like to discuss in this section concerns professional journals and venues of publication. In the previous section it was seen that mathematical tables and, more generally, results related to computations with individual cases (such as new values of Bernoulli numbers), did not find a natural and self-evident place in leading mathematical journals at the time. DH Lehmer published some of his early results in the *Duke Mathematical Journal* which was then in its beginnings, and this was certainly not his preferred choice. Many results of the joint work with Vandiver were published in the *Proceedings of the National Academy of Sciences*, which, as Vandiver wrote to Emma, "has a rule to the effect that any member presenting a paper for publication … is entitled to have it published".[11] This lack of suitable venues was solved by the foundation of a new journal, outside the mainstream mathematical establishment, willing to publish

[11] Vandiver to Emma Lehmer, October 30, 1953 (HSV).

material such as the Lehmers were producing. The interesting point is that with time the new journal became a highly prestigious journal of the AMS, *Mathematics of Computation*. I say a few words about this now.

I mentioned above that Kummer had produced elaborate tables of results related with his work on cyclotomic fields. These were not published as part of his work. In the first part of the nineteenth century, mathematical tables of various kinds were for some time published in leading venues such as the *Journal for reine und angewandte Mathematik* but very soon such journals were not considered anymore the right place for doing this. Tables as well as result related to computations with individual instances were confined to separate publications. In the last third of the nineteenth century the need for new and more accurate tabulated values of special functions became increasingly pressing for astronomers, engineers and physicists. Several initiatives were undertaken in order to cope with these needs and institutions were created as part of such initiatives. An interesting example of how table making was institutionalized came with the creation of the British Mathematical Tables Committee, under the leadership of James W.L. Glaisher (1848-1928) and the active participation of mathematicians such as Arthur Cayley (1821-1895) and Henry J.S. Smith (1826-1883), and the two leading British mathematical physicists, Sir William Thomson (1824-1907) and Sir George Stokes (1819-1903) [Croarken 2003].

Corresponding to the main motivations behind the creation of the Committee, most of the tables they compiled and published were devoted to functions of use in applied mathematical fields: elliptic functions, Legendrian functions and Bessel functions. 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. In 1873, factor tables of up to three millions were published and these were extended to nine millions in 1883. In 1899, the Committee supported the work of Allan Joseph Cunningham (1842-1928) and published tables of residues of powers of 2, to be used for testing divisibility, for factorizations, and for solving congruences to base 2. 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 and brought with him many technical, conceptual and organizational innovations to the Committee's activities [Croarken & Campbell-Kelly 2000, 50-52].

The Mathematical Tables Committee was a remarkable example of an institutional initiative that fulfilled a task that individual mathematicians typically left out of their agendas. The tables it elaborated were published only as large volumes that were updated periodically. This was the classical approach to table publication, and we have seen that it is the one followed by DN Lehmer for his own tables of prime numbers and related topics. But this was not a useful approach to follow when it came to tables that were too small or too specialized. In this regard, the Committee came up with an initiative, not before 1950, to actively collect unpublished mathematical tables and to deposit them in

the Royal Society Library [Croarken 1990, 251-256]. This was not the only place where such tables were deposited, and as was seen above, Lefschetz had also suggested Lehmer in1936 to deposit his tables with the AMS. As a matter of fact, the need to organize knowledge on existing tables had been felt since the end of WWI, and the USA National Research Council started back then a series of initiatives in this direction. In 1930 the council created a new Committee on the Bibliography of Mathematical Tables and Other Aids to Computation that would review not only existing mathematical tables but also existing computing machinery. After some delays and failed attempts a real leader for this project was found in 1939, who gave the necessary impetus to make it work. This was Raymond Claire Archibald (1875-1955), from Brown University [Grier 2001, Polachek 1995].

Archibald was essentially a historian of mathematics with a natural inclination to acknowledge the value of bibliographical work [Archibald 1948]. He had built a remarkable collection of about four thousand mathematical tables. The most significant step that Archibald undertook as chair was the founding in 1943 of the journal *Mathematical Tables and Other Aids to Computation* (*MTAC*), meant to expand the influence and scope of the Committee. The NRC did not initially support this initiative, but Comrie, who had been assisting the activities of the Committee form its inception strongly encouraged it, and his attitude proved crucial.

Archibald did most of the writing for the first two issues. In the introduction to the first issue he stated that the aim of the journal was "to serve as a clearing-house for information concerning mathematical tables and other aids to computation." Very soon the journal acquired a well defined style and structure. It always started with a series of

tables or reports on the work of computing groups. This was followed by a section on new published mathematical tables, errata for published tables, and a list of unpublished tables. In the same introductory note, Archibald wrote that during the past decade computation devices had "been vastly multiplied". Obviously, he was not speaking about high-speed electronic devices, but rather about a series of different kind of machines such as Vannevar Bush's Differential Analyzer, desk calculators then at use, the Burroughs Bookkeeping Machine, the Hollerith Multiplying Punch, and others which he later reviewed in the first issues of the journal.[12] Moreover, until recent times, large computational projects were still being conducted in the form of coordinated calculations involving large of groups of human computers with well defined tasks [Lowan, 1949, Grier 2003].

As the founding of this journal was nearly contemporaneous with the building of the first electronic computers it affords interesting insights to the complexity of the process of absorption of the new technology into the mathematical discipline and its institutions. In particular, it provides important contextual background to the use computers were put to use by the Lehmers in number theory. The Committee on High-Speed Computing Devices was established in 1946 by the NRC, with the participation of leading figures such as Von Neumann and Howard Aiken (1900-1973). The Association for Computing Machinery was established in 1947. Both institutions sought from very early on to collaborate with *MTAC*, and as a matter of fact, the ACM continued to use the *MTAC* as its main venue of publication until 1953. This was the only scientific journal in which the continued development of computing devices was steadily discussed, but the need for a

[12] See *MTAC*, Vol. 1, pp. 63-64, 96-97, 127-129, 165-167,

more specialized journal became gradually evident. The *Journal of the ACM* was founded only in 1954.

It is noteworthy that while the main aim of the Committee on High-Speed Computing Devices was to promote the development of new machine technology, their members also cared initially not to slow down in any way existing computing projects. But personal issues with some of the promoters of the ACM completely alienated Archibald from this new institution. In June 1949 he resigned the editorship of *MTAC* and DH Lehmer took the job. Lehmer edited the journal successfully but the entire conception of what computation is about underwent a deep transformation during the time of his editorship. Mathematical computation and the kind of pursuits embodied in *MTAC* became a relatively reduced part of the more general, emerging idea of computer science. Moreover, the traditional roles of mathematical tables gradually became obsolete, and thus the readership of *MTAC* was constantly reduced. Eventually the journal would become in 1960 *Mathematics of Computation*, under the editorship of Harry Polachek (1913-2002). Several professional societies expressed their interest in overtaking the responsibility for the journal, among them the Society for Industrial and Applied Mathematics (SIAM), the ACM and the AMS. But opinions within the AMS were quite divided on this issue, as a number of mathematicians considered that a journal devoted exclusively to computation was not a main interest of their society. It was only after much discussions and negotiations that the journal was finally transferred to the complete responsibility of the AMS in the third issue of 1965. In a retrospective account, Polachek summarized the processes undergone between 1959 and 1965 by the journal he had edited in the following words [Polachek 1995, 74]:

> The rapid expansion and the increased pace of research activity and publication in the field of mathematics of computation during this period is not surprising. This was the era when the field of computer science came to life. It was during this period that most of the larger universities began to acquire advanced high-speed computer systems and to establish computer science departments. By 1965, even the highbrow members of the American Mathematical Society, who earlier looked with some measure of disdain at any mathematical research that related to computation. now were more willing to accept research in this field as a challenging area of mathematical innovation. Thus during that year the prestigious American Mathematical Society took under its wing, to be published as one of its own regular journals, Mathematics of Computation. In so doing, it recognized the field of mathematics of computation as a bona fide branch of mathematical research.

In the next section I will describe the mathematical details of the calculations conducted by the Lehmers using electronic computers in relation with the question of the Mersenne primes. The actual historical significance of their activities will be now more clearly understood against the background of the institutional, technological, political, and disciplinary aspects just discussed in the present section.

7. The Lehmers, Robinson, and SWAC

The discussion in the previous sections allow us understanding the extent to which the tenure of DH Lehmer as director of INA, together with Emma's presence without a formal position, and combined with the availability of SWAC, represented a unique blend of unlikely circumstances under which number theoretical research with computational

methods implemented in high-speed electronic devices was systematic pursued at this early stage. In this section I discuss some of the details of this research, especially in connection with Mersenne primes.

As already stated, when SWAC became operational in 1950 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 [Huskey 1997]. It operated with words of 36 binary digits or, equivalently, 11 decimal ones. Being the person most directly involved in the actual programming of SWAC and in experimenting with specialized code, Emma found the binary character of the machine especially useful for storing number theoretical properties such as residuacy and primality. Problems involving powers of 2 were also easily manageable. In addition, the rate of 16,000 additions and 2,600 multiplications per second – "ultra-high speed" by the standards of the day – and the availability of an auxiliary storage provided by the drum opened new possibilities for the study of certain problems in number theory in which a material limit for calculation had been already exhausted. This was the case with both FLT and the Mersenne primes [E Lehmer 1956].

Three main classes of number theoretical issues were addressed with SWAC:

1. Specific problems for which the machine could provide a definite answer: factorizations, primality testing, solutions of a specific Diophantine equation.
2. Testing of open conjectures for large amount of cases and very high values.
3. Experimental problems useful in the design of strategies for theorem proving.

Concerning (3) Emma Lehmer gave only one example, and this referred to very specific problem, called the Jacobsthals' sums of Legendre characters. The numerical evidence furnished by SWAC, Emma said, "led to some theorems whose proofs were eventually worked out by the old-fashioned paper-and-pencil method". [13]

As for specific problems, primality testing was no doubt the most basic of all not only because of its intrinsic interest, but also because in handling all the other kinds of problems it was often necessary to know whether specific numbers under examination were prime or composite. One way to compactly store a table of primes was to have a string with zeros or ones, according to whether the corresponding number in the sequence of odd integers is prime or composite. A list of the thousand first primes occupied in this way fourteen words of memory, and, in addition, any number up to 1,000,000 could be easily tested in a few seconds by straightforward trial division of consecutive primes. In addition, more sophisticated tests would work for larger numbers of special forms, such as the Fermat numbers and the Mersenne numbers. Concerning Fermat numbers, in 1953 John Selfridge wrote a program that found the factors of F_{10} and F_{16} [Selfridge 1953]. This refuted an open conjecture, put forward by Lucas, according to which the numbers in the sequence $2 + 1, 2^2 + 1, 2^{2^2} + 1, \ldots$ are all prime [Lucas 1891, 354-355]. The result for F_{10}, on the other hand, corroborated an earlier result obtained also with SWAC, namely that this 363-digit number is composite. This latter result had been obtained by

[13] [E Lehmer 1956, 108]. Probably she was referring to [E Lehmer 1955]. See also [Robinson 1968].

Robinson, who also worked on the question of Mersenne primes about which I say more below.

The kind of number theoretic hypotheses tested with SWAC also tells an interesting story. Turing's work on the Riemann hypothesis at Manchester in 1945, mentioned above, was an improvement of his own earlier attempt of 1939 to use a differential analyzer that would calculate individual cases according to an idea introduced by Edward Charles Titchmarsh (1899-1963). This attempt was interrupted by the war and it later became obsolete with the advent of electronic computers. Before Turing would retake the thread with Mark I, Lehmer had made his own attempt in 1947 to implement the Titchmarsh approach working with ENIAC. Before the program he was working on was actually run, however, ENIAC was drastically modified and this program could not be run anymore on this machine. Then, in 1949, even before SWAC was completed, Lehmer had suggested the Riemann hypothesis for testing to J. Barkley Rosser (1907-1989), then director of INA. Rosser accepted it, but only as a low priority project. It should be pointed out that in 1939-40 Rosser and the Lehmers had a very interesting, fruitful, and largely forgotten interchange of ideas around FLT [Corry 2008a]. At any rate, only after DH Lehmer took his post at INA, actual work with SWAC on the hypothesis started. Lehmer developed sophisticated mathematical algorithms, and these were coded by Ruth Horgan, a main figure in the coding side of the SWAC project. In the early stages of the implementation and running, the first 5,000 zeroes of the zeta function were calculated and for the majority of them the conclusion that they lie on the ½ line was attained without any doubt. Some cases did not provide a clear cut answer at the early stages.

Later on, further calculations were done, and by 1956 it was confirmed that the first 15,000 zeros all lie on the ½ line [DH Lehmer 1956].[14]

Two other, less-known hypotheses that were approached with the help of SWAC deserve some comment here. In 1919 Georg Pólya (1887-1985) had conjectured that there are more numbers having an odd number than an even number of prime factors [Pólya 1919]. This can be formally expressed with the help of the Liouville function $\lambda(n)$, which takes the value +1 if n has an even number of prime factors or -1 if it has an odd number of prime factors. If we define now

$$L(N) = \sum_{n=1}^{N} \lambda(n),$$

then the conjecture states that $L(N) \leq 0$, for $N > 1$. SWAC calculated this function for values $N < 800{,}000$. The lowest previously known value of the function obtained at $N = 48{,}512$, and it was $L(n) = -2$. This was not improved by SWAC. With little modification the same coding could be used to verify an associated hypothesis, commonly (and perhaps wrongly) attributed to Paul Turán (1910-1976), namely, that the function:

$$M(N) = \sum_{n=1}^{N} \lambda(n)/n,$$

is positive. The interesting point is that as early as 1958 both conjectures had been disproven by C. Brian Haselgrove (1926-1964) [Haselgrove 1958]. Haselgrove run a program in EDSAC at Cambridge, and somewhat later, independently, another one in

[14] [Meller 1958] reached 25,000.

Mark I at Manchester, and showed that there exists a counterexample whose value he estimated to be around $e^{831.847} = 1.845 \times 10^{361}$. In 1960 R. Sherman Lehman found an explicit counterexample, $n = 906{,}180{,}359$ which he calculated with Berkeley's IBM 701 [Lehman 1960]. Later on, in 1980 Minoru Tanaka showed that the smallest counterexample to the Pólya conjecture is $n = 906{,}150{,}257$ [Tanaka 1980]. It is interesting to point out that Lehman had worked at the Aberdeen proving grounds after graduation in Stanford and there, among other things, in 1955 he checked the conjecture (together with W.G. Spohn) up to $n \leq 802{,}000$ using the ORDVAC. Lehmer met him there and in 1957 brought him to Berkeley [Moore 2007, 177-178]. Lehman excelled in a wealth of mathematical fields, and above all in computational number theory. Expanding on the work of Lehmer, he made the by then ground-breaking confirmation that the first 250,000 non-trivial zeroes of the Riemann zeta function all lie on the ½ line. He devised a careful strategy for error bound calculation and coded in ALGOL a program run in Berkeley's IBM 7090 [Lehman 1966].

By 1956 it seemed that calculations made with SWAC had added support for the validity of the Riemann conjecture as well as for the other two conjectures just mentioned. It also had likewise seemed to add further support to FLT. One can only speculate how much longer it might have taken before computing resources were devoted to calculations related with FLT were it not for the previous collaboration between Vandiver and the Lehmers on this topic, and the current involvement of the latter with electronic computers. Although it represented a natural continuation of the work done in 1935-40, with a new and much more powerful technology at hand, Vandiver did not immediately thought that SWAC should be used for this purpose. Emma Lehmer continually informed

Vandiver about progress on computations with Mersenne primes, and explicitly wrote him that "if you have some pet problem you would like to run, I might try my hand at coding it and maybe we can run it after hours".[15] Amazingly, as late as April 1952, Vandiver was still replying to her that "no particularly numerical problem occurs to me that may be handled by the machine; but if one does, I'll let you know".[16] Actual work on FLT with SWAC started only on June 1952, and the results of this joint research were published in 1954. Work was done in two parts: (1) identifying all the irregular primes < 2000; and (2) checking that each irregular prime thus found satisfies necessary criteria for ensuring that the theorem holds for 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. I have dealt with this topic elsewhere and thus I will not give further details here [Corry 2008a].

The historical significance of calculations related with Mersenne primes using electronic computers are best understood as part of the various developments just described in this and the previous sections. As already indicated, the main figure in this part of the story is Raphael Robinson, another unique, self-styled mathematician. Robinson's range of mathematical interests spanned fields as diverse as logic, set theory, combinatorics, geometry, complex analysis and number theory, in all of which he made significant contributions. He described himself as an "old-fashioned" mathematician that often

[15] Emma Lehmer to Vandiver: March 7, 1953 (HSV).

[16] Vandiver to Emma Lehmer: April 3, 1953 (HSV).

switched research fields and tackled neglected problems of various kinds. He joined the mathematical faculty at Berkeley at nearly the same time than Lehmer [Brillhart 1996, Henkin 1995]. Previous to his work on Mersenne primes, Robinson had published mainly on complex analysis and logic. Curiously, however, early in his career, in 1940, he developed a set of stencils that could be used to solving quadratic congruences $x^2 \equiv a \pmod{m}$. The stencils were produced in a spirit similar to D N Lehmer's factor stencils of 1929. They were implemented in Hollerith punch cards that were used to mechanically simulate the so- called "Gauss method of exclusion" [Robinson 1941].[17]

By 1952, the date of Robinson's incursion in the field, the test developed by DH Lehmer in 1930 was still the main tool for determining the primeness of any M_p (and it has remained so to this day). As already said above, one of the main contributions of Lucas had been to suggest a method whereby the primality of a given number is tested by checking if it divides a certain other number, rather than by whom it is divided (or not divided). Under Lehmer's additional contribution the test came to be based, specifically, on the behavior of a sequence that is defined recursively by: $s_0 = 4$; $s_{n+1} = s_n^2 - 2$. Lehmer showed that M_p is prime if and only if M_p divides s_{p-1}. Thus, with the help of this test knowledge about M_p for $p \leq 257$ had progressed considerably by 1952. The following table summarizes the state of the art at that time [Williams 1998, 200]:

$p \leq 257$	Character of M_p
2, 3, 5, 7, 13, 17 ,19, 31, 61, 89, 107, 127	Prime
11, 23, 29, 37, 41, 43, 47, 53, 59, 67, 71, 73, 79, 83, 97, 113, 151	Composite and completely factored

[17] See DH Lehmer's description in *Mathematical Reviews* 1942 (MR0002987).

163, 173, 179, 181, 223, 233, 239, 251	Two or more prime factors known
131, 167, 191, 197, 211, 229	Only one prime factor known
101, 193, 109, 137, 139, 149, 157, 193, 199, 227, 241, 257	Composite but no factor known

In January 1952 Robinson wrote from Berkeley to the Lehmers offering a program for primality testing and hoping that they "will at least have a chance to try [it] out". He thus wrote:[18]

> I have amused myself for the past few weeks by constructing a program for testing Mersenne and Fermat numbers on the SWAC. The program, and a rather complete explanation, are enclosed. I do not even know whether anyone else has made a similar program, but even if that is the case, mine should be of some interest. Some features [of it] … might be used in other programs.
>
> I have checked the program carefully, and feel sure that it is free from error. Whether the SWAC will actually run the program or not is another question. I have the feeling that this may be just the sort of program which the SWAC should theoretically do, but which it doesn't like because of its highly repetitive character. If so, I suppose we can only wait until the SWAC is in better shape.

And free from error it was! The program, that implemented the Lucas-Lehmer test, is a veritable landmark in the history of scientific computing. John Brillhart, who completed his PhD in 1967 at Berkeley under Lehmer, described it retrospectively in the following words [Brillhart 1996, 16]:

[18] Robinson to DH Lehmer , January 9, 1952. This, and following letters are found at the Emma & Dick Lehmer's Archive, Bancroft Library, UC Berkeley (hereafter DEL), and are quoted with permission.

> Actually Raphael had never seen nor programmed a computer, but he astonished everyone by writing a SWAC primality testing program up in Berkeley which ran the first time. This was typical of the kind of careful and clever work that Raphael did. He had figured out how the machine worked from some notes, and after asking some questions, had punched the binary program cards and sent the deck of cards down to UCLA to be run.
>
> The Lehmers, who were busy at the time, put the deck on a shelf, planning to debug the program when they had a free moment. Raphael (up in Berkeley) waited and waited but no word came. Finally he phoned and found out that they hadn't even tried his program. His response was to send a telegram: "TRY IT!" [19]

From DH Lehmer's correspondence and several short notes he published at that time, we know many details about progress in calculations with SWAC. Robinson's program was first run on January 30, and two new Mersenne primes were found that very day, M_{521} and M_{607}. These two numbers yield, respectively, the 13th and 14th perfect numbers [DH Lehmer 1952a]. DH Lehmer wrote to Turing in February asking for the current state of work at Manchester on the Mersenne primes as well as with the Riemann Zeta function. He informed Turing about their own progress: indices up to $n = 1733$ had been checked with only the first two new primes found thus far.[20] Turing was highly impressed by the ability to calculate up to such high values of Mersenne numbers. He informed that at Manchester very little progress had been done on this field, but some had been done on

[19] [Williams 1998, 286], who quotes this passages adds that in his article "Brilhart wrote 'RUN IT', but agrees now that he was mistaken. Raphael did tend to be soft-spoken, but of cours telegrams did not empoy lowercase letters."

[20] DH Lehmer to Turing, February 15, 1952 (DEL).

the Riemman zeta-function.[21] By June, Lehmer informed that the Mersenne program was "going along rather slowly. We are little beyond $n = 2000$ on the first run and over $n = 1300$ on the rerun." There was usually a gap of two weeks between the two runs. At this point, however, there were no new primes to report.[22] On June 25 M_{1279} was identified as prime with a test that took less than 13.5 minutes [DH Lehmer 1952b].[23] M_{2203} and M_{2281} were identified in October 7 and 9, respectively, with computing times of 59 and 66 minutes [DH Lehmer 1953].[24]

For each index n, the output of Robinson's program yielded the least non-negative residue of $s_{n-1} \pmod{M_n}$. In hexagesimal notation, this is a long string of zeros if M_n is prime. Otherwise the output was an apparently random sequence of digits. For those values of n for which no factor of M_n was known the program was run twice and even, in case of disagreement, three times. At any rate, a result was accepted as correct only if it was obtained twice, and indeed on different days. Eventually, testing again the already known values of Mersenne primes became a "check that SWAC in good working order."[25] Because of the repeated checkings, the project was not considered to be complete until late 1953. Only then Robinson officially reported the results of the project [Robinson 1954].

---

[21] Turing to DH Lehmer, February 19, 1952 (DEL).

[22] DH Lehmer to Turing, June 10, 1952 (DEL).

[23] DH Lehmer to Horace Uhler, August 19, 1952 (DEL).

[24] DH Lehmer to Horace Uhler, October 17, 1952 (DEL).

[25] DH Lehmer to Lowell Schoenfeld August 19, 1952 (DEL).

The physical limitations of the machine implied that the indexes to be calculated could not be over $p = 2309$. Indeed, as already said, the internal memory of SWAC had a capacity of 256 numbers of 36 binary digits (exclusive of sign). Half of this memory was used for storing the instructions, while the other half stored $2p$ binary digits of two numbers s_k and s_{k+1} (mod M_n). Thus, $2p \leq 128 \cdot 36$, and hence $p \leq 2304$.[26] Robinson estimated a running time of $0.25n^3+125n^2$ microseconds in SWAC for his program and the actual time came very close to this.[27] He was very proud to state that his testing of Mersenne numbers for primeness has been taken "about as far as is practicable using present day computers." A no lesser source of pride was the fact that each "minute of machine time is equivalent to more than a year's work for a person using a desk calculator."

Other than the new cases of Mersenne numbers identified as primes, Robinson did not publish the "hundreds of remainders obtained" for the other cases. These were deposited, as was customary with other tables at the time, at the Institute for Numerical Analysis. Robinson also reported on results obtained with SWAC in relation with Fermat numbers, by running a modified version of his program. This program showed that $2^{1024} + 1$ is composite. However, before this result of Robinson was published, Selfridge went further and actually found factors for F_{10} and F_{16}, as already stated above.

---

[26] DH Lehmer to Horace Uhler June 16, 1952 (DEL).

[27] In a letter to Horace Uhler (June 4, 1952 - DEL), however, DH Lehmer wrote that the estimated run time for a given p was $(p/100)^3$ seconds

Mersenne numbers remained now unchecked from 2^{2309}-1 on. Robinson stated that the next case of real interest would be 2^{8191}-1, because it constitutes a test case for yet another open conjecture, namely, that 2^n-1 is always prime when n is itself a Mersenne prime. This conjecture was known to be valid for the first four cases ($3 = 2^2$-1, $7 = 2^3$-1, $31 = 2^5$-1, and $127 = 2^7$-1), and the next number in line was $n = 8191 = 2^{13}$-1. However, a relevant computation had been recently performed in by Wheeler on ILLIAC, at the University of Illinois. After one hundred hours of machine time the remainder obtained was not zero, indicating that the number is composite. This seemed to disprove the conjecture, but Robinson went on the safe side by stating that "according to Dr. Wheeler, considerable confidence may be placed in this result, since the computation was carefully checked." [Robinson 1954, 846].

Robinson himself continued to be involved in some additional, related computations. In September-November 1956, with Selfridge operating SWAC, fourteen new factors of Fermat numbers were discovered for n = 39, 55, 63, 117, 125, 144, 150, 207, 226, 228, 268, 284, 316, 452 [Robinson 1957a]. In February-April 1957 he run new factorization routines, now on Berkeley's IBM 701, that could find factors smaller than 2^{35}. New factors were discovered for $2^{95} - 1$, $2^{109} - 1$, and $2^{157} - 1$, on the one hand, and for $2^{71} + 1$, $2^{109} + 1$, $2^{112} + 1$, $2^{113} + 1$, and $2^{134} + 1$, on the other hand. Robinson also confirmed Wheeler's disproof of the conjecture mentioned above, by finding now factors of M_m, when $m = 2^{17}$ -1 and $m = 2^{19} - 1$ [Robinson 1957b].

8. Concluding Remarks

Mersenne numbers continued to attract the interest of computational number theorists as well as of engineers looking for endurance tests for new machines and new programming techniques. The first important case immediately after Robinson was that of Hans Riesel, who in late 1957 run programs on the Swedish electronic digital computer BESK [Riesel 1958]. It discovered the 18th Mersenne Prime, M_{3217}, after 5hours and 30minutes of calculation, with a small error that was later corrected by Selfridge.[28] The latest important stage is the Great Internet Mersenne Prime Search, a unique web-based initiative launched in January 1996. It uses idle time of thousands personal computers of volunteers who have downloaded and installed a module that turns them into active partners in this huge, Internet-based, distributed project. The first prime found as part of GIMPS, $M_{1398269}$, was discovered in November 1996 by Joel Armengaud. The latest one, thus far, was discovered on September 4, 2006, by Curtis Cooper and Steven Boone. It is the 9,808,358- digit number $M_{32582657}$.

Improved machines and computation techniques were increasingly developed after 1955, and electronic computers gradually became ubiquitous in science. Pure mathematical fields in general and in particular number theory were slower and more hesitant in joining this trend. Computational number theory continued to develop along the twentieth century, but number theory as a whole remained, essentially, a purely theoretical discipline where the leading images and ideals were still similar to those promoted by Hilbert and likeminded mathematicians at the turn of the twentieth century, even if much more powerful and sophisticate techniques were continually adopted. The

[28] In *MTAC* 13, 1959, 142.

mathematicians mentioned in this article – Vandiver, the Lehmers, Robinson and some others – played a seminal role in introducing a direction of research that attracted little attention among the leading practitioners of the discipline and that has ever since produced many important results and opened new avenues of research. Were it not for the special circumstances that surrounded their careers, this direction might have taken much longer to start and to being pursued by many others.

9. References

Archibald, Raymond C. (1948) *Fifty mathematical table makers*. *Portraits, Paintings, Busts, Monuments. Bio-Bibliographical Notes*, New York, Scripta Mathematica.

Bateman. P.T., John L. Selfridge and Samuel S. Wagstaff, Jr. (1989), "The new Mersenne conjecture", *Am. Math. Monthly* 96, 125-128

Bell, Eric T. (1951), *Mathematics; Queen and Servant of Sciences*, New York, McGraw-Hill.

Booker, Andrew R. (2006), "Turing and the Riemann Hypothesis", *Notices AMS* 53 (10), 1208-1211.

Brent, R. P.; Cohen, G. L. L.; and te Riele, H. J. J (1991), "Improved Techniques for Lower Bounds for Odd Perfect Numbers", *Math. Comp.* 57, 857-868.

Brillhart, John (1992), "John Derrick Henry Lehmer", *Acta Arithmetica* 62, 207-213.

---- (1996), "Raphael M Robinson", *Bull. Inst. Combin. Appl.* 16, 15-18.

Martin Campbell-Kelly et al (eds.) (2003), *The History of Mathematical Tables. From Sumer to Spreadsheets*, Oxford, Oxford University Press.

Cole, Frank N. (1903), "On the factoring of large numbers", *Bull AMS* 10 (3), 134-137.

Corry, Leo (2007), "Fermat Comes to America: Harry Schultz Vandiver and FLT (1914-1963), *Mathematical Intelligencer* 29 (3), 30-40.

----- (2008a), "Number Crunching vs. Number Theory: Computers and FLT, from Kummer to SWAC (1850-1960), and beyond", *Archive for History of Exact Science* (Forthcoming).

----- (2008b), "FLT Meets SWAC: Vandiver, the Lehmers, Computers and Number Theory", *IEEE Annals of the History of Computing* (Forthcoming).

Croarken, Mary (1990), *Early Scientific Computing in Britain*, Oxford, Clarendon Press.

----- (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.

Décaillot, Anne-Marie (1998), "L'arithméticien Édouard Lucas (1842-1891): théorie et instrumentation", *Revue d'histoire des mathématiques* 4 (2), 191-236.

----- (2002), "Géométrie des tissus. Mosaïques. Échiquiers. Mathématiques curieuses et utiles", *Revue d'histoire des mathématiques* 8 (2), 145-206.

Drake, Stillman (1971), "The rule behind Mersenne's numbers", *Physis* 13, 421-424.

Fermat, Pierre de (Oeuvres), *Oeuvres de Fermat*, ed. Charles Henry and Paul Tannery. 5 vols., Paris, Gauthier-Villars et fils (1891-1922).

Gispert, Hélène (1991), *La France mathématique, La Société mathématique de France (1870-1914)*, Paris, Société française d'histoire des sciences et des techniques & Société mathématique de France.

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 (2007a), "A Book on Search of a Discipline (1801-1860)", in Goldstein et al (eds.) (2007), 3-65.

---- (2007b), "Several Disciplines and a Book (1860-1901)", in Goldstein et al (eds.) (2007), 67-103.

Goldstein, Catherine, Norbert Schappacher and Joachim Schwermer, (eds.) (2007), *The Shaping of Arithmetic after C.F. Gauss's Disquisitiones Arithmeticae*, New York, Springer.

Grier, David A. (2001), "The Rise and Fall of the Committee on Mathematical Tables and Other Aids to Computation", *IEEE Annals of the History of Computing* 23 38-49.

----- (2003), "Table Making for the Relief of Labour", in Martin Campbell-Kelly et al (eds.) (2003), 265-292.

Guy, R. K. (1994), *Unsolved Problems in Number Theory* (2nd ed.), New York, Springer-Verlag.

G. H. Hardy (1940), *A Mathematician's Apology*, Cambridge University Press.

Haselgrove, C.B. (1958), "A disproof of a conjecture of Pólya", *Mathematika* 5, 141-145.

Henkin, Leon (1995), "In Memoriam: Raphael Mitchel Robinson", *Bull. Symbolic Logic* 1 (3), 340-343.

Hilbert, David (1998), *The Theory of Algebraic Number Fields*, Berlin, Springer. (English translation of Hilbert 1879 by F. Lemmermeyer and N. Schappacher.)

Huskey, Harry D. (1997)**, "**SWAC-Standards Western Automatic Computer", *IEEE Annals of the History of Computing* 19, 51-61.

Huskey, Harry et al. (1997)**, "**The SWAC Design Features and Operating experience", *Annals of the History of Computing* 19, 46-50.

Minkowski, Hermann (1905), "Peter Gustav Lejeune Dirichlet und seine Bedeutung für die heutige Mathematik", *Jahresb. DMV* 14, 149-163

Jensen, Kaj Løchte (1915), "Om talteoretiske Egenskaber ved de Bernoulliske Tal", *Nyt Tidsskrift for Matematik* 26, 73-83.

Legendre, Adrien M. (1798), *Théorie des nombres*, Paris (2d, ed. – 1808 ; 3d ed. 1830).

Lehman, R. Sherman (1960), "On Liouville's function", *Math. Comp.* 14, 311-320.

----- (1966), "Separation of Zeros of the Riemann Zeta-Function", *Math. Comp.* 20 (96), 523-541.

Lehmer, Derrick H. (1932), "Hunting big Game in the Theory of Numbers", *Scripta Mathematica* 1, 229-235.

----- (1933), "A photo-electric number-sieve", *Amer. Math. Monthly* 40, 401-406.

----- (1935), "Lacunary recurrence formulas for the numbers of Bernoulli and Euler", *Ann. Math.* 36, 637-648.

----- (1936), "An extension of the table of Bernoulli numbers**",** *Duke Math. Journal* 2, 460-464.

----- (1952a), "Recent Discoveries of Large Primes", Note 131, *MTAC* 6, 61.

----- (1952b), "A New Mersenne Prime", Note 138, *MTAC* 6, 205.

----- (1956), "On the roots of the Riemann zeta-function", *Acta Mathematica* 95 291-294.

----- (1974), "The influence of computing on research in number theory", in: Joseph P. LaSalle (ed.), *Analytic Number Theory* (Proc. Sympos. Appl. Math. 20, Amer. Math. Soc.), 3–12.

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.

---- (1914), *List of prime numbers from 1 to 10 006 721*, Washington, Carnegie Institution of Washington.

---- (1929), *Factor Stencils*, (Revised and extended by J. D. Elder) Washington, Carnegie Institution of Washington.

Lehmer, Emma (1955), "On the number of solutions of $u^k+D \equiv w2 \pmod{p}$", *Pacific J. Math*. 5, 103-118.

----- (1956), "Number Theory on the SWAC", *Proc. Symp. Applied Math*. 6, Providence, AMS, 103-108.

Lowan, Arnold N. (1949), "The Computational Laboratory of the National Bureau of Standards", *Scripta Mathematica*, Vol. 15, 33-63.

Lucas, Édouard (1890), "Les appareils de calcul et les jeux de combinations" *Revue Scientifique* 65, 1-13.

----- (1891), *Théorie des Nombres*, Paris, Gauthier-Villars.

----- (1887), "Sur le neuvieme nombre parfait", *Mathesis* 7. 73-75.

Meller, N.A. (1958), "Computations connected with the check of Riemann's hypothesis", (Russian) *Dokl. Akad. Nauk* (USSR) 123, 246-248.

Moore, Calvin C. (2007), *Mathematics at Berkeley. A History*, Wellesley, MA, AK Peters.

Polachek, H. (1995), "History of the journal *Mathematical Tables and other Aids to Computation*, 1959-1965", *Annals of the History of Computing* 17 (3), 67-74.

Pólya, George, "Verschiedene Bemerkungen zur Zahlentheorie", *Jahresber. DMV* 28, 31-40.

Powers, R. E. (1911), "The tenth perfect number", *Am. Math. Monthly* 18, 195-197.

----- (1914), "On Mersenne's numbers", *Proc. London Math. Soc.* 13 (2): xxxix.

Reitwiesner, George W. (1950), "An ENIAC Determination of π and e to more than 2000 Decimal Places", *MTAC* 4, 11-15.

Riesel, Hans (1958), "Mersenne Numbers", *MTAC* 12, 207-13.

Robinson, Raphael M. (1940), *Stencils for solving* $x^2 \equiv a \pmod{m}$**,** Berkeley, California, University of California Press.

----- (1954), "Mersenne and Fermat Numbers", *Proc. AMS* 5, 842-846.

----- (1957a), "Factors of Fermat Numbers", *MTAC* 11, 21-22.

----- (1957b), "Some factorizations of numbers of the form $2^n \pm 1$", *MTAC* 11, 265–268.

Robinson, S.F. (1968), "Theorems on Brewer sums", *Pacific J. Math*. 25, 587-596.

Ruskeepää, Heikki (1998), *Mathematica Navigator : Graphics and Methods of Applied Mathematics*, Amsterdam, Elsevier.

Rutland, Davis (1995), *Why Computers are Computers. The SWAC and the PC*, Philomath, OR, Wren Publishers.

Sandifer, Ed (2006), "Odd Perfect Numbers", in *Ed Sandifer's "How Euler Did It"*, MAA Online (November 2006) (http://www.maa.org/news/howeulerdidit.html)

Selfridge, John (1953), "Factors of Fermat numbers", *MTAC* 7, 274-275.

Siegmund-Schultze, Reinhard (1998), *Mathematiker auf der Flucht vor Hitler*, Wiesbaden, Vieweg-DMV.

Tanaka, M. (1980), "A Numerical Investigation on Cumulative Sum of the Liouville Function*", Tokyo Journal of Mathematics* 3, 187-189.

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.

Vandiver, Harry S. (1914), "Extensions of the criteria of Wieferich and Mirimanoff in connection with Fermat's last theorem," *J. für Math.* 144, 314-318.

----- (1929), "On Fermat's last theorem," *Transactions AMS* 31, 613-642.

----- (1937), "On Bernoulli numbers and Fermat's last theorem," *Duke Mathematical Journal* 3, 569-584.

----- (1939), "On Bernoulli numbers and Fermat's last theorem (second paper)," *Duke Mathematical Journal* 5, 418-427.

Vandiver, Harry S. and George E. Wahlin (1928), *Algebraic Numbers - II. Report of the Committee on Algebraic Numbers*, Washington, D.C., National Research Council, p. 182.

Williams, Hugh C. (1998), *Édouard Lucas and Primality Testing*, New York, John Wiley and Sons.