TURING AND THE PRIMES

ANDREW R. BOOKER

Alan Turing's exploits in code breaking, philosophy, artificial intelligence and the foundations of computer science are by now well known to many. Less well known is that Turing was also interested in number theory, in particular the distribution of prime numbers and the Riemann Hypothesis. These interests culminated in two programs that he implemented on the Manchester Mark 1, the first stored-program digital computer, during its 18 months of operation in 1949–50. Turing's efforts in this area were modest,[1] and one should be careful not to overstate their influence. However, one cannot help but see in these investigations the beginning of the field of computational number theory, bearing a close resemblance to active problems in the field today, despite a gap of 60 years. We can also perceive, in hindsight, some striking connections to Turing's other areas of interests, in ways that might have seemed far fetched in his day. This chapter will attempt to explain the two problems in detail, including their early history, Turing's contributions, some of the developments since the 1950s, and speculation for the future.

A bit of history

Turing's plans for a computer. Soon after his involvement in the war effort ended, Turing set about plans for a general-purpose digital computer. He submitted a detailed design for the *Automatic Computing Engine* (ACE) to the National Physics Laboratory in early 1946. Turing's design drew on both his theoretical work "On Computable Numbers" from a decade earlier, and the practical knowledge gained during the war from working at Bletchley Park, where the Colossus machines were developed and used. One of the key differences between Turing's design and earlier computers like Colossus was that the ACE was to be a *stored program computer*, meaning that, in principle, its programming could be changed quickly, or even dynamically.[2]

There were several delays in realizing Turing's plans. First, the existence and capabilities of the Colossus machines were officially classed as secret information for decades after the war, so Turing was forbidden from disclosing what he already knew to be achievable. As a result, his plans were deemed overly ambitious and had to be scaled back. Second, Turing apparently met with a lot of bureaucracy from the management of NPL, so that even the scaled-down version, the Pilot ACE, was not completed until 1950, by which time Turing had resigned his post out of frustration.

[1] I think that Turing himself would agree with this; indeed, it seems clear from his writings at the time that he was disappointed with the results obtained in both instances.

[2] This idea is often credited to John von Neumann, who contributed to the design of two computers contemporary to the ACE: the EDVAC (successor to the highly successful ENIAC, designed by Eckert and Mauchly), and the computer at the Institute for Advanced Study in Princeton. However, it is unclear who really originated the idea, or if it is even possible to attribute it to any one person.

Max Newman and the Manchester Mark 1. Meanwhile, in late 1946, Turing's former lecturer at Cambridge, Max Newman, received a large grant from the Royal Society to build a computer at Manchester University. Initially it was to be based on von Neumann's design for the IAS computer. However, a few months later, a parallel effort was begun by Freddie Williams and his assistant Tom Kilburn in the Electrical Engineering department at Manchester, and Newman ultimately abandoned his own plans for a computer and joined Williams' group instead. This was a fortuitous turn of events, for despite their late start, Williams and Kilburn were the first to solve one of the key engineering challenges for stored-program computers: building a memory bank (or store, as it is called in the UK) that is simultaneously large, fast and reliable. Their design stored bits of information as dots on a CRT screen; it worked well enough to build a working prototype computer (the SSEM, or "Baby") by the summer of 1948, and the full-scale Mark 1 was mostly operational within another year.

This left Newman, along with two other mathematicians in his group, I. J. Good and D. Rees, free to ponder how best to make use of the new machine. Newman, a pure mathematician, was apparently keen that it be used for research in algebra and topology. In part this was to contrast the effort at Manchester with Turing's ACE, which at the time was viewed as Britain's major effort in the computing realm, and was expected to be used mostly for applied science (possibly including Britain's forthcoming atomic bomb program).

Upon resigning his post at NPL, Turing began a readership at Manchester in late 1948, under the invitation of Newman. He was put in charge of leading the software development on the Mark 1. Good and Rees left the project not long after, leaving Turing as its main user.

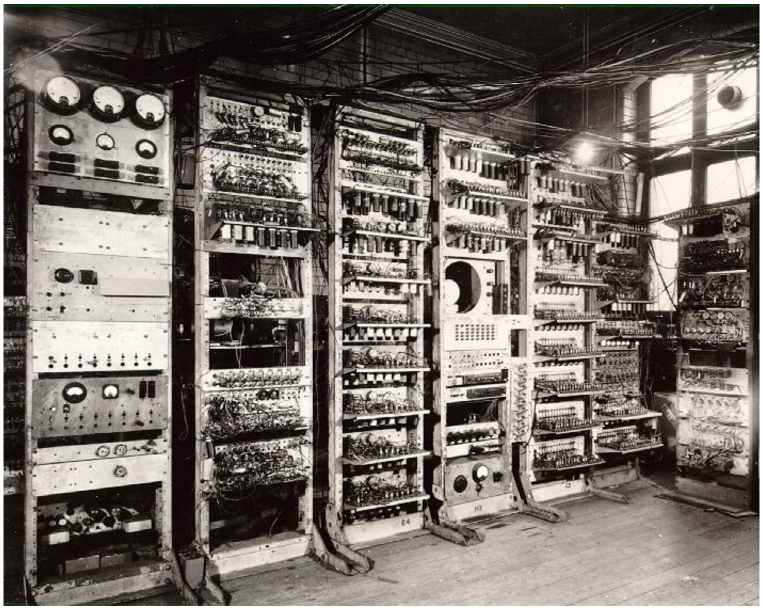

Figure 1. The left half of the Manchester Mark 1

Prime numbers

The reader may recall from grade school that a *prime number* is a positive integer that is only divisible by itself and 1. Ask any modern-day number theorist, however, and you are likely to find the traditional definition eschewed in favor of an analogy to chemistry, in which we liken the numbers to molecules and multiplication to chemical reactions. The primes, then, are what play the role of atoms, those molecules that cannot be broken down any further (chemically). In much the same way that every molecule is a unique collection of atoms (e.g. every water molecule consists of two atoms of hydrogen and one of oxygen, giving rise to its chemical symbol H_2O), every positive integer can be written uniquely, apart from changing the order of multiplication, as a product of prime numbers (e.g. $117 = 3^2 \times 13$).[3] This result was important enough to 19th century mathematicians that they started calling it the *Fundamental Theorem of Arithmetic* (FTA).[4]

People have been interested in prime numbers since at least the ancient Greeks. Euclid recorded a proof that there are infinitely many of them around 300 BC [10, §1.1.2]. His proof, still one of the most elegant in all of mathematics, can be expressed as an algorithm:

(1) Write down some prime numbers.
(2) Multiply them together and add 1; call the result n.
(3) Find a prime factor of n.

For instance, if we know that 2, 5 and 11 are all prime, then applying the algorithm with these numbers we get $n = 2 \times 5 \times 11 + 1 = 111$, which is divisible by the prime 3. By an earlier theorem in Euclid's *Elements*, the number n computed in step (2) must have a prime factor (and in fact it can be factored uniquely into a product of primes by the Fundamental Theorem of Arithmetic), so step (3) is always possible. On the other hand, from the way that Euclid constructs the number n, the prime factor found in step (3) cannot be any of the primes written down in step (1). Thus, no list of primes can be complete, i.e. there are infinitely many of them.

Note that n can have more than one prime factor (e.g. the number 111 in our example is also divisible by 37), and Euclid doesn't specify which one we should take in step (3). In 1963, Albert Mullin made Euclid's proof completely constructive by starting with just the prime 2 and repeating the algorithm to add a new prime to the list, always choosing the smallest prime factor of n in step (3). Similarly, one can instead always choose the largest prime factor, and these two constructions result in the so-called *Euclid–Mullin sequences* of primes [10, §1.1.2], the first few terms of which are shown in Table 1. Mullin posed the natural question of whether *every* prime number eventually occurs in each sequence. This is still unknown for the first sequence, though it has been conjectured that the answer is yes.

[3] There is a long-running debate, often pitting amateur and professional mathematicians against one another, as to whether the number 1 should be considered prime. In the chemical analogy, 1 (which is what we have before multiplying by anything) is like empty space (which is what we have before introducing any atoms). Thus, while it satisfies the definition of prime number given above from a puritanical point of view, it clearly does not satisfy the spirit of the analogy. More to the point, making 1 a prime would wreak havoc with the uniqueness of prime factorization, since any factorization could include an arbitrary number of 1's. To avoid this pathology, the modern convention is to consider 2 to be the first prime, and modify the definition accordingly.

[4] The most common approach to proving the FTA goes back to Euclid, but it was not until Gauss' work in 1801 that this point of view was emphasized and a complete proof was given.

first sequence (smallest prime factor)	second sequence (largest prime factor)
2	2
3	3
7	7
43	43
13	139
53	50207
5	340999
6221671	2365347734339
38709183810571	4680225641471129
139	1368845206580129

Table 1. First ten terms of the Euclid–Mullin sequences

On the other hand, it was shown recently (in 2011) that infinitely many primes are missing from the second sequence. This demonstrates how even very old topics in number theory can generate interesting research.

Euclid was followed within a century by Eratosthenes, who found an algorithm to list the primes that is still in use today. These results typify the contrasting ways that one can study and use prime numbers: either by looking at individual ones (as in the case of Eratosthenes), or by trying to understand general properties of the sequence of all primes, even those that may be well beyond our capacity to compute (as in the case of Euclid). As we will see, Turing's two programs on the Manchester Mark 1 fall squarely within these two respective camps.

Large primes

The first of these programs was an idea of Newman, conceived of as a way to test the capabilities of the new machine and draw publicity for the project. It was to search for a large prime number.

Mersenne primes. In much the same way that there is heaviest-known element at any given point in history, there is also a largest-known prime number. At the time of writing this stands at $2^{57,885,161} - 1$, a number with over 17 million digits, but that record is unlikely to stand for long. This is an example of a *Mersenne prime*, those that are 1 less than a power of 2. They are named for the French monk Marin Mersenne, who in 1644 predicted that $2^n - 1$ is prime for $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$, and for no other values of $n < 258$. All but the last four were known at the time of his prediction, and we now know that he was wrong about 67 and 257 and also omitted $n = 61$, 89 and 107, which do yield primes. The name has stuck nevertheless!

Throughout recent history (the last 150 years or so), the largest-known prime number has usually been a Mersenne prime. This is probably because it turns out to be a bit easier to find primes among the Mersenne numbers than for more general classes of numbers, and thus they have received more attention, for a few reasons. First, it is not hard to see that if $2^n - 1$ is prime then n itself must be prime, which helps weed out most of the non-primes. (Unfortunately, this test only works one way, i.e. even if n is prime, it is not guaranteed that

$2^n - 1$ will be; the smallest counterexample is $2^{11} - 1 = 2047 = 23 \times 89$.) Second, there is very fast algorithm, described by Lucas in 1876 and later refined by D. H. Lehmer, for testing the primality of a given candidate $2^n - 1$ when n is a prime bigger than 2:

(1) Start with the number $x = 4$.
(2) Replace x by the remainder from dividing $x^2 - 2$ by $2^n - 1$.
(3) Repeat step (2) a total of $n - 2$ times.
(4) Then $2^n - 1$ is prime if the final value of x is 0, and not otherwise.

(The reader is invited to try this with $n = 3$ or $n = 5$. With some paper and a pocket calculator to hand, it's also fun to check that the test correctly proves that $2^{11} - 1$ is not prime.) Third, the form of the Mersenne numbers (1 less than a power of 2) makes some of the arithmetic in the Lucas–Lehmer test particularly easy for computers, since they do calculations internally in binary.

Another reason for studying Mersenne primes is their connection to the so-called *perfect numbers*, which are those numbers that equal the sum of their proper divisors. For instance, the proper divisors of 28 are 1, 2, 4, 7 and 14, and these total 28. These numbers have also been studied since antiquity, and in fact Euclid was aware that if $p = 2^n - 1$ is prime then $p(p + 1)/2$ is perfect; thus, for instance, the perfect number $28 = 7 \times 8/2$ noted above is related to the Mersenne prime $7 = 2^3 - 1$, and each new Mersenne prime that is found also yields a new perfect number. (Incidentally, $p(p+1)/2$ is also the sum of the numbers from 1 to p, e.g. $28 = 1 + 2 + 3 + 4 + 5 + 6 + 7$, so it is no wonder that the ancient mathematicians regarded these numbers as having mystical properties compared to ordinary numbers, to the point of calling them "perfect".) About 2000 years later, Euler proved the converse statement that any *even* perfect number comes about by Euclid's construction, so there is a direct correspondence between Mersenne primes and even perfect numbers. It is still unknown whether there are any odd perfect numbers, though it is generally believed that none such exist.

Mersenne primes in the electronic era. By 1947, all the Mersenne numbers $2^n - 1$ for n up to 257 had been checked by hand, settling Mersenne's original claim. The largest prime among those was $2^{127} - 1$, discovered by Lucas in 1876. All Mersenne primes since then have been discovered by machines. (However, Ferrier discovered that $(2^{148} + 1)/17$ is prime in 1951 using only a mechanical desk calculator; it remains the largest prime discovered "manually".) The first such investigation was made by Turing, together with Newman and engineers Tom Kilburn and Geoff Tootill, in the summer of 1949. From a letter[5] that Turing wrote to D. H. Lehmer in March, 1952, we know that the team verified all of the known Mersenne primes and extended the search out to $n = 433$, though Turing described their efforts as unsystematic. Ultimately, the test brought the publicity for the new machine that Newman sought, but came up short, since they ended the search before finding any new primes.

One may debate the scientific value of their work because of that, though even if they had found a new prime number, it would by now be just a footnote in history. In any case, it wasn't long before new record primes were discovered by computer; Miller and Wheeler found several new ones in 1951 using the EDSAC at Cambridge, and Robinson found the next five Mersenne primes in 1952 using the SWAC at the National Bureau of Standards in Los

[5] found in the Emma and D. H. Lehmer Archive at Bancroft library, UC Berkeley

Angeles. Robinson's calculation, described in detail by Corry [4], is particularly impressive since he wrote his program having never seen a computer before. He sent the punchcards containing the code by mail to D. H. and Emma Lehmer in Los Angeles. They first ran the program on January 30, 1952; it ran bug free and found the next Mersenne prime, $2^{521}-1$, on the same day. Turing expressed how impressed he was with Robinson's results in his letter to D. H. Lehmer.

The search for Mersenne primes has continued unabated ever since. This presumes, of course, that there are more to find; however, there is no analogue of Euclid's proof for the Mersenne primes, and despite clear heuristic and empirical evidence, we still have no proof that there are infinitely many of them. At the time of writing, 48 are known, 36 of which were found by computers.[6] Since the mid-1990s, the search has been dominated by the aptly named Great Internet Mersenne Prime Search, set up by computer scientist George Woltman. Woltman's program uses spare time from the personal computers of thousands of volunteers, linked by the internet.[7] They have discovered new world-record primes at the rate of about one per year.

General primality testing and public key cryptography. The famous British mathematician and pacifist G. H. Hardy wrote in 1940 that

> No one has yet discovered any warlike purpose to be served by the theory of numbers or relativity, and it seems unlikely that anyone will do so for many years.

Hardy viewed number theory as the "purest" of disciplines, untainted by the demand for applications. With this point of view in mind, it comes as no surprise that Newman would choose a search for prime numbers to inaugurate the machine that he intended to use for pure mathematics.

In hindsight, Hardy's remarks are a bit ironic. Understanding of special relativity led to the development of nuclear weapons within just a few years of his writing. As for number theory, and the study of prime numbers in particular, one could plausibly maintain Hardy's opinion until the late 1970s and the advent of public-key cryptography. As a way of explaining the latter, we now know that it is theoretically possible for two people who have never met or even communicated before to stand at opposite ends of a crowded room and send each other messages in total secrecy using a pair of megaphones.[8]

The most commonly deployed public-key cryptosystem is RSA, invented by Rivest, Shamir and Adleman in 1978.[9] It relies crucially on the fact that it is easy to multiply prime numbers together but, as far as anyone knows, very difficult to determine which primes were

[6] This sentence raises a philosophical question: Should the computer be credited with the discovery along with the people involved in writing and running its program? A particularly interesting case occurred on April 12, 2009, when a computer proved that the number $2^{42,643,801}-1$ is prime, making it the third largest known Mersenne prime; however, no human took notice of that fact until June 4 of that year. Which should be considered the date of discovery?

[7] The reader is invited to participate; visit `www.mersenne.org` for details.

[8] It is not suggested that this be put into practice.

[9] A similar system was described five years earlier by Clifford Cocks of GCHQ, but was kept a secret until 1998.

multiplied when given only their product, even though the FTA guarantees that there is a unique answer.[10]

It might have been disastrous for the Allies had public-key cryptography been available during the war, for it is likely that even minds as clever as Turing's would not have been able to break the codes. However, today it is generally regarded as a good thing, and some might even call it essential to modern life. An example that is less absurd than a room with megaphones but still close to home is secure internet connections, which are usually initiated using the RSA cryptosystem. That is why, for example, we can feel safe when sending our credit card numbers to a website via the public internet.

One wrinkle in this theory is that we have no proof that the security of the currently known public-key cryptosystems cannot easily be broken, or even that such a system exists *in principle*; this is the famous P vs. NP problem, arguably the most important unsolved problem in computer science. To mitigate the potentially calamitous effects of a cryptosystem being broken, researchers have created many different systems that are not obviously related to one another, so there would be no shortage of substitutes if, for instance, someone discovered a fast way to factor numbers. However, this does not rule out panic until the replacement systems were fully deployed.[11]

Researchers also frequently play the adversarial role, testing the strength of various cryptosystems. Thus, RSA has generated interest in both primality testing, i.e. algorithms to decide whether a given number is prime or not, and factoring. On the theoretical side, it was finally proven in 2002 by Agrawal, Kayal and Saxena that primality testing is indeed "easy" for general numbers,[12] though algorithms that are faster in practice were already known. In practical terms, anyone with a high-end desktop PC purchased today can download free software that can quickly prove primality of numbers with thousands of digits, and factor any 100-digit number within about a day. The difficulty of factoring increases rapidly with the size, so for instance factoring general 230-digit numbers is currently possible, but only with a significant investment of time and money. Typical implementations of RSA in use today employ numbers with at least 1024 bits (about 300 digits), though that minimum size is expected to increase as the available computing power and algorithms improve.

The distribution of prime numbers

The second problem that Turing investigated on the Manchester Mark 1 was the Riemann Hypothesis (or RH), which has to do with the asymptotic distribution of prime numbers. This was a problem close to Turing's heart, and in fact he made an earlier attempt to investigate RH in 1939 with a special-purpose analog machine, using an elaborate system of gears. Turing had apparently cut most of the gears for the machine before he was interrupted by the war. By the time that he returned to the problem, in June of 1950, the progress toward general-purpose digital computers during the war had made Turing's 1939 machine obsolete. (The machine was never completed, though we do have a blueprint for it drawn

[10] The proofs that we have of the FTA are all *existence* proofs, i.e. they assert that every number has a unique prime factorization but offer no useful information about how to find it.

[11] Another concern is that current public-key cryptosystems are all thought to be vulnerable to attack if large *quantum computers* are developed. However, with quantum computers also comes the promise of even stronger methods of secure transmission, ones that are theoretically impossible to intercept.

[12] in contrast to tests for numbers of a special form, such as the Lucas-Lehmer test for Mersenne numbers, which have been around for a long time

up by Turing's friend Donald McPhail. A project has recently been proposed to build it; ironically, the first step of that undertaking will be a computer simulation.) Indeed, it had become practical, if only barely so, to consider much more than was possible with any analog machine—testing RH algorithmically, with no human intervention. As we will see below, this aspect of the problem, often taken for granted in modern discussions of the subject, was of keen interest to Turing.

The story behind the Riemann Hypothesis goes back to Gauss, who as a boy of 15 or 16 (in 1792–3) made long lists of prime numbers in order to understand just how common they are. (It seems fair to say that Gauss was a computational number theorist before there were computers!) He came to the conjecture that around a large number x, roughly 1 in every $\ln x$ integers is prime;[13] thus, if we want to know how many primes there are among the numbers 2, 3, 4, …, x (without actually counting them), we can estimate this by the integral $\int_2^x \frac{1}{\ln t}\,dt$, which is usually denoted $\mathrm{Li}(x)$. One might call this a quantitative version of Euclid's qualitative result that there are infinitely many primes.

x	$\pi(x)$	nearest whole number to $\mathrm{Li}(x)$
1000	168	177
10^6	78,498	78,627
10^{12}	37,607,912,018	37,607,950,280
10^{24}	18,435,599,767,349,200,867,866	18,435,599,767,366,347,775,143

Table 2. Comparison of $\pi(x)$ vs. $\mathrm{Li}(x)$

Table 2 shows the number of primes up to x, usually denoted $\pi(x)$ (although it has nothing to do with the constant $\pi = 3.14159\ldots$), for various powers of 10. Also shown is the nearest whole number to Gauss' approximation $\mathrm{Li}(x)$. One thing that is immediately apparent is that $\mathrm{Li}(x)$ seems to give an overestimate of the true count, and in fact that is true for every value of $\pi(x)$ for x at least 8 that has ever been computed. It was thought for a while that it must always be the case that $\mathrm{Li}(x) > \pi(x)$ for large x, but Littlewood proved in 1914 that this is false for some x, and moreover the inequality flips direction infinitely many times. In 1933, Skewes made Littlewood's theorem effective by showing that the first flip occurs before $x = 10^{10^{10^{34}}}$ if the unproven Riemann Hypothesis (discussed below) is true. This is an unimaginably large number, so much so that Hardy called it "the largest number which has ever served any definite purpose in mathematics". (That might have been true in 1933, but mathematicians have since found ways to make use of much larger numbers, such as those encountered in *Ramsey theory*.)

Turing worked on an improvement to Skewes' argument, hoping to reduce the bound significantly and remove the assumption of RH [7, 8]. He made some progress toward both goals in the summer of 1937, and returned to the problem again around 1952–3, but never published his work. In any case, both Skewes' and Turing's approaches have since been supplanted by later work based on computational methods; the latest results are discussed below.

[13] Here ln denotes the natural logarithm, to base $e = 2.71828\ldots$.

The Riemann zeta-function. The Riemann zeta-function is the infinite series

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \ldots = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{1}$$

As we learn in calculus class, this series converges for every $s > 1$ and diverges for every $s \leq 1$; the borderline case $s = 1$ is the well-known *harmonic series*, $\sum_{n=1}^{\infty} \frac{1}{n}$. The connection between the zeta-function and the prime numbers comes from another formula for $\zeta(s)$, derived by Euler in 1737 [10, §1.1.4]:

$$\zeta(s) = \frac{1}{1-\frac{1}{2^s}} \times \frac{1}{1-\frac{1}{3^s}} \times \frac{1}{1-\frac{1}{5^s}} \times \cdots = \prod_{p \text{ prime}} \frac{1}{1-\frac{1}{p^s}}. \tag{2}$$

Here it is given as an infinite product rather than a sum, and the variable p runs through all prime numbers (2, 3, 5, 7, 11, ...).

The equivalence between (1) and (2) is a sort of analytic expression of the Fundamental Theorem of Arithmetic mentioned above. To see this, we first expand the factor $\frac{1}{1-\frac{1}{p^s}}$ using the formula for a geometric series:

$$\frac{1}{1-\frac{1}{p^s}} = 1 + \frac{1}{p^s} + \left(\frac{1}{p^s}\right)^2 + \left(\frac{1}{p^s}\right)^3 + \ldots = 1 + \frac{1}{p^s} + \frac{1}{(p^2)^s} + \frac{1}{(p^3)^s} + \ldots$$

Next, we multiply together these geometric series for all choices of p. To do this, we have to imagine every conceivable product of the terms $\frac{1}{(p^k)^s}$ for various primes p and exponents k. For instance, one term that arises is $\frac{1}{(3^2)^s} \times \frac{1}{13^s} = \frac{1}{117^s}$, coming from the corresponding terms for $p = 3$ and $p = 13$. More generally, it is not hard to see that every product of terms will take the form $\frac{1}{n^s}$ for some positive integer n. In fact, for any given n, the term $\frac{1}{n^s}$ must eventually occur, since n has some prime factorization. Finally, because the prime factorization of n is unique, $\frac{1}{n^s}$ occurs exactly once. Thus, we arrive at the original defining series (1).

All of these manipulations make sense and can be made completely rigorous whenever $s > 1$. Euler had the clever idea of letting s tend to 1, so that (1) tends to the harmonic series, which diverges.[14] Thus, it must also be the case that (2) gets arbitrarily large as s gets close to 1. From this,[15] Euler concluded that there are infinitely many prime numbers p, since otherwise (2) would make sense and remain bounded even as s approached 1. This proof, while fiendishly clever, may seem much ado about nothing given that Euclid had already shown that there are infinitely many primes some 2000 years earlier. What makes Euler's proof important is that it can be generalized in ways that Euclid's cannot.

[14] This is a modern interpretation of his argument; in the 18th century, the notions of limit and convergence were not yet formulated rigorously, so Euler would have more brazenly set s equal to 1 and not worried so much about the extent to which it made sense to do so. The pendulum may yet swing the other way; the subject of *non-standard analysis* allows for a rigorous formulation of Euler's more direct approach, though, as its name implies, it is not yet fully accepted by all mathematicians.

[15] An alternate version, popular among algebraic number theorists, is to consider instead $s = 2$. Another theorem of Euler's says that $\zeta(2) = \pi^2/6$, and if there were only finitely many prime numbers then, by (2), this would be a rational number. However, Legendre proved in 1794 that π^2 (and hence also $\pi^2/6$) is irrational.

First, in 1837, Dirichlet showed how to modify Euler's proof to show that an arithmetic progression

$$a, a+b, a+2b, a+3b, \dots,$$

contains infinitely many primes, as long as a and b have no common factor [10, §2]. (If a and b have a common factor then it is easy to see that this progression can contain at most one prime; for instance the progression 6, 10, 14, 18, ... contains no primes since every term is even.) To do so, he introduced certain modified versions of the zeta-function, the so-called "L-functions" that now bear his name, and again studied their behavior as s tends to 1. Dirichlet's theorem is important in the sense that it has been used as an ingredient in countless other theorems in number theory. Moreover, it marks the beginning of what we now call *analytic number theory*, using techniques from real and complex analysis to study fundamental questions about numbers.

Second, in 1859, Riemann wrote a path-breaking paper on the zeta-function, his only paper related to number theory [10, §4]. In it, he sketched how a detailed study of $\zeta(s)$ (notation introduced by Riemann) can be used to see not only that there are infinitely many primes, but also understand the asymptotics of their distribution, ultimately leading to a proof of Gauss' conjecture that was completed independently by Hadamard and de la Vallée Poussin in 1896; we now call this result the *Prime Number Theorem* [12]. Riemann's key insight was to consider $\zeta(s)$ not just for real numbers s, but complex s as well. In fact, he showed, through the principle of *analytic continuation*, how to make sense of $\zeta(s)$ for all complex s apart from 1. The crucial point turns out to be understanding those values of s for which $\zeta(s) = 0$. It is known that this holds for $s = -2, -4, -6, \dots$, and for infinitely many non-real values of s with real part between 0 and 1. Riemann computed approximations of the first few non-real zeros, which are shown in Table 3. (The zeros come in complex-conjugate pairs, i.e. for every zero at $x + iy$, there is another one at $x - iy$. Thus, it is enough to list the ones with positive imaginary part.) He then made the bold guess that all of them have real part exactly $\frac{1}{2}$.

$0.5 + i14.134725141734693790 45\dots$
$0.5 + i21.022039638771554992 62\dots$
$0.5 + i25.010857580145688763 21\dots$
$0.5 + i30.424876125859513210 31\dots$
$0.5 + i32.935061587739189690 66\dots$

Table 3. First five zeros of Riemann's zeta-function with positive imaginary part

We are still unsure of this guess, now called the Riemann Hypothesis [3], over 150 years later, though there is significant evidence in favor of it, and most mathematicians today believe it to be true. If true, RH implies that Gauss' estimate of the number of primes up to x is accurate to "square root order", which, in other words, means that roughly the top half of the digits of the estimate are correct; for instance, while it is currently well beyond our technology to say exactly how many primes there are with at most 50 digits, Gauss' formula predicts the number to be about

$$\underline{8762680317507841688781768}6264040687098603110995 0,$$

and it is very likely that the underlined digits are correct. In the absence of a proof of RH, we have had to make do with weaker results; for instance, we know for sure that the number of correct digits in Gauss' approximation increases with the number of digits of x (which is the qualitative statement of the Prime Number Theorem), but we don't yet know that it does so linearly.

Turing and the Riemann Hypothesis. One thing that makes RH a good conjecture is its falsifiability, i.e. if it does turn out to be false then that can clearly be shown by observing a counterexample. There are some philosophical reasons to believe in the truth of RH, but aside from that, our best evidence in its favor is the many numerical tests that have been performed, not one of which has shown it to be false. (On the other hand, as the $\pi(x)$ vs. $\mathrm{Li}(x)$ question shows, one should not rely entirely on numerical evidence.) Curiously, Turing was not convinced of its truth; indeed, it is clear from his paper on the subject [11] that he had hoped the Manchester Mark 1 would find a counterexample. In his defense, skepticism of the conjecture was not uncommon in the first half of the 20th century, and some near counterexamples found in early investigations made it seem like a true one might be uncovered with just a bit more computation.

As mentioned above, the first computation of this type was made by Riemann himself,[16] and probably figured in his formulation of the conjecture. By the 1930s, Titchmarsh had extended the computation out to more than 1000 zeros, which were all found to obey RH. Titchmarsh's method, which was essentially derived from Riemann's, consisted of two main steps:

(1) Find all the zeros with real part $\frac{1}{2}$ and imaginary part between 0 and some large number T. Although the values of $\zeta(\frac{1}{2}+it)$ for real numbers t are typically complex, it turns out that one can define a real-valued function $Z(t)$ with the same absolute value as that of $\zeta(\frac{1}{2}+it)$. Thus, the zeros of $Z(t)$ correspond to the zeros of Riemann's zeta-function with real part $\frac{1}{2}$, and they can be found simply by inspecting the graph of $Z(t)$ and noting where it crosses the t-axis (see Figure 2, top pane).

(2) Find, by an auxiliary computation, the total number, say $N(T)$, of non-real zeros of the zeta-function with imaginary part up to T. If this agrees with the count of zeros with real part $\frac{1}{2}$ found in step (1) then all zeros with imaginary part up to T obey RH.

Of these two steps, the first is relatively straightforward. In fact, Riemann had already found a formula (later published by Siegel) that could be used to evaluate $Z(t)$ very quickly, which he used for his computations. The second step is a great deal more complicated; the methods used in all investigations up to and including Titchmarsh's were ad hoc and not guaranteed to work for large values of T. That was not good enough for Turing, who wanted the machine to work as autonomously possible. Instead, he found a criterion that could be used to decide if all of the zeros had been found *using the values that had already been computed.* Thus, Turing effectively replaced the most cumbersome step in the verification by an automatic check.

Turing's method was based on a careful comparison of the observed values of $N(T)$ versus its known asymptotic formula as T increases. Riemann postulated, and it was later rigorously

[16] This was only discovered decades after Riemann's death by examining his unpublished notes in the Göttingen library.

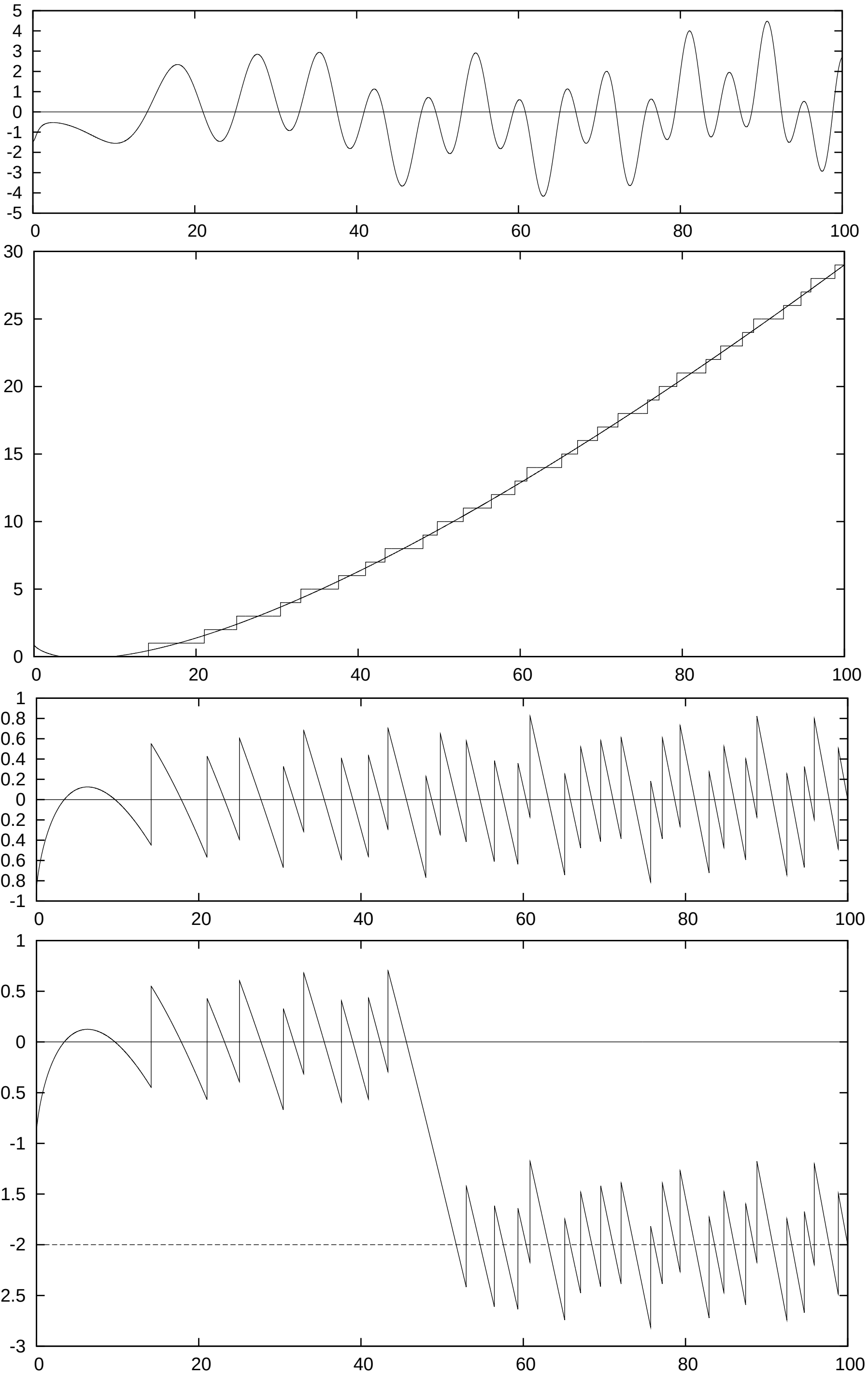

FIGURE 2. From top to bottom: $Z(t)$, $N(T)$ vs. $M(T)$, $E(T)$, and $E(T)$ with a pair of "missing" zeros

proven, that $N(T)$ can be approximated by the smooth function

$$M(T) = \frac{T}{2\pi}\ln\biggl(\frac{T}{2\pi e}\biggr) + \frac{7}{8}.$$

(Figure 2, second pane, shows the graphs of $N(T)$ and $M(T)$ for T up to 100. Notice how every jump in the graph of $N(T)$ occurs at a zero crossing of $Z(t)$; this confirms RH up to height 100.) This is an asymptotic approximation, meaning that the percentage error in the prediction tends to 0 as T grows, but in absolute terms it can be out by a large margin for an individual T. In practice it has never been observed to be wrong by more than 4, though it is known theoretically that the error is typically large for very large T. In any case, this renders the formula useless when it comes to deciding whether we have found all the zeros for a given value of T.

Turing had the clever idea that one should look at the error term $E(T) = N(T) - M(T)$ for a range of values of T instead of just one. It was shown by Littlewood that $E(T)$ has average value close to 0 when T is large, and thus it tends to oscillate around 0, as is visible in Figure 2, third pane. If we imagine drawing that graph using measured data, any zeros that were missed would skew the average; for instance, if two zeros were missed,[17] it would begin to oscillate around -2, as shown in the bottom pane. This can be turned into a rigorous proof that none are missing, as long as one has a version of Littlewood's theorem with explicit constants. One of the main theoretical results in Turing's paper [11] was a painstaking derivation of such a theorem.

Although Turing carried out his investigation in 1950, his paper was not published until 1953, just a year before his death. The project was apparently not a high priority task for the Mark 1, as the following quotation from the paper makes clear:

> The calculations had been planned some time in advance, but had in fact to be carried out in great haste. If it had not been for the fact that the computer remained in serviceable condition[18] for an unusually long period from 3 p.m. one afternoon to 8 a.m. the following morning it is probable that the calculations would never have been done at all. As it was, the interval $2\pi.63^2 < t < 2\pi.64^2$ was investigated during that period, and very little more was accomplished.

Evidently Turing was disappointed with the results obtained. As we now know, computers have become substantially faster, less expensive, and more reliable than in 1950, and these improvements came about very quickly. However, that would have been difficult to anticipate at the time, which might explain Turing's pessimism. D. H. Lehmer had this to say in his Mathematical Review of the paper:

> Although the author tends to belittle the actual results obtained in a few hours of machine time, the paper shows that a great deal of careful work has been done in preparing the calculation for the machine and this work will be of value to future computers. Since 1950 there has been a large increase in the number and reliability of large scale computers. No doubt further results on this problem will appear in due course.

[17] Since the zeros are located by sign changes, one always misses an even number of them.

[18] The Mark 1, like all of the early electronic digital computers, employed thousands of *vacuum tubes* (or thermionic valves), a technology that evolved from the incandescent light bulb. As is the case with light bulbs, one could expect an individual tube to last for years, but when using thousands of them, it was inevitable that at least one would burn out every day. To guard against this, it was standard practice on the Mark 1 to repeat sections of code every few minutes and halt the machine when a discrepancy was discovered.

Indeed, by 1956, Lehmer himself had applied Turing's method to extend the computations to ranges well beyond the reach of mechanical calculators. With modern computers and improved algorithms, they have reached extremes that would have been unfathomable in the 1950s. For instance, the first 10 trillion zeros have been found to obey RH, as has the 10^{32}nd zero and hundreds of its neighbors; all such calculations continue to rely on Turing's method as a small but essential ingredient. It is unfortunate that Turing would never see any of that come to pass.

Formal proofs. There are many other interesting quotations in Turing's 1953 paper [11], but one in particular speaks to his mindset at the time:

> If definite rules are laid down as to how the computation is to be done one can predict bounds for the errors throughout. When the computations are done by hand there are serious practical difficulties about this. The computer will probably have his own ideas as to how certain steps should be done.[19] [...] However, if the calculations are being done by an automatic computer one can feel sure that this kind of indiscipline does not occur.

It should be noted that Turing was writing "Computing Machinery and Intelligence" around the same time, and in that context the quotation is not surprising. Nevertheless, it was far ahead of its time; even two decades later, when the first proof of the *four color theorem* was announced, there was considerable doubt over whether it could be accepted if it was not practically possible for a human to check. Turing was declaring in 1950 that not only is it acceptable, but in fact *preferable* for machines to replace humans in some settings.

The tide is slowly turning toward Turing's point of view, in that mathematicians are now more trusting of results obtained by computer, though one still frequently hears the argument that such proofs are less elegant than those obtained by "pure thought". The shift in perceptions is illustrated by another controversy, similar to that surrounding the four color theorem, concerning Thomas Hales' proof in 1998 of the *Kepler conjecture*; this time it was not so much about whether the *machine* could be trusted, but rather its *programmers*, since the implementation was technically very challenging.

As the use of computers in pure mathematics increases, and proofs become more complicated as a result, such controversies seem likely to become more prevalent. One response is a thriving interest in *formal proofs* [6], in which a computer is used to check every single step starting from the basic axioms; for instance, we now have two independent formal proofs of the Prime Number Theorem, both completed within the last decade. Following this trend, it is easy to imagine a future in which Turing's vision is the de facto standard, and mathematical proofs would not be fully accepted until they had undergone formal verification by a machine.

Present day and beyond

Given the economies of scale achieved in speed, reliability and availability of computing machines noted above, it is no surprise that their use has exploded in all sorts of human endeavors. They are now ubiquitous in applied mathematics and are starting to come to prominence in pure mathematics as well, including number theory. For instance, when it

[19] Turing's use of the word "computer" here to refer to a human reflects the common usage up until the 1940s.

comes to primality testing, it is now routine to find prime numbers with thousands of digits, and this helps keep our online transactions secure.

For analytic number theory and RH in particular, a wealth of new understanding has come from computations of the zeta-function, much in the spirit of Turing's work in 1950. Foremost among these are computations done in the 1980s by Andrew Odlyzko who, together with Schönhage, found an algorithm that could be used to compute many values of $Z(t)$ simultaneously very quickly, the first theoretical improvement along these lines since the discovery of the Riemann–Siegel formula. The new algorithm enabled Odlyzko to expose a link between the zeros of the zeta-function and *random matrix theory*, a tool used by physicists to model the energy levels of heavy atoms. Figure 3 shows a graph produced by Odlyzko comparing the nearest-neighbor spacing distribution of zeros of the zeta-function to that of eigenvalues of random Hermitian matrices (the so-called *GUE ensemble*). Roughly speaking, the curve gives the probability that a gap of a given size will occur between two consecutive zeros; thus, for instance, we see that the zeros are rarely close together, i.e. they tend to repel each other.

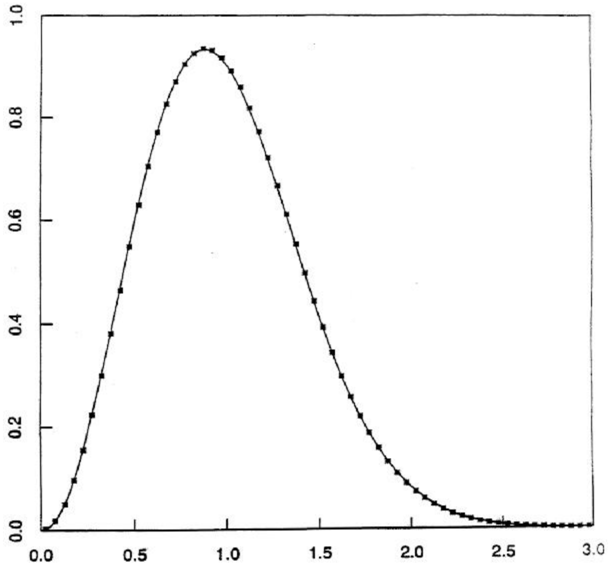

Figure 3. Nearest-neighbor spacing distribution of about 79 million zeros of ζ around the 10^{20}th zero (scatter plot), compared with the GUE model (smooth curve).

The first hint of a connection between the zeta-function and random matrix theory came from a chance meeting between mathematician Hugh Montgomery and physicist Freeman Dyson at the Institute for Advanced Study in 1972. Montgomery had conjectured a formula for one statistic, the *pair correlation*, of the zeros of the zeta-function, and Dyson immediately recognized that it was the same formula as in the GUE model. However, Odlyzko's numerics, such as in Figure 3, were definitive in making the case for what otherwise might have seemed a curious coincidence.

What is still unclear is *why* the zeros of the zeta-function follow GUE statistics. One possibility is that there is a physical system, similar to a heavy atom, whose spectrum is exactly the set of zeros of ζ. If so, finding the system would realize an approach, now called the Hilbert–Pólya conjecture, to proving RH that was suggested by Pólya a century ago.

A more mundane possibility is that this is a universal phenomenon, in the same way that Gaussian distributions turn up a lot in nature, a view strengthened by computations involving other L-functions which have found similar results. There are now many mathematical objects that fall under the general moniker of L-function [1], the prototypes of which are the Riemann zeta-function and the original L-functions of Dirichlet. The *Langlands Program*, a major area of research in modern number theory, aims to classify the various kinds and relations between them, and we are just beginning to explore the full potential of computational methods in this area.[20] In part, the interest in other L-functions grew out of our inability to prove RH, since when mathematicians are stuck on one problem they often try to make progress in different directions by generalizing. Thus, for every one of these more general L-functions there is an associated "Riemann Hypothesis", though there are still no cases in which it has been proven.

Whatever the reason for the GUE phenomenon, one can argue that a thorough understanding of it is necessary before a proof of RH can be found. Although this still seems a long way off, we are just now moving past the point of verifying conjectures, as Turing and Odlyzko did, and are starting to use such computations as a replacement for RH when solving problems. Here are three examples related to prime numbers:

(1) *Counting primes.* As we saw above, Gauss' formula gives a good approximation for how many primes there are among the numbers 2, 3, …, x. But what if we want to know the exact answer for a particular x? Until the 19th century, the best known way to determine that was to find all of the primes with Eratosthenes' algorithm and count them. Fortunately, mathematicians have found some more clever ways since then. The fastest method currently known was proposed by Lagarias and Odlyzko in 1987; it works by adding various correction terms to Gauss' formula by using the computations that go into verifying RH. A version of it was used for the first time in 2010 by Buethe, Franke, Jost and Kleinjung, who computed the last entry of Table 2. Their method assumed RH, but that assumption has very recently been removed in an independent calculation by Platt.

(2) *The $\pi(x)$ vs.* Li(x) *problem.* Using numerical approximations of the first 22 million zeros of the Riemann zeta-function, Saouter and Demichel showed in 2010 that $\pi(x)$ exceeds Li(x) for some value of x below 1.3972×10^{316}, and there is reason to believe that the first such occurrence is near there. Thus, while we might never know the first occurrence exactly, the question of the best possible improvement to Skewes' bound has effectively been solved.

(3) *The Goldbach conjecture.* On June 7, 1742, Christian Goldbach wrote a letter to Euler in which he conjectured that every integer greater than 5 can be written as the sum of three prime numbers.[21] Essentially no progress was made on this until the 20th century. In the 1930s, Vinogradov showed that the conjecture is true for all sufficiently large *odd* numbers, though the even case has remained elusive. (The conjecture turns out to be much harder for even numbers, since at least one of the

[20] See `www.L-functions.org`.

[21] It was still common to consider 1 a prime number in Goldbach's time, so he actually wrote 2 in place of 5.

> primes must be 2 in that case, leaving only two degrees of freedom.) Here the meaning of "sufficiently large" has been reduced over the years, but it still stands at over 10^{1300}, far too large to check all smaller numbers directly, even with modern computers. On the other hand, it is known that Goldbach's conjecture holds for all odd numbers if RH is true for the Riemann zeta-function and Dirichlet L-functions. Numerical verification of RH, as in Turing's work, promises to allow us to bridge the gap between these results in the not-too-distant future.

Besides investigating existing conjectures and problems, over the last 60 years computers have proven to be extremely useful in suggesting new lines of enquiry. A good example is the *BSD conjecture*, discovered in the early 1960s by Birch and Swinnerton-Dyer using the EDSAC at Cambridge. The conjecture concerns *elliptic curves*, which are equations of the shape $y^2 = x^3 + ax + b$, where a and b are fixed integers. (Elliptic curves are the subject of another famous problem in number theory, the Shimura–Taniyama conjecture, whose proof by Wiles and Taylor in 1995 led finally to a complete proof of Fermat's Last Theorem after 350 years.) Given an elliptic curve, one can associate an L-function, and like the Riemann Hypothesis before it, the BSD conjecture is a prediction about the zeros of that function. It is now considered to be one of the most important open problems in number theory, and even partial results toward it have had striking applications. One such is Tunnell's resolution in 1983 of the 1000-year-old *congruent number problem* [2], which asks, for a given number n, whether there is a right triangle which has area n and sides of rational length. (Strictly speaking, Tunnell's algorithm can only be proven to work assuming the BSD conjecture, but a full proof of the conjecture is not necessary in order to apply the algorithm.) Another is Goldfeld's effective resolution of the *class number problem* [5], posed by Gauss in 1801; for instance, this work tells us (among many other things) all the integers that can be written uniquely as a sum of three perfect squares.

Thus, computers have been instrumental in addressing some long-standing (sometimes ancient) problems in number theory. On the other hand, there are other questions which our current techniques seem completely inadequate to solve, leaving numerical experiments as the *only* way of attacking them at present. For instance, we have already encountered a few questions in this chapter for which our theoretical knowledge is not significantly advanced beyond what Euclid knew around 300 BC:

(1) Does every prime appear in the first Euclid–Mullin sequence?
(2) Are there any odd perfect numbers?
(3) Are there infinitely many Mersenne primes?

One should never try to place a limit on the ingenuity of human beings (or their machines), but as Gödel showed, there are questions to which the answer is simply unknowable, and it is conceivable that one of these is in that category. (In fact, finding a "natural" example of such a question was the original motivation behind Mullin's construction.) In a way this is good, since it leaves open an avenue for amateur mathematicians and hobbyists, including those that may form the next generation of computational number theorists, to get involved in what is in other ways becoming a sophisticated and impenetrable subject.

The future of computers in number theory. We have arrived at a point now where nearly every mathematician has on his or her desk a tool that Gauss could only dream of. As we saw above, computers are starting to shape the outcome of research in number theory. It seems likely that this trend will continue to the point that they will become indispensable for doing research, and no one will work entirely without them. Perhaps, as a natural evolution of the current boom in formal proofs, the computers will even start to do some of the thinking themselves.

In a famous address in 1900, David Hilbert gave a list of 23 unsolved problems outlining his vision for the development of mathematics in the following century. Problem number 8 on the list was the theory of prime numbers, including both RH and the Goldbach conjecture. Sadly, we are hardly any closer to a proof of RH today than in 1900, with revelations such as the link to random matrix theory seeming to generate more questions than answers. (Hilbert might have anticipated this; he is quoted as saying "If I were to awaken after having slept for a thousand years, my first question would be: has the Riemann hypothesis been proven?") Nevertheless, significant progress has been made on most of Hilbert's problems, sometimes in unexpected ways; for instance, Gödel's work mentioned above, as well as that of Turing after him, was very much contrary to Hilbert's expectations.

With the turn of another century in 2000, several lists were proposed as replacements for Hilbert's problems. The one that has received the most attention is the list of seven Millennium Prize Problems published by the Clay Mathematics Institute, which offers $1 million for the solution to any one of them. To date, one problem, the Poincaré conjecture, has been solved. Of the remaining six, we have encountered three in this chapter while discussing Turing's work: the Riemann Hypothesis, the BSD conjecture and the P vs. NP problem. That is not to say that Turing's investigations on the Manchester Mark 1 had very much direct influence on these things, but if nothing else it is testimony to his uncanny ability to recognize and get involved in problems of lasting interest.

What will the list for the 22nd century look like? Probably no one alive today can make a meaningful prediction. However, it seems a safe bet that it will include at least one problem from number theory; if so, perhaps it will be one that was discovered by a computer. Turing, who was never afraid to speak his mind, said it best in an interview following the initial press coverage of the Mark 1:

> This is only a foretaste of what is to come, and only the shadow of what is going to be. We have to have some experience with the machine before we really know its capabilities. It may take years before we settle down to the new possibilities, but I do not see why it should not enter any of the fields normally covered by the human intellect and eventually compete on equal terms.

References

[1] Andrew R. Booker. Uncovering a new L-function. *Notices Amer. Math. Soc.*, 55(9):1088–1094, 2008.

[2] V. Chandrasekar. The congruent number problem. *Resonance*, 3:33–45, 1998. 10.1007/BF02837344.

[3] J. Brian Conrey. The Riemann Hypothesis. *Notices Amer. Math. Soc.*, 50(3):341–353, 2003.

[4] Leo Corry. Hunting prime numbers—from human to electronic computers. *Rutherford Jour.*, 3, 2010.

[5] Dorian Goldfeld. Gauss's class number problem for imaginary quadratic fields. *Bull. Amer. Math. Soc. (N.S.)*, 13(1):23–37, 1985.

[6] Thomas C. Hales. Formal proof. *Notices Amer. Math. Soc.*, 55(11):1370–1380, 2008.

[7] Dennis A. Hejhal. A few comments about Turing's method. In S. Barry Cooper and J. van Leeuwen, editors, *Alan Turing - His Work and Impact*. Elsevier Science, 2012.

[8] Dennis A. Hejhal and Andrew M. Odlyzko. Alan Turing and the Riemann zeta function. In S. Barry Cooper and J. van Leeuwen, editors, *Alan Turing - His Work and Impact*. Elsevier Science, 2012.

[9] Andrew Hodges. *Alan Turing: the enigma.* A Touchstone Book. Simon & Schuster, New York, 1983. Chapters 6 and 7 cover the period discussed here, including a detailed history of the design and development of the ACE and Manchester Mark 1 computers

[10] Władysław Narkiewicz. *The development of prime number theory: From Euclid to Hardy and Littlewood.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000.

[11] A. M. Turing. Some calculations of the Riemann zeta-function. *Proc. London Math. Soc. (3)*, 3:99–117, 1953.

[12] D. Zagier. Newman's short proof of the prime number theorem. *Amer. Math. Monthly*, 104(8):705–708, 1997.