CWI Quarterly Volume 7 (4) 1994, pp. 285 – 335

Computational Number Theory at CWI in 1970 – 1994

H.J.J. te Riele
Centrum voor Wiskunde en Informatica
P.O. Box 94079, 1090 GB Amsterdam, The Netherlands
e-mail: herman@cwi.nl

J. van de Lune
Noordermiedweg 31, 9074 LM Hallum (Frl.), The Netherlands

In this paper we present a concise survey of the research in Computational Number Theory, carried out at CWI in the period 1970 – 1994, with updates to the present state-of-the-art of the various subjects, if necessary. This research was stimulated greatly by the continuous availability to CWI-researchers of excellent contemporary computing facilities. It enabled the researchers to considerably "move the boundaries" of our knowledge of various classical number-theoretic problems, like the Riemann hypothesis, the Mertens conjecture, and the Goldbach conjecture. In addition, the computational results often gave rise to new insights and the development of new theory and algorithms. The main topics covered here are:

- the Riemann zeta function, its complex zeros and the Riemann hypothesis, the Mertens conjecture, the sign of the difference $\pi(x)-\mathrm{li}(x)$, and the zeros of the error term in an asymptotic formula for the mean square of $|\zeta(\frac{1}{2}+it)|$;
- special zeros of partial sums of the Riemann zeta function;
- decomposition of large integers into prime factors;
- aliquot sequences and aliquot cycles like amicable numbers;
- four smaller projects: the Goldbach conjecture; the constant of De Bruijn-Newman; the Diophantine equations $1^k+2^k+\cdots+(x-1)^k=x^k$ and $x^3+y^3+z^3=k$.

1. Introduction.

In this paper we present a concise survey of the research in Computational Number Theory which was carried out at CWI in the past 25 years. The excellent computing facilities and the "availability" of much idle CPU-time have been, and still are, a continuous stimulus. Where appropriate, we will update the present state-of-the-art of the subjects treated. The computational number theory group at CWI is part of CWI's Department of Numerical Mathematics, and this partly explains the choice of some number-theoretical problems with *numerical* aspects, like the separation of the zeros of the Riemann zeta function.

The Riemann hypothesis, which is one of the most famous and notorious unresolved conjectures in mathematics, and related subjects like the Mertens conjecture, are treated in Section 2. The location of certain zeros of partial sums of the Riemann zeta function is discussed in Section 3. The problem of the decomposition of large integers into prime factors is dealt with in Section 4. This classical problem has attracted renewed attention after the discovery by Rivest, Shamir and Adleman, in 1978, of an important application in public-key cryptography [124]. Number-theoretic sequences in which each term is computed from the previous term by the application of a given number-theoretic function, are the subject of Section 5. In particular, if this function is chosen to be the sum of certain divisors, we obtain (generalized) aliquot sequences. Section 6, finally, discusses four smaller subjects, in order to illustrate the broad range of number-theoretical topics, which have been studied at CWI in the past 25 years.

Traditionally, computers have played an important helping role in number theory. Early computations were with integers and rationals, but the discovery by Riemann of the connection between the distribution of primes and the complex zeros of the Riemann zeta function (see Section 2.1) has stimulated computations on analytic functions. A survey of analytic computations in number theory will appear soon [98].

In the early seventies our research was carried out with the help of the Electrologica EL X8 computer. Jobs were submitted on punch cards or paper tape. Development and debugging of programs, especially the paper tape ones, was a time-consuming activity. In the early eighties, a Control Data Cyber 175 computer at SARA (Academic Computer Center Amsterdam) became our favourite number cruncher. The advent, in 1984, of the CDC Cyber 205 vector computer at SARA marked the beginning of the vector and parallel computing era at CWI, at least for the computational number theory group. This machine was replaced, early 1990, by a Cray Y-MP vector computer with four CPUs; early 1994 this one was succeeded by a Cray C90, also with four CPUs. Meanwhile, powerful workstations have become a common researcher's tool. We now have access to 70 SGI workstations which can be used at night and in the weekends as a big parallel distributed memory computer. At present, this cluster of workstations is used mainly for the factorization of large numbers: the algorithms are extremely well parallelizable and require a minimal amount of communication (see Section 4).

Many number-theoretic computations deal with *large* integers which do not fit in one computer word. Therefore, one often has to resort to multiple-precision packages. Some of our factorization software (see Section 4) is built on a multiple-precision package of Dik Winter for basic integer arithmetic. A very reliable higher-level package which we have often used, e.g., in [97] and [118], is Brent's MP-package [19]. A more recent package, which runs efficiently on vector computers, and which employs advanced algorithms like FFT for operations on extremely large numbers, is Bailey's MPFUN-package [6]. The packages of Brent and Bailey work with a floating point representation of the large numbers involved, but by a small extension of the precision the packages can be used conveniently for exact computations with large integers. A very fast symbolic package which has been especially tailored to number-theoretic computations is PARI [8]; it provides tools which are rarely found in other symbolic packages, such as direct handling of mathematical objects, for example p-adic numbers, algebraic numbers and finite fields, etc. More general, but less efficient for large-scale computations, are *computer algebra* packages like MAPLE and MATHEMATICA. VARGA [135] has recently discussed a set of mathematical problems and conjectures which require the help of software for multiple-precision arithmetic. This illustrates the power of such software as a modern tool for attacking mathematical problems and conjectures.

2. THE RIEMANN HYPOTHESIS: SEPARATION AND LOCATION OF THE COMPLEX ZEROS OF $\zeta(s)$

The Riemann hypothesis is one of the most famous conjectures in pure mathematics. The standard textbook on this subject is [132]. For an excellent treatment of the history and the computational aspects of the Riemann hypothesis, we refer to [43].

Consider the function $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$, where $s = \sigma + it$ is a complex variable. If $\sigma > 1$, then the series converges, so that $\zeta(s)$ is properly defined there. Riemann, who was the first to study this function for *complex* s, showed by using analytic continuation that there exists a unique function which coincides with $\zeta(s)$ for $\sigma > 1$, and which is analytic in the whole complex plane, except at the point $s = 1$ (where the function has a pole of order 1). This function is known as the *Riemann zeta function* and it plays a prominent role in prime number theory. If we define

$$\xi(s) = \frac{1}{2}s(s-1)\Gamma(s/2)\pi^{-s/2}\zeta(s), \tag{1}$$

where Γ is Euler's gamma-function, i.e., a generalization of the factorial function $n!$ ($\Gamma(n+1) = n!$ for positive integers n), then $\xi(s)$ is an entire function satisfying the *functional equation*

$$\xi(s) = \xi(1-s). \tag{2}$$

Using well-known properties of the gamma-function, it follows that $\zeta(s) = 0$ for $s = -2n$, $n = 1, 2, 3, \ldots$. These zeros are the so-called *trivial* zeros of $\zeta(s)$.

This terminology suggests that $\zeta(s)$ has more zeros. These do exist indeed and are located in the so-called *critical strip* $0 \le \sigma \le 1$. It can be proved that the function $\xi(\frac{1}{2}+is)$ is an *even entire function of order* 1. According to Hadamard's general theory of entire functions, such functions have an infinite number of zeros. By means of the so-called *Euler product formula*

$$\sum_{n=1}^{\infty} n^{-s} = \prod_{p \text{ prime}} (1-p^{-s})^{-1} \qquad (\sigma > 1),$$

and by using (2), it is not difficult to show that $\xi(s)$ has no zeros outside the critical strip. The precise location of these zeros has been the subject of much research. Since

$$(1-2^{1-s})\zeta(s) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \ldots > 0 \qquad (0 < s < 1),$$

and $\zeta(0) = -\frac{1}{2}$, $\zeta(s)$ has no zeros on the real axis between 0 and 1. Moreover, we have $\zeta(\overline{s}) = \overline{\zeta(s)}$, so that the complex zeros lie symmetrically with respect to the real axis. In combination with the functional equation this implies that these zeros either lie on the line $\sigma = \frac{1}{2}$, or lie in pairs symmetrically with respect to this line. In a famous paper published in 1859 [122], Riemann wrote that it is very likely that all these zeros lie *on* the line $\sigma = \frac{1}{2}$. So far, nobody has been able to (dis)prove this assertion, which is known now as the *Riemann hypothesis.*

What is the relation between the Riemann hypothesis and prime number theory? Consider the function $\pi(x)$ which denotes the number of primes $\le x$. As early as in 1792 or 1793, Gauss conjectured that the density of the prime numbers close to x is approximately equal to $1/\log x$, and that the so-called logarithmic integral

$$\mathrm{li}(x) = \int_0^x \frac{dt}{\log t} \tag{3}$$

is a good approximation of the function $\pi(x)$. Extensive numerical computations [123, pp. 380–383] suggest that the error in this approximation is proportional to $\sqrt{x}$: for $x = 10^{12}$, 10^{14}, 10^{16}, 10^{17}, 10^{18} we have $(\pi(x) - \mathrm{li}(x))/\sqrt{x} = -0.038$, -0.031, -0.032, -0.025, and -0.022, respectively. The following is known: if, for some η,

$$\pi(x) = \mathrm{li}(x) + \mathcal{O}(x^{\eta}) \quad \text{as} \quad x \to \infty,$$

then $\zeta(s)$ has no zeros in the half plane $\sigma > \eta$. Conversely, if $\zeta(s) \neq 0$ for $\sigma > \eta$, then

$$\pi(x) = \mathrm{li}(x) + \mathcal{O}(x^{\eta} \log x) \quad \text{as} \quad x \to \infty.$$

We can safely choose $\eta = 1$ but not $\eta < 1$ (see below), although the experiments suggest that $\eta = 1/2$ is still possible.

What is known about the location of the complex zeros of $\zeta(s)$? Extensive numerical computations have *proved* that the first 1.5×10^9 complex zeros of $\zeta(s)$ are *all simple* and lie on the line $\sigma = \frac{1}{2}$ [78], and the same holds for long sequences of consecutive zeros in the neighborhood of zeros of rank 10^{18}, 10^{19}, and 10^{20} [95]. The famous Prime Number Theorem says that $\pi(x) \sim x/\log x$ as $x \to \infty$. One can show that this is equivalent to the statement that $\zeta(s)$ has no zeros on the line $\sigma = 1$. So far, this result has not been improved essentially, i.e., with our present knowledge we cannot exclude the possibility that there are complex zeros of $\zeta(s)$ arbitrarily close to the line $\sigma = 1$. What we do know is that most complex zeros lie close to the critical line ($\sigma = \frac{1}{2}$) in the sense that for each $\epsilon > 0$ all complex zeros have a distance to the critical line which is $< \epsilon$, with the possible exception of a subset of asymptotic density 0 within the set of all non-trivial zeros. For the *total* number of complex zeros $\beta + i\gamma$ with $0 < \gamma \leq T$, denoted by $N(T)$, we have

$$N(T) \sim \frac{T}{2\pi} \log \frac{T}{2\pi} - \frac{T}{2\pi} + \mathcal{O}(\log T) \quad \text{as } T \to \infty. \tag{4}$$

With respect to the zeros *on* the critical line, it is known that at least two-fifths of all complex zeros of $\zeta(s)$ lie on that line [33]. For more references and details, see [87, 126].

At CWI a considerable amount of numerical work has been carried out in relation to the complex zeros of $\zeta(s)$ [22, 77, 78, 80, 103, 137, 110, 111, 97, 117, 60].

In Section 2.1 we describe computations carried out to verify the Riemann hypothesis for the first 1.5×10^9 complex zeros of $\zeta(s)$. As a result, the Riemann hypothesis is true for $0 < \Im s < 545{,}439{,}823$.

In Section 2.2 we describe joint work of A.M. Odlyzko and the first author resulting in a disproof of the conjecture of Mertens. For this purpose the first 2000 complex zeros of $\zeta(s)$ were computed with an accuracy of about 105 decimal digits. The truth of the Mertens conjecture would have implied the truth of the Riemann hypothesis.

The difference $\pi(x) - \mathrm{li}(x)$ is known to have infinitely many sign changes. Nevertheless, for all values of x for which this difference has been computed explicitly, it is found to be negative. In Section 2.3 we describe how from the knowledge of the truth of the Riemann hypothesis in the critical strip with $0 < \Im s < 450{,}000$, and from the knowledge of the first 15,000 complex zeros to about 28 digits, and the next 35,000 to about 14 digits, it was proved that $\pi(x) - \mathrm{li}(x)$ changes sign for some $x < 6.69 \times 10^{370}$. The method used is similar to the one used by SHERMAN LEHMAN [64] who proved that a sign change occurs for some $x < 1.65 \times 10^{1165}$.

The mean square $I(t)$ of the Riemann zeta function on the critical line:

$$I(t) = \int_0^t \left| \zeta \left(\frac{1}{2} + iu \right) \right|^2 du$$

is known to have the "asymptotic expansion"

$$I(t) = t \log \frac{t}{2\pi} + (2\gamma - 1)t + o(t) \quad \text{as } t \to \infty$$

(where γ is Euler's constant). The $o(t)$-term plays a central role in the theory of the Riemann zeta function. In Section 2.4 computations are described of the zeros below $t = 500,000$ of the function

$$I(t) - t\left(\log \frac{t}{2\pi} + 2\gamma - 1\right) - \pi$$

(which has mean value 0). For these computations we used the Euler-Maclaurin and Riemann-Siegel formulas for computing $\zeta(\frac{1}{2}+it)$, described in Section 2.1.

2.1. Numerical verification of the Riemann hypothesis

2.1.1. Mathematical background

With the help of the well-known Newton process it is possible to find an approximation of a complex zero of $\zeta(s)$, but this process can not be used to *prove rigorously* that such a zero has real part exactly equal to $\frac{1}{2}$. Fortunately, the problem can be formulated in a different way such that it is really possible to give a *mathematical proof* of the truth of the Riemann hypothesis in a finite part of the critical strip, namely as follows.

In the previous section we have seen that the non-trivial zeros of $\zeta(s)$ are precisely the zeros of $\xi(s)$. From (2) and $\xi(\overline{s}) = \overline{\xi(s)}$ it follows that

$$\xi\left(\frac{1}{2}+it\right) = \xi\left(\frac{1}{2}-it\right) = \overline{\xi\left(\frac{1}{2}+it\right)},$$

so that, for real t, $\xi(\frac{1}{2}+it)$ must be real-valued. This means that complex zeros of $\xi(s)$ which lie on the line $\sigma = \frac{1}{2}$ can be determined by finding *sign changes* of the continuous function $\xi(\frac{1}{2}+it)$. Furthermore, it is appropriate to divide this function by the real quantity

$$\frac{1}{2}(-t^2 - \frac{1}{4})\left|\Gamma(\frac{1}{4}+\frac{it}{2})\pi^{-\frac{1}{4}-\frac{it}{2}}\right|.$$

The function obtained in this way is denoted by $Z(t)$, and we have, using (1),

$$Z(t) = \frac{\xi(1/2+it)}{\frac{1}{2}(-t^2-\frac{1}{4})|\Gamma(\frac{1}{4}+\frac{it}{2})\pi^{-\frac{1}{4}-\frac{it}{2}}|} = \frac{\Gamma(\frac{1}{4}+\frac{it}{2})}{|\Gamma(\frac{1}{4}+\frac{it}{2})|}\frac{\pi^{-\frac{1}{4}-\frac{it}{2}}}{|\pi^{-\frac{1}{4}-\frac{it}{2}}|}\zeta(\frac{1}{2}+it) =$$

$$= \exp\left(i\Im \log\Gamma(\frac{1}{4}+\frac{it}{2})\right)\pi^{-it/2}\zeta(\frac{1}{2}+it),$$

so that $|Z(t)| = |\zeta(\frac{1}{2}+it)|$. Like $\xi(\frac{1}{2}+it)$, $Z(t)$ is real-valued for real t and its (real) zeros γ correspond precisely to the zeros $\frac{1}{2}+i\gamma$ of $\zeta(s)$ on the critical line. Furthermore, $Z(t)$ is continuous, so that, if we can *prove* that $Z(t)$ changes sign between t_1 and t_2, then we have shown the existence of a zero s_0 (of odd multiplicity) of $\zeta(s)$ *on* the line $\sigma = \frac{1}{2}$ with $t_1 < \Im s_0 < t_2$.

We write

$$Z(t) = e^{i\theta(t)}\zeta(\frac{1}{2} + it)$$

where

$$\theta(t) = \Im \log \Gamma(\frac{1}{4} + \frac{it}{2}) - \frac{t}{2}\log \pi$$

with $\theta(t)$ continuous and $\theta(0) = 0$. In the next section we will describe two methods to compute $Z(t)$. By means of Stirling's formula for $\log \Gamma(s)$ it is possible to derive the following asymptotic expansion for $\theta(t)$:

$$\theta(t) = \frac{t}{2}\log\frac{t}{2\pi} - \frac{t}{2} - \frac{\pi}{8} + \sum_{k=1}^{n} \frac{|B_{2k}|(1-2^{1-2k})}{4k(2k-1)} t^{1-2k} + r_n(t), \tag{5}$$

where $B_2 = 1/6$, $B_4 = -1/30$, $B_6 = 1/42$, $B_8 = -1/30$, ... are the Bernoulli-numbers, and

$$|r_n(t)| < \frac{(2n)!}{(2\pi)^{2n+2}t^{2n+1}} + \exp(-\pi t)$$

for all $t > 0$ and $n \geq 0$. The function $\theta(t)$ has a minimum value of about -3.53 in the neighborhood of $t = 2\pi$, and is monotonically increasing for $t \geq 7$. For integral $m \geq -1$ we define the m-th *Gram point* g_m as the unique solution $x \in [7, \infty)$ of the equation

$$\theta(x) = m\pi.$$

After Riemann, GRAM [47] was the first to work on the numerical verification of the Riemann hypothesis. He computed 15 zeros of $\zeta(s)$ on the line $\sigma = \frac{1}{2}$. He also succeeded in proving that his list contained *all* (ten) zeros in the interval $0 \leq t \leq 50$, so that the Riemann hypothesis holds true for this interval. An important observation which Gram made was that $Z(t)$ changes sign between two consecutive Gram points; to be more precise:

$$\operatorname{sign} Z(g_n) = (-1)^n. \tag{6}$$

A Gram point for which (6) holds, is called "good", otherwise it is called "bad". "Gram's Law" is known as the assertion that all Gram points are good, although nowadays we know that this "Law" fails infinitely often. What is correct is that *on average* there is exactly one zero of $Z(t)$ between two consecutive Gram points. If one wants to prove the Riemann hypothesis in a given finite part of the critical strip, this is an extremely handy "rule-of-thumb" for efficiently finding sign changes of $Z(t)$. It can be formulated more precisely as follows: let

$$S(t) = N(t) - 1 - \frac{\theta(t)}{\pi} \tag{7}$$

where $N(t)$ is the function defined above formula (4). Then Gram's law holds whenever $|S(t)| < 1$. Numerical experiments have shown that this is indeed the case in more than 70% of the range where the first 1,500,000,000 complex zeros of $\zeta(s)$ are located. In the rest of this range, $|S(t)| < 2$ holds almost everywhere and $|S(t)| > 3$ has not been observed so far, although it is known that $S(t)$ is unbounded.

We have seen how in a finite part of the critical strip zeros of $\zeta(s)$ can be found which lie *on the critical line*. If we can prove now that these are *all* the zeros in that part of the critical strip, then here the Riemann hypothesis is true. The following theorem of Littlewood and Turing is very helpful:

> *If $Z(t)$ has at least $n+1$ zeros between $t = 0$ and a good Gram point $t = g_n$, and if for every next good Gram point $t = g_{n+j}$, $j = 1, \ldots, k$, with $k = \lceil 0.0061(\log g_n)^2 + 0.08 \log g_n \rceil$, $Z(t)$ has at least $n + j + 1$ sign changes in the interval $[0, g_{n+j}]$, then $\zeta(s)$ has at most $n+1$ zeros with imaginary part in the interval $[0, g_n]$.*

In the case that not all k Gram points g_{n+j}, $j = 1, \ldots, k$, are good, a more general version of this theorem can be invoked [20, Theorem 3.2].

To summarize, we can verify the Riemann hypothesis up to a good Gram point g_n by finding $n+1$ sign changes of $Z(t)$ in the interval $[0, g_n]$ and by finding sufficiently many sign changes between $t = g_n$ and a few subsequent good Gram points.

2.1.2. The formulas of Euler-Maclaurin and Riemann-Siegel

So far we have seen that zeros of $\zeta(s)$ on the critical line can be found by means of sign changes of the real-valued function

$$Z(t) = e^{i\theta(t)}\zeta(\frac{1}{2} + it). \tag{8}$$

So, it is necessary that we are able to determine the sign of $Z(t)$ with *mathematical certainty*. This means that, if we wish to compute $Z(t)$, together with its sign, on a computer, we have to make an analysis of all possible errors which might occur. Therefore, together with the expansion given below in (12), we shall give an upper bound for the error which we commit by truncating this expansion after a finite number of terms. Rounding errors can be analyzed by means of Wilkinson's backward error analysis [136]. The latter are generally much smaller than the former; therefore we shall not pay attention to them here (although, of course, they may not be neglected). Here, we describe the so-called *Euler-Maclaurin* and the *Riemann-Siegel* formulas for computing $\zeta(s)$, and $Z(t)$, respectively. The latter method is more efficient than the former to compute $\zeta(1/2 + it)$ for moderately large values of t ($t > 100$, say). ODLYZKO and SCHÖNHAGE [96] have given algorithms which are more efficient than the Riemann-Siegel formula, when *many values at closely spaced points* are needed (like in the numerical verification of the Riemann hypothesis).

The *Euler-Maclaurin* formula enables us to compute $\zeta(s)$ to any prescribed accuracy, provided m and n are chosen properly:

$$\zeta(s) = \sum_{j=1}^{n-1} j^{-s} + \frac{1}{2}n^{-s} + \frac{n^{1-s}}{s-1} + \sum_{k=1}^{m} T_{k,n}(s) + E_{m,n}(s), \tag{9}$$

where

$$T_{k,n}(s) = \frac{B_{2k}}{(2k)!} n^{1-s-2k} \prod_{j=0}^{2k-2} (s+j) \tag{10}$$

and

$$|E_{m,n}(s)| < \left| T_{m+1,n}(s) \frac{s+2m+1}{\sigma+2m+1} \right| \tag{11}$$

for all $m \geq 0$, $n \geq 1$, and $\sigma = \Re s > -(2m+1)$. If we use this formula for $s = \frac{1}{2} + it$, we may choose $n \approx t/2\pi$. It is also sufficient to choose $n = \mathcal{O}(t)$ and $m = \mathcal{O}(t)$. Therefore, the amount of work is roughly proportional to t.

The *Riemann-Siegel* formula is (sort of) an asymptotic expansion of $Z(t)$. For large values of t this formula is much more efficient than the Euler-Maclaurin formula, since the required amount of work is $\mathcal{O}(t^{1/2})$ instead of $\mathcal{O}(t)$.

Let $\tau := t/(2\pi)$, $m := \lfloor \tau^{1/2} \rfloor$, and $z := 2(\tau^{1/2} - m) - 1$. The Riemann-Siegel formula with $n+1$ error terms is given by

$$Z(t) = 2\sum_{k=1}^{m} k^{-1/2} \cos[t \log k - \theta(t)] + \tag{12}$$

$$+(-1)^{m+1}\tau^{-1/4} \sum_{i=0}^{n} \Phi_i(z)(-1)^i \tau^{-i/2} + R_n(\tau),$$

where

$$R_n(\tau) = \mathcal{O}(\tau^{-(2n+3)/4})$$

for $n \geq -1$ and $\tau > 0$ (for $\theta(t)$, see (5)). Here, the $\Phi_i(z)$ are certain entire functions which can be expressed in terms of the derivatives of

$$\Phi_0(z) := \Phi(z) := \frac{\cos[\pi(4z^2+3)/8]}{\cos(\pi z)}.$$

We have, for example,

$$\Phi_1(z) = \frac{\Phi^{(3)}(z)}{12\pi^3}$$

and

$$\Phi_2(z) = \frac{\Phi^{(2)}(z)}{16\pi^2} + \frac{\Phi^{(6)}(z)}{288\pi^4}.$$

For $R_n(\tau)$, $n = 0, 1, 2, 3$, and $\tau > 32$ ($t > 200$) the following upper bounds hold [45]:

$$|R_n(\tau)| < d_n \tau^{-(2n+3)/4}$$

with $d_0 = 0.032$, $d_1 = 0.0054$, $d_2 = 0.00045$ and $d_3 = 0.0005$.

If we write $\Phi_i(z)$ as a power series in z:

$$\Phi_i(z) := \sum_{j=0}^{\infty} c_{ij} z^j,$$

then it turns out that Φ_i has an *even* power series for even i, and an *odd* power series for odd i. For $i = 0, 1, 2$ and 3, the first 15 non-zero coefficients c_{ij} of $\Phi_i(z)$ are given in Table 1.

j	$c_{0,j}$	$c_{1,j+1}$	$c_{2,j}$	$c_{3,j+1}$
0	0.38268343237	0.02682510263	0.00518854283	0.00133971609
2	0.43724046808	−0.01378477343	0.00030946584	−0.00374421514
4	0.13237657548	−0.03849125048	−0.01133594108	0.00133031789
6	−0.01360502605	−0.00987106630	0.00223304574	0.00226546608
8	−0.01356762197	0.00331075976	0.00519663741	−0.00095485000
10	−0.00162372532	0.00146478086	0.00034399144	−0.00060100385
12	0.00029705354	0.00001320794	−0.00059106484	0.00010128858
14	0.00007943301	−0.00005922749	−0.00010229973	0.00006865733
16	0.00000046556	−0.00000598024	0.00002088839	−0.00000059854
18	−0.00000143273	0.00000096413	0.00000592767	−0.00000333166
20	−0.00000010355	0.00000018335	−0.00000016424	−0.00000021919
22	0.00000001236	−0.00000000447	−0.00000015161	0.00000007891
24	0.00000000179	−0.00000000271	−0.00000000591	0.00000000941
26	−0.00000000003	−0.00000000008	0.00000000209	−0.00000000096
28	−0.00000000002	0.00000000002	0.00000000018	−0.00000000019

TABLE 1. Coefficients c_{ij} of $\Phi_i(z)$

2.1.3. Large-scale computations verifying the Riemann hypothesis for the first 1.5×10^9 complex zeros of $\zeta(s)$

In a series of four papers [20], [22], [77], [78], the results were presented of large-scale computations concerning the verification of the Riemann hypothesis for the first 1,500,000,001 complex zeros. Brent checked the zeros with rank up to 156,800,001 and Van de Lune, Te Riele, and Winter (LRW) checked the others with rank up to 1,500,000,001, by using the Riemann-Siegel formula (12), with $n = 2$ (Brent) and $n = 1$ (LRW), respectively.

The problem is to *separate* the zeros of $Z(t)$ by evaluating Z in consecutive Gram points and checking the signs. On average there is exactly one zero in a Gram interval (i.e., between two consecutive Gram points). A sign change in two consecutive Gram points means that there are 1, or 3, ... zeros, and no sign change means 0, or 2, ... zeros. It turned out that among the first 1.5×10^9 Gram intervals, 72.6% have 1 zero, 13.8% have no zeros, 13.4% have 2 zeros, 0.18% have 3 zeros, and that there are only 33 Gram intervals with 4 zeros. LRW developed a strategy to trace the correct number of zeros by a close-to-minimal number of Z-evaluations, by carefully looking at the behaviour of Z in Gram intervals violating Gram's law. They reduced the average number of Z-evaluations needed to separate one zero to 1.2 (against 1.4 in Brent's program).

Sign changes were determined rigorously with the help of a complete error analysis of all errors made in the computation of $Z(t)$. A fast single precision (46 bits' accuracy) and a slow double precision (93 bits' accuracy) subroutine for computing $Z(t)$ were developed. The slow, but more accurate version was invoked when the fast, less accurate version produced such a small $|Z|$-value that the sign of Z could not be determined rigorously, given the upper bound of the error determined by the error analysis. With the slow, accurate version not a single value of Z was encountered for which the corresponding sign could not be determined without doubt.

The major part of the computations were done on a CYBER 205 vector computer, where the most time-consuming part of the method, the computation of the first sum in (12), was vectorized. The time required for one $Z(t)$-evaluation for t at the end of the interval under investigation (where $t \approx 5.45 \times 10^8$ and $m \approx 9300$) was about 2 msec [137]. Many statistics were collected concerning places where Z has 0 or at least 2 zeros between two consecutive Gram points. Also intervals where consecutive Z-zeros are extremely close to each other and intervals where they are extremely far apart, were recorded. The statistics collected show that with the LRW strategy at least 1.137 Z-evaluations were needed to separate the first 1.5×10^9 zeros of $\zeta(s)$, so that the overhead amounted to $100(1.2 - 1.137)/1.137 = 5.5\%$. On a CYBER 205 about 1000 CPU-hours were spent on this project, and on a CYBER 175/750 about 900 CPU-hours. The program on the CYBER 205 ran about 10 times faster than that on the CYBER 175/750.

2.2. Disproof of the Mertens conjecture

The Möbius function $\mu(n)$ is defined as follows:

$$\mu(n) := \begin{cases} 1, & n = 1, \\ 0, & \text{if } n \text{ is divisible by the square of a prime number}, \\ (-1)^k, & \text{if } n \text{ is the product of } k \text{ distinct primes.} \end{cases}$$

Taking the sum of the values of $\mu(n)$ for all $n \leq x$, we obtain the function

$$M(x) = \sum_{1 \leq n \leq x} \mu(n),$$

which is the difference between the number of squarefree positive integers $n \leq x$ with an even number of prime factors and those with an odd number of prime factors.

In 1885, Stieltjes claimed in a letter to Hermite to have a proof that the function $M(x)/\sqrt{x}$ oscillates between two fixed bounds, no matter how large x

may be. In passing, Stieltjes added that one could probably take -1 and $+1$ for these bounds. It is possible that this assertion was based on some tables of $M(x)$ which were found in Stieltjes' inheritance. The motivation for Stieltjes' work on $M(x)$ was that the size of $M(x)$ is closely related to the location of the complex zeros of the Riemann zeta function. In fact, the boundedness of $M(x)/\sqrt{x}$ would imply the Riemann hypothesis as follows. For $\sigma = \Re s > 1$, we have (by using partial summation)

$$1/\zeta(s) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \sum_{n=1}^{\infty} \frac{M(n) - M(n-1)}{n^s} =$$

$$= \sum_{n=1}^{\infty} M(n) \left\{ \frac{1}{n^s} - \frac{1}{(n+1)^s} \right\} = \sum_{n=1}^{\infty} M(n) \int_n^{n+1} \frac{s dx}{x^{s+1}} =$$

$$= s \sum_{n=1}^{\infty} \int_n^{n+1} \frac{M(x)dx}{x^{s+1}} = s \int_1^{\infty} \frac{M(x)dx}{x^{s+1}},$$

since $M(x)$ is constant on each interval $[n, n+1)$. The boundedness of $M(x)/\sqrt{x}$ would imply that the last integral in the above formula defines a function analytic in the half plane $\sigma > \frac{1}{2}$, and this would give an analytic continuation of $1/\zeta(s)$ from $\sigma > 1$ to $\sigma > \frac{1}{2}$. In particular, this would imply that $\zeta(s)$ has no zeros in the half plane $\sigma > \frac{1}{2}$, which is, by the functional equation for $\zeta(s)$, equivalent to the Riemann hypothesis. In addition, it is not difficult to deduce from the above formula that all complex zeros of $\zeta(z)$ would be simple (see, e.g., [97, p.141]).

After Stieltjes, many other researchers have computed tables of $M(x)$, in order to collect more numerical data about the behaviour of $M(x)/\sqrt{x}$. The first one after Stieltjes was Mertens who, in 1897, published a paper with a 50–page table of $\mu(n)$ and $M(n)$ for $n = 1, 2, \ldots, 10000$. Based on this table, Mertens concluded that the inequality

$$|M(x)| < \sqrt{x}, \quad x > 1,$$

is "very probable". This is now known as the *Mertens conjecture.*

In 1942, Ingham [59] published a paper which raised the first serious doubts about the validity of the Mertens conjecture. Ingham's paper showed that it is possible to prove the existence of certain large values of $|M(x)|/\sqrt{x}$ without explicitly computing $M(x)$. This stimulated a series of subsequent papers until, in 1985, Odlyzko and Te Riele [97] finally disproved the Mertens conjecture. Some historical notes are given in [115, 119].

Here, we shall give a sketch of the indirect disproof of the Mertens conjecture, which does not give any single value of x for which $|M(x)|/\sqrt{x} > 1$. Write $x = e^y$, $-\infty < y < \infty$, and define

$$m(y) := M(x)x^{-1/2} = M(e^y)e^{-y/2}$$

and

$$\underline{m} := \liminf_{y\to\infty} m(y), \quad \overline{m} := \limsup_{y\to\infty} m(y).$$

Then we have the following ([59], [61], [97])

THEOREM 1. *Suppose that* $K(y) \in C^2(-\infty,\infty)$, $K(y) \geq 0$, $K(-y) = K(y)$, $K(y) = \mathcal{O}((1+y^2)^{-1})$ as $y \to \infty$, *and that the function* $k(t)$ *defined by*

$$k(t) = \int_{-\infty}^{\infty} K(y) e^{-ity} dy$$

satisfies $k(t) = 0$ *for* $|t| \geq T$ *for some* T, *and* $k(0) = 1$. *If the zeros* $\rho = \beta + i\gamma$ *of the Riemann zeta function with* $0 < \beta < 1$ *and* $|\gamma| < T$ *satisfy* $\beta = \frac{1}{2}$ *and are simple, then for any* y_0,

$$\underline{m} \leq h_K(y_0) \leq \overline{m},$$

where

$$h_K(y) = \sum_{\rho} k(\gamma) \frac{e^{i\gamma y}}{\rho\zeta'(\rho)}.$$

Hence, by finding large values of $|h_K(y)|$, which is less difficult than finding large values of $|M(x)|/\sqrt{x}$, it is possible to disprove the Mertens conjecture.

The simplest known function $k(t)$ that satisfies the conditions of Theorem 1 is based on the Féjer kernel

$$K(y) = \left(\frac{\sin \pi y}{\pi y}\right)^2$$

used by Ingham, for which

$$k(t) = \begin{cases} 1 - |t|/T, & |t| \leq T, \\ 0, & |t| > T. \end{cases} \tag{13}$$

This yields

$$h_K(y) = \sum_{|\gamma|<T} \left(1 - \frac{|\gamma|}{T}\right) \frac{e^{i\gamma y}}{\rho\zeta'(\rho)} = 2 \sum_{0<\gamma<T} \left(1 - \frac{\gamma}{T}\right) \frac{\cos(\gamma y - \psi_\gamma)}{|\rho\zeta'(\rho)|}, \tag{14}$$

where

$$\psi_\gamma = \arg \rho\, \zeta'(\rho).$$

It is known that $\sum_\rho |\rho\, \zeta'(\rho)|^{-1}$ diverges, so that the sum of the cos-coefficients in (14) can be made arbitrarily large by choosing T large enough. If we could manage to find a value of y such that all $\gamma y - \psi_\gamma$ were close to integer multiples of 2π, then we could make $h_K(y)$ arbitrarily large. This would contradict, by Theorem 1, the Mertens conjecture $|M(x)|/\sqrt{x} < 1$, and even any conjecture of the form $|M(x)|/\sqrt{x} < C$, for any constant $C > 0$. JURKAT and PEYERIMHOFF [61] observed that the size of the sum $h_K(y)$ is determined largely by the first few terms since the numbers $(\rho\zeta'(\rho))^{-1}$ typically appear to be of order ρ^{-1}. Therefore, they searched for values of y such that

$$\cos(\gamma_1 y - \pi\psi_1) = 1$$

and

$$\cos(\gamma_i y - \pi\psi_i) > 1 - \epsilon \quad \text{for} \quad i = 2, \ldots, N+1,$$

for a suitably chosen ϵ, N being as large as feasible. This gives an inhomogeneous Diophantine approximation problem, for which Jurkat and Peyerimhoff devised an ingenious algorithm. In addition, they used a kernel which is different from the one which induces (13), viz.,

$$K(y) = \frac{2}{\pi^2}\left(\frac{2\cos\pi y}{1-4y^2}\right)^2, \tag{15}$$

for which $k(t) = g(t/T)$ where

$$g(t) = \begin{cases} (1-|t|)\cos(\pi t) + \pi^{-1}\sin(\pi|t|), & |t| \le 1, \\ 0, & |t| > 1. \end{cases} \tag{16}$$

This function $k(t)$ gives more weight to the first cos-terms in the sum in (14) than (13) (cf. [110, Figure 1]). By applying their algorithm with $N = 12$ Jurkat and Peyerimhoff found that $\overline{m} \ge 0.779$.

A remarkably efficient algorithm of LENSTRA, LENSTRA and LOVÁSZ [66] for finding short vectors in lattices was applied by Odlyzko and Te Riele to the above mentioned inhomogeneous Diophantine approximation problem. It was estimated that $N = 70$ would be sufficient, in order to disprove the Mertens conjecture. Any value of y that would come out was likely to be quite large, viz., of the order of 10^{70} in size. Therefore, it was necessary to compute the first 2000 γ's to a precision of about 75 decimal digits (actually, 100 decimal digits were used). The best upper and lower bounds found for $\underline{m}$ and $\overline{m}$ were -1.009 and 1.06, respectively, which disproved the Mertens conjecture. Figure 1 gives the graph of the function $h_K(y_0+t)$, for $t \in [-3, +3]$, where K is given by (15), y_0 is given on the next two lines:

$$y_0 = -14045\,28968\,05929\,98046\,79036\,16303\,99781$$
$$12740\,05919\,99789\,73803\,99659\,60762.521505,$$

and $h_k(y_0) = 1.061545$. It shows just how atypical large values of $h_K(y)$ are, and that the local maximum found for this y_0 is really a needle in a haystack. Figure 2 is an enlargement of the central part of Figure 1. As stated above, the disproof is ineffective: no actual value of x, nor an upperbound for x

FIGURE 1. Graph of the function $h_K(y_0 + t)$ for $t \in [-3, +3]$

where $|M(x)|/\sqrt{x}$ becomes large, is derived in [97]. PINTZ [99] gave an *effective* disproof in the sense that he showed that $|M(x)|/\sqrt{x} > 1$ for some $x \leq \exp(3.21 \times 10^{64})$. In his proof the sum

$$h_1(y, T, \epsilon) := 2 \sum_{0<\gamma<T} e^{-\epsilon\gamma^2} \left[\frac{\cos(\gamma y - \pi\psi_\gamma)}{|\rho\zeta'(\rho)|} \right]$$

had to be evaluated for $y \approx 3.2097 \times 10^{64}$ (the precise value is given in the last line of Table 3 in [97]), $T = 1.4 \times 10^4$, and $\epsilon = 1.5 \times 10^{-6}$. This computation was carried out by the first named author using the known 100–digit accurate values of the first 2000 γ's and the 28–digit accurate values of the next 12950 γ's ($< 1.4 \times 10^4$).

Various authors have computed the function $M(x)$ *systematically*, in order to find extrema of $M(x)/\sqrt{x}$. DRESS [42] established the bounds $-0.513 < M(x)/\sqrt{x} < 0.571$ for $200 < x \leq 10^{12}$. Recently, LIOEN and VAN DE LUNE [73] verified that the same result holds if one replaces the upper bound 10^{12} on x by 1.7889×10^{13}. The computations by Dress of $M(x)$ up to 10^{12} took 4000 CPU-hours on three Sun SPARCstations 2, while those of Lioen and Van de Lune (using vectorized sieving) took about 400 CPU–hours on a Cray C90 super vector computer.

FIGURE 2. Enlargement of the central part of Figure 1

The above computations of Dress, and Lioen and Van de Lune, are examples of *systematic* computations of number-theoretic functions. Earlier computations of this kind, carried out in the early 90s, deal with Gauss' lattice point problem [81, 133]. Similar results by VAN DE LUNE and E. WATTEL on Dirichlet's divisor problem will be published in 1995 [82]. Recently, Lioen and Van de Lune have developed a number of fast *vectorized* sieve procedures for the systematic computation of a large variety of number-theoretic functions. Applications to other functions, like Liouville's function and the sum of divisors' function (for the computation of amicable numbers), will be implemented in the near future.

2.3. The sign of the difference $\pi(x)-\mathrm{li}(x)$

One version of the Prime Number Theorem, proved in 1896 by Hadamard and (independently) by de la Vallée Poussin, states that $\pi(x) \sim \mathrm{li}(x)$ as $x \to \infty$. This result tells us that the ratio $\pi(x)/\mathrm{li}(x)$ tends to 1 as $x \to \infty$, but it does not say anything about the sign of the difference $\pi(x)-\mathrm{li}(x)$. This difference is *negative* for all values of x for which $\pi(x)$ has actually been computed. However, already in 1914, Littlewood proved that $\pi(x)-\mathrm{li}(x)$ changes sign infinitely often. In 1955, Skewes obtained the upper bound

$$\exp(\exp(\exp(\exp(7.705))))$$

for the smallest x for which $\pi(x) > \mathrm{li}(x)$. This bound was brought down considerably by SHERMAN LEHMAN in 1966 [64], who proved that between 1.53×10^{1165} and 1.65×10^{1165} there are more than 10^{500} consecutive integers x for which $\pi(x) > \mathrm{li}(x)$. Sherman Lehman performed two major computations to prove this result, namely a verification of the Riemann hypothesis for the first 250,000 zeros of $\zeta(s)$, i.e., for the complex zeros $\beta + i\gamma$ for which $0 < \gamma <$ 170,571.35, and the computation of the zeros $\frac{1}{2} + i\gamma$ of $\zeta(s)$ with $0 < \gamma <$ 12,000 to about 7 decimal places.

In [117], the first named author proved, by using Sherman Lehman's method and more extensive computations, that there are more than 10^{180} successive integers x between 6.62×10^{370} and 6.69×10^{370} for which $\pi(x) > \mathrm{li}(x)$. In this proof, use was made of the knowledge of the truth of the Riemann hypothesis for the complex zeros $\beta + i\gamma$ with $0 < \gamma <$ 450,000, and the knowledge of the first 15,000 complex zeros of $\zeta(s)$ with an accuracy of 28 digits, and the next 35,000 zeros with an accuracy of 14 digits. Sherman Lehman's method is based on finding values of T, α, and ω, for which the sum (which runs over the imaginary parts γ of the complex zeros $\frac{1}{2} + i\gamma$ of $\zeta(s)$)

$$H(T, \alpha, \omega) = - \sum_{0 < |\gamma| \le T} \frac{e^{i\gamma\omega}}{\rho} e^{-\gamma^2/2\alpha}$$

assumes a value > 1. After some experimentation near the value $\omega = 853.853$, suggested by Sherman Lehman, it was found that

$$H(\gamma_{50,000}, 2 \times 10^8, 853.852286) \approx 1.0240109\ldots,$$

where the absolute value of the error was bounded above by 5×10^{-6}. This value of H was used in a rather complicated theorem of Sherman Lehman to prove the upper bound on x given above for which $\pi(x) > \mathrm{li}(x)$.

2.4. The zeros of the error term in an asymptotic formula for the mean square of $|\zeta(\frac{1}{2} + it)|$

Let, for $t \ge 0$,

$$E(t) = \int_0^t \left| \zeta(\frac{1}{2} + iu) \right|^2 du - t \log\left(\frac{t}{2\pi}\right) - (2\gamma - 1)t \tag{17}$$

denote the error term in the asymptotic formula for the mean square of the Riemann zeta function on the critical line (where γ is Euler's constant). This function plays a central role in the theory of the Riemann zeta function. It has mean value π [51], and in [60] the zeros of $E(t) - \pi$ and related topics have been studied both from a theoretical and a numerical point of view. With respect to the gaps between consecutive zeros, it is shown there that the function $E(t) - \pi$ always has a zero of odd order in the interval $[T,\ T + cT^{1/2}]$ (for some $c > 0$, $T \ge T_0$). In the opposite direction it is shown that for every positive $\epsilon < 1/4$ there are arbitrarily large values of T such that $E(t) - \pi$ does not vanish in the interval $[T,\ T+T^{1/4-\epsilon}]$. An algorithm is given in [60] for the computation of the zeros of $E(t)-\pi$ below a given bound with the help of the Euler-Maclaurin and the Riemann-Siegel formulas for computing the values of $\zeta(\frac{1}{2}+it)$ in (17); the integral is approximated by means of the repeated Simpson rule with extrapolation. For $t \leq 500{,}000$, 42,010 zeros of $E(t)-\pi$ were found with this algorithm. The first 40 of them are given in Table 2. Various statistics concerning the zeros t_n, the zero differences $t_n - t_{n-1}$, and graphs of $E(t)-\pi$ are presented in [60]. As an example we give in Table 3 some data concerning the gaps $t_n - t_{n-1}$ between consecutive zeros of $E(t)-\pi$. The numerical results obtained in [60] were considered to support the conjecture that $t^{1/4}$ is the best upper bound for the gaps between consecutive zeros close to t. However, HEATH-BROWN [55] has shown recently that the true upper bound is about $t^{1/2}$.

n	t_n	n	t_n	n	t_n	n	t_n
1	1.199593	11	45.610584	21	81.138399	31	117.477368
2	4.757482	12	50.514621	22	85.065503	32	119.182848
3	9.117570	13	51.658642	23	90.665198	33	119.584571
4	13.545429	14	52.295421	24	95.958639	34	121.514013
5	17.685444	15	54.750880	25	97.460878	35	126.086783
6	22.098708	16	56.819660	26	99.048912	36	130.461139
7	27.706900	17	63.010778	27	99.900646	37	136.453527
8	31.884578	18	69.178386	28	101.331134	38	141.371299
9	35.337567	19	73.799939	29	109.007151	39	144.418515
10	40.500321	20	76.909522	30	116.158343	40	149.688528

TABLE 2. The first 40 zeros $t_1, \ldots, t_{40}$ of $E(t)-\pi$

3. ZEROS OF PARTIAL SUMS OF THE RIEMANN ZETA FUNCTION

In 1948, TURAN [134] related the Riemann hypothesis to certain zeros of partial sums of the Riemann zeta function. He showed that the Riemann hypothesis is true if there are positive numbers N_0 and C such that for all $N \in \mathbb{N}$, $N > N_0$ the functions

$$\zeta_N(s) := \sum_{n=1}^{N} n^{-s}, \quad (s \in \mathbb{C}, s = \sigma + it)$$

have no zeros in the halfplane $\sigma \geq 1 + C/\sqrt{N}$. In 1958, HASELGROVE [52] showed that there exist infinitely many $N \in \mathbb{N}$ for which $\zeta_N(s) = 0$ for some s with $\sigma > 1$. We shall call such zeros of $\zeta_N(s)$ *special zeros.* SPIRA [129], with the help of a computer, identified $N = 19, 22, \ldots, 27, 29, \ldots, 50$ as values for which $\zeta_N(s)$ has special zeros, but he did not explicitly compute any. In [76] two different methods have been studied for the explicit computation of special zeros of $\zeta_N(s)$. The first method systematically finds, for given N, the

n	$d_n := t_n - t_{n-1}$	$d_n/t_{n-1}^{1/2}$	$d_n/t_{n-1}^{1/4}$	$\log d_n/\log t_n$
2	3.557889	3.2484	3.3996	0.8137
5	4.140015	1.1249	2.1580	0.4945
10	5.162754	0.8685	2.1175	0.4435
20	3.109583	0.3620	1.0609	0.2612
50	2.834485	0.2096	0.7708	0.1994
100	2.389098	0.1132	0.5200	0.1427
200	0.075980	0.0024	0.0136	−0.3743
500	3.624824	0.0690	0.5000	0.1625
1000	0.753268	0.0096	0.0850	−0.0325
2000	0.596044	0.0051	0.0550	−0.0543
5000	7.983033	0.0403	0.5670	0.1964
10000	22.172542	0.0741	1.2818	0.2718
20000	1.240345	0.0027	0.0583	0.0176
42010	1.636594	0.0023	0.0615	0.0375

TABLE 3. Various data about the gaps between consecutive zeros of $E(t) - \pi$

special zeros (if any) of ζ_N with imaginary part in a given interval. The second method uses the property of $\zeta_N(s)$ that it is an *almost periodic* function in t [12], which roughly means that if we consider the function $\zeta_N(\sigma + it)$ for fixed σ in a given t-interval, and give a $\delta > 0$, then this part is repeated somewhere else, possibly not exactly, but with an error (in some norm) less than δ. Several almost periods were computed and by adding these to zeros of $\zeta_N(s)$ with real part very close to 1 (but not necessarily greater than 1), many special zeros were found explicitly. In the next Subsection we shall briefly explain the two methods, and give some examples. For details, we refer to [76] and [75, pp. 77–88].

In 1983, H.L. MONTGOMERY [88] proved that if c is such that $0 < c < \frac{4}{\pi} - 1$, then for all $N > N_0(c)$, $\zeta_N(s)$ has zeros in the half-plane

$$\sigma > 1 + c\frac{\log\log N}{\log N}.$$

This implies that the Riemann hypothesis cannot be proved by means of Turan's implication.

3.1. A systematic method for finding special zeros of $\zeta_N(s)$

This method is based on some knowledge of the zero curves of the real and imaginary parts of $\zeta_N(s)$ in the complex plane. Defining

$$R_N(\sigma, t) := \Re\zeta_N(s) = \sum_{n=1}^{N} \frac{\cos(t \log n)}{n^\sigma}$$

and

$$I_N(\sigma,t) := \Im\zeta_N(s) = -\sum_{n=1}^{N} \frac{\sin(t\log n)}{n^\sigma},$$

we obviously have $\zeta_N(s) = 0$ if and only if both $R_N(\sigma,t) = 0$ and $I_N(\sigma,t) = 0$.

First we consider the zero curves of $R_N(\sigma,t)$. It is easy to see that $R_N(\sigma,t) > 0$ for $\sigma \geq 2$ so that the zero-set of $\zeta_N(s)$ is located in the halfplane $\sigma < 2$. An analysis for large *negative* σ shows that the zero set of $R_N(\sigma,t)$ consists of simple zero curves having

$$-\infty + \frac{(2k+1)\pi i}{2\log N} \quad (k \in \mathbb{Z})$$

as asymptotical points. A further analysis shows that a zero curve starting at one of these asymptotic points moves to the right, makes a U-turn, and "returns" to some other asymptotic point at $\sigma = -\infty$ (possibly not a neighboring one).

For the zero curves of $I_N(\sigma,t)$ an analysis for large negative σ shows that the zero set of $I_N(\sigma,t)$ consists of simple zero curves having

$$-\infty + \frac{k\pi i}{\log N} \quad (k \in \mathbb{Z})$$

as asymptotical points, so these curves alternate with those of $R_N(\sigma,t)$ at $\sigma = -\infty$ with a fixed distance of $\pi/(2\log n)$. For large *positive* σ the zero curves of $I_N(\sigma,t)$ turn out to have

$$+\infty + \frac{k\pi i}{\log 2} \quad (k \in \mathbb{Z})$$

as asymptotical points. The zero curves starting at one of these points at $\sigma = -\infty$ show two different patterns: some go to the right, and return to some other point at $-\infty$; others traverse the s-plane, and go to one of the asymptotic points at $\sigma = +\infty$. The complete pattern is sketched in Figure 3. This suggests the heuristic principle on which the systematic method in [76] is based: find an interval $[t_1, t_2]$ on the line $\sigma = 1$ where a zero curve of $R_N(\sigma,t)$ crosses this line two times (i.e., where $R_N(1,t_1) = R_N(1,t_2) = 0$, and $R_N(1,t) < 0$ for $t_1 < t < t_2$). Check whether a zero curve of $I_N(\sigma,t)$ crosses the line $\sigma = 1$ in $[t_1,t_2]$, i.e., check whether $I_N(1,t)$ changes sign between t_1 and t_2. If so, there must be a *special* zero of $\zeta_N(s)$ nearby, namely where the zero curves of $I_N(\sigma,t)$ and $R_N(\sigma,t)$ intersect. This point can then easily be found with Newton's method. Usually it lies close to $(\sigma,t) = (1,t_1)$ or $(1,t_2)$.

The zeros of $R_N(\sigma,t)$ on the line $\sigma = 1$ can be found systematically by using the maximum slope principle as follows. Since

$$R_N(1,t) = \sum_{n=1}^{N} \frac{1}{n}\cos(t\log n)$$

FIGURE 3. Sketch of the zero curves of $R_N(\sigma, t)$ (solid) and $I_N(\sigma, t)$ (dotted)

we have

$$\frac{\partial}{\partial t} R_N(1,t) = -\sum_{n=2}^{N} \frac{\log n}{n} \sin(t \log n)$$

and

$$\sup_{t\in\mathbb{R}} \left| \sum_{n=2}^{N} \frac{\log n}{n} \sin(t \log n) \right| \le \sum_{n=2}^{N} \frac{\log n}{n} =: M_N.$$

Hence, we have a fixed upperbound for $\partial R_N(1,t)/\partial t$. This implies that if $R_N(1,a) = b$ with $b > 0$, then also $R_N(1,t) > 0$ for

$$a - \frac{b}{M_N} < t < a + \frac{b}{M_N}.$$

Starting with $t = 0$ and $R_N(1,0) = \sum_{1\le n\le N} n^{-1} > 0$, we jump forward with steps $R_N(1,t)/M_N$ until we find a value of t for which $R_N(1,t) < \epsilon$ for some suitably chosen $\epsilon > 0$. The maximum slope principle guarantees us that so far we have not passed a sign change of $R_N(1,t)$. Then we take a suitably chosen step δ hoping to find a *negative* value of R_N, thus crossing a zero of $R_N(1,t)$ and hence a point where the zero curve of $R_N(\sigma,t)$ crosses the line $\sigma = 1$. A similar procedure is followed to find the next sign change of $R_N(1,t)$ (from negative to positive). If successful, we have found two consecutive points on the line $\sigma = 1$ where a zero curve of $R_N(\sigma,t)$ crosses this line, and then we start to find a zero of $I_N(1,t)$ between these two points in a similar way in order to trace a possible special zero. This search is continued until all the intervals on the line $\sigma = 1$ with $0 \le t \le T$ (for some suitably chosen T depending on the CPU-time we wish to spend) have been found where the zero curves of $R_N(\sigma,t)$ cross that line. It should be remarked that this search method may miss two very close zeros of $R_N(1,t)$ in case their distance is smaller than δ. However, in that case (which we regard as improbable in view of our experiments with various choices of ϵ and δ) there is only a very small chance that just in between these close zeros a zero curve of $I_N(\sigma,t)$ crosses the line $\sigma = 1$.

This search method has been refined in several ways ([76] and [75]). It was implemented on a CDC 6600 computer and it quickly yielded the smallest special zeros of ζ_N for $N = 19$ and 23, and, after more computational effort, also for $N = 24, 25, 26, 31$ and 47. For $N = 22$ no special zero of $\zeta_N(s)$ was found in the interval $0 \le t \le 75{,}000{,}000$. However, with the (non-exhaustive) method described in the next section, we were able to find a special zero of ζ_{22} near t=558,159,406 (cf. Table 5 below), but this left us with the question whether that zero is the *smallest* special zero of ζ_{22}. Only recently, the first author succeeded to find the smallest special zero of ζ_{22} with the systematic method, in a computation which took about 105 CPU-hours on an SGI workstation. Table 4 lists the values of N and the corresponding smallest special zeros (rounded to 6 decimal digits) found by means of the systematic search method described above.

N	σ	t
19	1.001096	600884.203428
22	1.000825	343003465.806653
23	1.008497	8645.524423
24	1.004042	32520751.785995
25	1.000449	32520751.802239
26	1.001472	3202110.435371
31	1.007104	52331955.658761
47	1.000392	20749499.964083

TABLE 4. Smallest special zeros of $\zeta_N(s)$ found with systematic search method

3.2. A special zero search method based on almost periods

As indicated in the previous section, the function $\zeta_N(s)$ is almost periodic in t. If we would know a good almost period, we could add some of its multiples to *nearly* special zeros of $\zeta_N(s)$, and hope to find a special zero s_0 of $\zeta_N(s)$ with $\Re s_0 > 1$. The nearly special zeros could have been found with the systematic method of the previous section.

Crucial for exploiting this idea is to have good almost periods. Let p_j be the j-th prime ($p_1 = 2$, $p_2 = 3, \ldots$), let $\pi(x)$ be the number of primes $\leq x$, and let $j_0 \in \{1, 2, \ldots, \pi(N)\}$ be fixed. If we have "sufficiently good" (to be specified later) approximations of the $\pi(N)$ (> 1) numbers $\log p_j / \log p_{j_0}$ by rational numbers with the same denominator, then this gives a good almost period of $\zeta_N(s)$ as follows. Let k be the common denominator, i.e.,

$$k \frac{\log p_j}{\log p_{j_0}} \equiv \epsilon_j \bmod 1$$

where $\epsilon_{j_0} = 0$ and the other ϵ_j's are small (but not zero, since the logarithms of the primes are linearly independent over $\mathbb{Q}$). Let the decomposition of n ($\leq N$) into primes be written as $n = \prod_{j=1}^{\pi(N)} p_j^{\alpha_j(n)}$. Then for $T := 2\pi k / \log p_{j_0}$ and for any fixed $s \in \mathbb{C}$ we have

$$\zeta_N(s + iT) = \sum_{n=1}^{N} n^{-s} \exp(-iT \log n)$$

and

$$T \log n = k \frac{2\pi}{\log p_{j_0}} \sum_{j=1}^{\pi(N)} \alpha_j(n) \log p_j = 2\pi \sum_{j=1}^{\pi(N)} k \frac{\log p_j}{\log p_{j_0}} \alpha_j(n)$$

$$\equiv 2\pi \sum_{j=1}^{\pi(N)} \epsilon_j \alpha_j(n) \bmod 1.$$

If the ϵ_j's are small enough, we may expect $T \log n \bmod 1$ to be small, so that $|\zeta_N(s+iT) - \zeta_N(s)|$ will be small, for any $s \in \mathbb{C}$. In [76], we have applied two algorithms to find rational approximations of $\log p_j / \log p_{j_0}$, $(j = 1, 2, \ldots, \pi(N)$, $j \neq j_0)$, namely the modified JACOBI-PERRON [9] and the SZEKERES algorithm [131], the latter of which turned out to be more efficient than the former. We carried out various experiments, and in Table 5 we present the special zeros of $\zeta_N(s)$ (rounded as in Table 4) which we found for those values of N for which we could not find special zeros by means of the systematic method of the previous section.

N	σ	t
27	1.000410	61242054160408938.599681
29	1.003705	2589158977352418.117815
30	1.000358	2589158977352418.105466
32	1.001659	2589158977352418.102189
33	1.003113	2589158977352418.090841
34	1.002243	2589158977352418.079913
35	1.002719	2589158977352418.069385
37	1.003865	2589158977352418.068063
38	1.006121	2589158977352418.058852
39	1.008019	2589158977352418.049988
40	1.001380	2589158977352418.044122
41	1.000997	2589158977352418.052908

TABLE 5. Special zeros of $\zeta_N(s)$ found with the "almost period" method

About five years after the publication of [76], the well-known LLL-algorithm was published [66], and we expect that algorithm to yield much better results than the two other algorithms mentioned above. This implies that by means of the LLL-algorithm it might be possible to find special zeros of $\zeta_N(s)$ with smaller imaginary parts than those given in Table 5.

4. FACTORIZATION OF LARGE POSITIVE INTEGERS

Because of its fundamental role in the theory of the natural numbers, the problem of decomposing a given number into its prime factors ("factorization") has always attracted much attention from number theorists, both professionals and laymen. The discovery, in 1978, by RIVEST, SHAMIR and ADLEMAN [124] that the difficulty of factoring large numbers can be exploited in the design of so-called public-key cryptographic systems, has added an extra dimension to the natural attractivity of this field of research. In particular, the question of the size of the numbers which can be factored within a reasonable amount of physical time, is permanently actual here, because the safety of the cryptosystems mentioned above depends heavily on the answer.

For a given number to be decomposed into prime factors, one usually starts checking for small prime divisors by trial division up to a certain bound. Next, a compositeness test like the Rabin-Miller test [31, pp. 414–415] is applied to the remaining number, which determines with a high probability whether this is composite. If the test proves compositeness, one attempts to factor the number. If the test fails to prove compositeness, an attempt is made to prove that the number is prime. Until 1980, the available primality tests of N required the knowledge of the prime factors of $N-1$ (or $N+1, \dots$) and became impractical for numbers having more than 100 digits. A breakthrough came when ADLEMAN, POMERANCE and RUMELY [1] found a method to test primality of much larger numbers. This test was simplified and improved by H. COHEN and H.W. LENSTRA, Jr. [29]. The resulting test was implemented by A.K. LENSTRA and H. COHEN with the help of DIK WINTER [30], and made it possible to prove primality of numbers up to 300 decimal digits in a few minutes CPU-time. At present, one is able to prove primality of numbers with 1000 and more digits [4, 16]. For an excellent treatment of old and modern primality tests, see [31, pp. 416–418 and pp. 437–468].

The size of the numbers which could still be factored at a given time with the available algorithms and computer technology, was about 25 decimal digits in 1967 [25, p. 87], 40–50 in 1974 [39, Figure 1, p. 185], 70–80 in 1987 [127], and 120–130 in 1994 [89]. This illustrates the rapid developments, both in algorithms and in hardware, if we realize that for the best known methods the computational effort roughly *doubles* if the number to be factored grows with 2–3 decimal digits.

Two important algorithmic discoveries have effectuated a jump in the size of the numbers which can be factored within a reasonable time: the quadratic sieve method (QS) published in its modern form in 1985 [101] (but with main ideas going back to 1926 [63]), and the elliptic curve method (ECM) published in 1987 [71]. ECM is suitable to find factors up to 35–40 decimal digits of large numbers. Its complexity, as conjectured theoretically, and as observed in the experiments, depends primarily on the *size* of the smallest prime factor p of the number N which we wish to factor. Whether or not ECM finds a factor of N depends on the smoothness of the order of certain elliptic curve groups mod p which are known to lie in the interval $[p+1-2\sqrt{p},\ p+1+2\sqrt{p}]$. The complexity of the quadratic sieve method depends on the size of N, and not on its prime factors. It is still the method by which the largest numbers (not of a special form like $a^n \pm b$ where a and b are small compared to N) have been factored. ECM and QS are methods which complement each other nicely: one usually tries ECM first in order to find factors less than 25–30 decimal digits (or 30–35 if more computer power is available), and in the next step QS is tried, provided that the number to be factored is small enough: popularly spoken, ECM finds smaller factors of larger numbers, QS finds larger factors of smaller numbers.

A third method, called the Number Field Sieve (NFS) and published in 1993 [65, 67], is expected to be more efficient for general numbers than the quadratic sieve, and it is the subject of intensive current research to find out where the cross-over point between NFS and QS lies. For numbers of the special form $a^n \pm b$ (as above), NFS is known to be more efficient than QS.

At CWI much time and effort has been spent on the efficient implementation of QS on large vector mainframes like the CDC Cyber 205, the NEC SX-2, and the Cray Y-MP and Cray C90 vector computers [102, 72, 104, 105]. Two "factors" have favoured this approach: firstly, the bulk of the computational work in QS consists of adding fixed quantities to numbers in a large array at positions which lie in an arithmetic progression, so this work is suitable for vectorization; secondly, CWI has always had excellent facilities for access to large vector computers, including an abundance of low-priority CPU-time.

In the course of years, various new factorization records have been established by the CWI Computational Number Theory group. Almost all factored numbers were contributions to the so-called Cunningham Table [24] and to an extension of this table [23]. Several factorizations contributed to the proof of the non-existence of odd perfect numbers below 10^{160} [18], and below 10^{300} [21].

A survey of modern integer factorization algorithms is presented by Peter Montgomery in this CWI Quarterly Issue. In Section 4.1 we will sketch the principal steps of the quadratic sieve method (QS), and list the factorization records obtained with QS at CWI on vector computers in the past eight years. In Section 4.2 we explain the latest QS- and NFS-results obtained at CWI (partly in cooperation with Oregon State University).

4.1. The quadratic sieve method

Suppose that we wish to factor the large integer N, which by the little theorem of Fermat is known to be composite, and whose smallest prime divisor could not be found by trial division, Pollard Rho, Pollard $p-1$, Williams' $p+1$, or ECM [89]. The idea of the quadratic sieve is to find two different integers X and Y which satisfy the congruence $X^2 \equiv Y^2 \bmod N$, from congruences of the form $U_i^2 \equiv W_i \bmod N$, the latter congruences being generated by means of a quadratic polynomial, and where the numbers W_i are such that they only consist of prime factors below some bound B. A pair (U_i, W_i) is called a *relation*. As soon as more relations (U_i, W_i) have been found than the total number of different prime factors which occur in *all* of the W_i's, then indeed such an (X, Y)-congruence can be found (see Steps 6 and 7 of the QS algorithm below). Next we compute $d := \gcd(X-Y, N)$ by Euclid's algorithm and if $1 < d < N$, then d is a proper divisor of N. If insufficiently many (U_i, W_i)-pairs have been found with the help of one quadratic polynomial, then more polynomials are constructed following ideas of Peter Montgomery [100].

The one-polynomial version of the quadratic sieve method can be explained as follows. Let $U(x) := x + \lfloor N^{1/2} \rfloor$ (where $\lfloor y \rfloor$ is the greatest integer $\leq y$), and $W(x) := U^2(x) - N$, $x \in \mathbb{Z}$, and $x \ll N^{1/2}$. Then we have

$$U^2(x) \equiv W(x) \bmod N$$

and

$$W(x) \approx 2xN^{1/2} \ll N. \tag{18}$$

Hence, $W(x)$ can be expected to be easier to factor than N. Moreover, since $W(x)$ is a quadratic polynomial, it has the nice property that if $p|W(x_0)$ for some $x_0 \in \mathbb{Z}$, then also $p|W(x_0 + kp)$, for all $k \in \mathbb{Z}$. Such an x_0 can be found for given p as follows:

$$W(x) \equiv 0 \bmod p \;\text{ implies that }\; (x + \lfloor N^{1/2} \rfloor)^2 \equiv N \bmod p;$$

this equation generally has two solutions if N is a quadratic residue of p (shortly denoted by the Legendre symbol as: $\left(\frac{N}{p}\right) = 1$). These solutions can be computed easily [123, pp. 284–285]. Similar results apply for powers of the prime p. We now give the different steps of the **Quadratic Sieve factorization algorithm (QS)**:

1. Choose a factor base $FB := \{q = p^e \leq B \mid p \text{ prime and } \left(\frac{N}{p}\right) = 1\}$ for some suitable B (these are the prime powers which can occur in the $W(x)$-values, which we wish to factor completely).
2. $\forall q \in FB$ solve $W(x) \equiv 0 \bmod q$; this yields two solutions, denoted by r_{q1} and r_{q2}.
3. Initialize a *sieving* array $SI(j)$, $j = -M, \ldots, M-1$, to 0, where M is suitably chosen.
4. (Sieving) $\forall q \in FB$, $\forall j \in [-M, M-1]$ such that $j \equiv r_{q1} \bmod q$ or $j \equiv r_{q2} \bmod q$: $SI(j) := SI(j) + \log p$.
5. (Selection) Select those $x \in [-M, M-1]$ for which $|SI(x)| \approx \log(MN^{1/2})$ and store these numbers into x_1, $x_2, \ldots$. (Because of (18) and the fact that $\log|W(x)|$ is very slowly varying for $x \in [-M, M-1]$, we may expect the $W(x_i)$ to be composed only of primes which belong to the factor base FB.) Write $W(x_i)$ as

$$W(x_i) = (-1)^{\alpha_{i0}} \prod_{j=1}^{F} p_j^{\alpha_{ij}},$$

   where $p_1, p_2, \ldots, p_F$ are the primes in the factor base FB. Associate with x_i and $W(x_i)$ the vector of exponents $\underline{\alpha}_i^T = (\alpha_{i0}, \alpha_{i1}, \ldots, \alpha_{iF})$.
6. (Gaussian elimination) Collect at least $F+2$ completely factored $W(x_i)$-values (assuming this is possible for the current choice of B and M) and find linear combinations of vectors $\underline{\alpha}_i$ which, added (mod 2), yield $\underline{0}$. This can be carried out by means of Gaussian elimination (mod 2).
7. Multiply those $W(x)$-values whose linear combination of exponent vectors yield the $\underline{0}$-vector. This implies that we have found a congruence of the form $X^2 \equiv Y^2 \bmod N$; compute these X and Y, and $\gcd(X-Y, N)$ which should yield a factor of N with probability at least 0.5. If this gcd equals 1 or N, then try another linear combination of exponent vectors: in our experience, the Gaussian elimination always yields more than one linear relation, although theoretically it might yield precisely one.

The most time-consuming part of this algorithm is Step 4, because in order to factor a large number N, the parameters B and M have to be chosen very large (implying many primes in the sieving step and a long sieving array). Step 5 also consumes a non-trivial portion of the computing time: it has to select those values of x for which $SI(x)$ is large. The Gaussian elimination Step 6 deserves special attention, not because of the time, but because of the memory it requires.

We have vectorized our Fortran program on the following vector computers: Cyber 205, NEC SX-2 [72], Cray Y-MP [105], and Cray C90. For Step 4 we measured maximum speeds of 13, 90, 110, and 270 million floating point additions per second, respectively. These speeds were obtained with the *smallest* sieving primes: in that case the *number* of additions in the sieving array SI is large enough to reach vector performance. However, if we increase the sieving primes, the performance degrades, because the vector lengths decrease. For Step 5, in which *comparisons* rather than additions are done, we measured 25, 90, 150, and 370 million comparisons per second on the Cyber 205, NEC SX-2, the Cray Y-MP, and the Cray C90, respectively.

Several refinements were implemented in our program. Here, we mention them briefly; for details, see [100, 104].

1. *Use of a multiplier.* Sometimes, it is worthwile to premultiply the number N which we want to factor by a small integer, with the purpose to bias the factor base towards the smaller primes.
2. *Small prime variation.* When we sieve with a prime p, the number of sieving steps is $\lfloor 2M/p \rfloor$. This number is largest for small prime p, and in that case its corresponding $\log p$-value does not contribute too much to the total $\log |W(x)|$-value. Therefore much time is saved by *not* sieving with the smallest primes, and compensate for that by lowering the threshold-value in the selection step. The price to pay is the generation of some W-values which are not fully factorizable over the primes in the factor base (see also the next refinement).
3. *Large prime variations.* By lowering the report-threshold with a suitably chosen value, we accept $W(x)$-reports which are not completely factorizable with the primes from FB. Let the remaining part in such reports be denoted by R. In the *one-large-prime variation* of the quadratic sieve we accept those reports for which R is a prime; the corresponding reports are called *partial relations.* In the *two-large-primes variation* of QS we *also* accept those reports for which R is the product of *two* primes; the corresponding reports are called *partial–partial relations.* The partial and partial–partial relations which will come out have to be combined, if possible, to relations which factor completely over the factor base.
   In case of the one-large-prime variation, this amounts to sorting the partial relations according to their "big" primes, and finding relations with the same large prime. If we have $k \geq 2$ relations with the same large prime, we can deduce $k-1$ new *complete* relations from them by multiplying the second by the first, the third by the first, etc.

In the two-large-primes variation, the problem can be formulated in terms of finding all the basic cycles in a graph [68].

4. *Generation of polynomials.* We choose $U(x) = a^2x + b$ and $W(x) = a^4x^2 + 2a^2bx + a^2c$ with $b^2 - N = a^2c$, $a^2 \approx \sqrt{2N}/M$, and $|b| < \frac{1}{2}a^2$. Then we have $U^2(x) \equiv W(x) \bmod N$ and there are many possible choices for a and b (c follows from a and b), each choice yielding a new polynomial. For details about efficient polynomial generation in the quadratic sieve method, we refer to [100, 127, 104, 3].

In Table 6 we give some figures about record factorizations found at CWI on vector computers. All the results were obtained on *one* processor of the vector computer listed. On the Cray Y-MP we *could* have used four CPUs, thus reducing the sieving time by a factor of about four, since Steps 2–5 of the quadratic sieve algorithm are almost perfectly parallelizable (each CPU is given its own polynomial for sieving and selection).

year	machine	size of numbers (decimals)	sieving time (hours)	Gaussian elim. time (seconds)	approximate order of sparse system
1986	Cyber 205 [102, 72]	72	4.3	21	6,070
		75	12.2	37	7,400
1988	NEC SX-2 [72, 104]	87	30	200	18,800
		92	95	700	24,300
1991	Cray Y-MP [105]	101	475	1800	50,200

TABLE 6. Record factorizations with QS on vector (super)computers

4.2. Recent results

The latest records were obtained in the summer of 1994 with the help of the Cray C90 at SARA (The Academic Computing Centre Amsterdam), and many workstations at Oregon State University and CWI: a 162-digit Cunningham number was factored with the "Special Number Field Sieve" (SNFS, for which the number N to be factored has the form $N = a^n \pm b$, a and b being small compared to N), and a 105-digit number was factored with the "General Number Field Sieve" (GNFS, for which no special form of N is known). For details, see [89] and [58]. One month after the latter result was obtained, Arjen Lenstra, Bruce Dodson, and Peter Montgomery cracked a 116-digit partition number with GNFS. On November 26, 1994 Scott Contini, Bruce Dodson, Arjen Lenstra, and Peter Montgomery completed the factorization of a 119-digit cofactor of the 123-digit 13171th partition number $p(13171)$ into two primes of 52 and 67 digits using GNFS. From the time they used (about 250 mips years) they estimate that this is about 2.5 times less than what they would need to factor a number of comparable size with PPMPQS.

Peter Montgomery and Marije Huizing factored several other numbers with SNFS (of 98, 99, 106, 119, 123, 135, and 137 decimal digits) including some *more* and *most* wanted Cunningham numbers, using Montgomery's new algorithm for computing the square root of the product of many algebraic numbers, and his new iterative block Lanczos algorithm for finding dependencies in large sparse matrices over GF(2) [89]. Marije Huizing also factored an 87-digit number with GNFS. Certainly not a record, but worth mentioning here was the factorization, in June 1994, of a 99-digit cofactor of the more wanted number with code "2,914M C133" from the Cunningham table. This "C133" is the composite number of 133 decimal digits $(2^{457} + 2^{229} + 1)/(5 \times 71293)$; Montgomery had found a 34-digit prime factor of this number with ECM, and left a 99-digit composite cofactor. We decomposed it into the product of a 49- and a 50-digit prime by using the one-large-prime variation of the quadratic sieve, with the help of all processors of an eight processor IBM 9076 SP1, and 69 Silicon Graphics workstations. The total amount of time for the sieving was about 19,500 workstation CPU-hours. The calendar time for this factorization was about four weeks. The Gaussian elimination step was carried out on a Cray C90; it required about 0.5 Gbytes of central memory, and one hour CPU-time.

At various occasions, CWI has "donated" idle workstation cycles to joint Internet factorization projects [69, 67, 40, 5].

Currently, most factorization research at CWI aims at contributing to the Cunningham table [24] and to the extended Cunningham table [23]. In the first update to the table [23], all the composite numbers with less than 86 decimal digits were completed. This bound has been raised now (December 1994) to 89 decimal digits. Marije Huizing is experimenting with an implementation of GNFS on a CWI cluster of 70 workstations [58]. Henk Boender and the first named author are carrying out experiments on the Cray C90 with the two-large-primes variation of the quadratic sieve method, in order to collect experience with this method, and to find out where it beats the one-large-prime variation of the quadratic sieve [11]. Test numbers are the numbers of 89 and more decimal digits from [23] which are known to be composite, but whose factors are still unknown.

5. Aliquot sequences and generalizations

Many computational papers have been published on sequences which are obtained by repeated application of a given number-theoretic function $f(n)$. For a concise survey, see [112]. A notorious example is the "$3x+1$"-sequence (known in the literature under various different names) where $f(n) = n/2$ if n is even, and $f(n) = 3n + 1$ if n is odd. Starting, e.g., with $n_0 = 19$, and defining $n_{i+1} = f(n_i)$, $i = 0, 1, \ldots$, we find $n_1 = 58$, $n_2 = 29$, $n_3 = 88, \ldots, n_{18} = 4$, $n_{19} = 2$, $n_{20} = 1$, $n_{21} = 4$, so that the sequence becomes periodic. All instances of such f-sequences computed so far eventually run into this cycle, but no proof is known that this holds *for all* $n \in \mathbb{N}$. There is extensive literature concerning this problem [50, Problem E16]. In Section 5.1 we shall report on aliquot sequences and cycles, which have been the subject of much research at CWI. In Section 5.2 we shall discuss generalizations of aliquot sequences.

5.1. Aliquot sequences and cycles

Aliquot sequences arise when we repeatedly apply the function

$$s(n) = \sigma(n) - n$$

to a given starting value, where $\sigma(n)$ is the sum of all the divisors of n and $s(n)$ is known as the sum of the *aliquot* divisors of n. Since σ is a multiplicative function, we can compute it quickly if we know the factorization into primes of n, but this also means that computing aliquot sequences actually becomes difficult if the terms become large. There are five starting numbers < 1000, namely 276, 564, 660, 840, and 996, for which it is not known whether the corresponding aliquot sequence terminates at 1 (the previous term being a prime number), becomes periodic, or is unbounded. The terminating sequence with largest known maximum value is the one which starts with 840. GUY and GUY [49] and, independently, CREYAUFMÜLLER [34] found that $s^{746}(840) = 601$, and $s^{747}(840) = 1$, while the 840-sequence reaches its maximum at

$$s^{287}(840) = 3463982260143725017429794136098072146586526240388$$

$$= 2^2.64970467217.6237379309797547.2136965558478112990003.$$

The latest published status report on aliquot sequences is [49]. CREYAUFMÜLLER [34] reports to have computed the terms $s^{886}(276), s^{579}(552), s^{1104}(564)$, $s^{312}(660)$, and $s^{319}(966)$, having 88, 76, 73, 82, and 77 decimal digits, respectively. The first named author has constructed an aliquot sequence with more than 5092 monotonically increasing terms [107]. This result is based on the observation that if n is an even perfect number, i.e., $n = 2^{k-1}q$, $q = 2^k - 1$, q prime, and if m is an odd number such that $\gcd(q, m) = 1$, then the aliquot sequence starting with the number mn increases monotonically as long as $\gcd(q, t^i(m)) = 1$, $i = 1, 2, \ldots$, where $t(m) = 2\sigma(m) - m$. H.W. LENSTRA, JR. [70] proved that for every integer k there exists an aliquot sequence with k monotonically increasing terms.

When n is a perfect number, i.e., a number for which $\sigma(n) = 2n$, its aliquot sequence is n, n, ..., and this is a *periodic* sequence with period length 1. As is well-known, the *even* perfect numbers have the form $n = 2^{k-1}(2^k - 1)$, where k is an integer such that $2^k - 1$ is a (Mersenne-)prime. At present, we know 33 even perfect numbers, namely for $k = 2, 3, 5, \ldots, 216091, 756839, 859433$. The number $2^{859433} - 1$ is the largest known prime number, consisting of 258716 decimal digits. Concerning *odd* perfect numbers: it is known that if they exist, then they are larger than 10^{300} [21].

An aliquot sequence—period of length 2 is called an *amicable pair* and such a sequence has the pattern n, m, n, ..., where $m = \sigma(n) - n$ and $n = \sigma(m) - m$. So an amicable pair (n, m) may be defined as:

$$\sigma(n) = \sigma(m) = n + m, \quad n < m. \tag{19}$$

The smallest amicable pair is

$$n = 220 = 2^2 5.11, \quad m = 284 = 2^2 71.$$

This was known already in the ancient times of Pythagoras. The largest known amicable pair has 1041 decimal digits. It was found around 1988 by Holger Wiethaus, a student of E. Becker in Dortmund, Germany, and communicated by YAN and JACKSON in [138]. Many tens of thousands of amicable pairs are known [121, 7], but the question of the existence of infinitely many amicable numbers is still unanswered. Recently, COHEN ET AL. [27] have introduced a natural generalization of amicable numbers, called *multiamicable numbers*, defined as follows. Two numbers m and n are (α, β)-*amicable* if

$$\sigma(m) - m = \alpha n \quad \text{and} \quad \sigma(n) - n = \beta m$$

for positive integers α and β. If $\alpha = \beta = 1$ then m and n are amicable. Example: $m = 52920 = 2^3 3^3 5.7^2$ and $n = 152280 = 2^3 3^4 5.47$ form a $(1, 7)$-amicable pair.

Essentially four different methods are known to find amicable pairs:

1. The first is an exhaustive, numerical search method in which a number n is chosen, $m := \sigma(n) - n$ is computed, and, if $m > n$, $t := \sigma(m) - m$ is computed. If $t = n$, (n, m) is an amicable pair. By letting n run through a given interval, one finds *all* amicable pairs (n, m) with n in that interval. Exhaustive lists of amicable pairs were computed in this way by ROLF [125] (to 10^5), ALANEN ET AL. [2] (to 10^6), BRATLEY ET AL. [17] (to 10^7), COHEN [28] (to 10^8), TE RIELE [116] (to 10^{10}), and MOEWS ET AL. [86] (to 10^{11}). MOEWS ET AL. found 3340 amicable pairs below 10^{11}.
2. In the second method an assumption is made about the prime structure of n and m, for example $n = 2^k pq$, $m = 2^k r$, where $k \in \mathbb{N}$ and p, q and r are mutually different primes. Substitution in (19) leads to *Euler's rule* for amicable numbers: *$n = 2^k pq$ and $m = 2^k r$ are amicable numbers, if the three integers $p = 2^{k-j} f - 1$, $q = 2^k f - 1$ and $r = 2^{2k-j} f^2 - 1$ are primes, with $f = 2^j + 1$ and $k > j \geq 1$.* This rule yields amicable numbers for the five pairs $(k, j) = (2, 1)$, $(4, 1)$, $(7, 1)$, $(8, 7)$ and $(40, 11)$ [108]; the three amicable number pairs known for $j = 1$ are the only ones for $k \leq 20,000$ [14].
3. In the third method, amicable numbers are constructed from special numbers called *breeders* [15], which may be amicable numbers themselves [114]. To illustrate this, we give two rules for generating amicable numbers, from which many thousands of new amicable numbers have been generated.

   Rule 1 [113] *Let (au, ap) be a given amicable pair with* $\gcd(a, u) = \gcd(a, p) = 1$*, where p is a prime. If a pair of prime numbers (r, s)*

with $r < s$ *and* $\gcd(a, rs) = 1$ *exists, satisfying the bilinear Diophantine equation*

$$(r-p)(s-p) = \frac{\sigma(a)}{a}(\sigma(u))^2$$

and if a third prime q *exists, with* $\gcd(au, q) = 1$ *and* $q = r + s + u$*, then* $(auq,\ ars)$ *is also an amicable pair* (by using the definition of an amicable pair, it is easy to see that the right hand side above is an integer).
The next rule was suggested partly by the results of the systematic search for amicable pairs $< 10^{10}$ [116]. It is a generalization of a rule given in [15], and also **Rule 1** is a special case of it. One difference is that a and u need not be relatively prime.
Rule 2 [116] *Let* a*,* u *and* x *be such that* $au + ax = \sigma(au) = \sigma(a)(x+1)$*. Take any factorization of* $C = (x+1)(x+u)$ *into two different factors:* $C = D_1 D_2$*. Then, if the numbers* $s_i = x + D_i$ *for* $i = 1, 2$*, and also* $q = u + s_1 + s_2$ *are primes not dividing* a*, then* $(auq,\ as_1 s_2)$ *is an amicable pair.*
Other rules are given in [15] and [114].

4. The fourth method is based on the following observation of Erdős. Let $x_1, x_2, \ldots$ be solutions of the equation $\sigma(x) = s$; then any pair (x_i, x_j) for which $x_i + x_j = s$ is an amicable pair. If we have about $\sqrt{s}$ solutions of the equation $\sigma(x) = s$, and if these solutions are "randomly" distributed in the interval $[1, s]$, then we have a reasonable chance to find a pair of solutions which has sum s. Inspection of lists of known amicable pairs shows that in most cases s consists only of small prime divisors. In [120] an algorithm is presented for finding as many solutions of $\sigma(x) = s$ as possible, by the use of a table of precomputed values of $\sigma(p^a)$ for all primes p and exponents a such that $\sigma(p^a) < B$, where B is suitably chosen. Running this algorithm for many "smooth" values of s (i.e., values which only consist of small prime factors), we obtained more than 100 new amicable pairs. To give an example, $s = 3 \times 14!$ yielded the two amicable pairs [120]

$$(2^3 29.53.83.103.1231, 2^3 23.167.179.24023)$$

and

$$(2.5.11.41.1091.26399, 2.5.11.103.503.23099).$$

In 1913, L.E. DICKSON [41] defined an *amicable* k*-tuple* as k positive integers $(n_1, n_2, \ldots, n_k)$ for which

$$\sigma(n_1) = \sigma(n_2) = \ldots = \sigma(n_k) = n_1 + n_2 + \ldots n_k.$$

For $k = 2$ this reduces to (19). Our method for finding amicable pairs also applies to finding such k-tuples for $k > 2$: among the solutions of $\sigma(x) = s$ just try to find the k-tuples which sum up to s. In fact, as k increases, the chances to find k-tuples grow. For example, if we have

N solutions of $\sigma(x) = s$, then there are $N(N-1)(N-2)/6$ possible triples to check for $k = 3$, against $N(N-1)/2$ pairs for $k = 2$. With this method, we have found 277 amicable triples below 10^6 [106], whereas the total number of amicable *pairs* below 10^6 is 42.

As contrasted with the abundance of known aliquot cycles of length 2, not many cycles of length ≥ 3 are known. There are 37, 1, 1, 2, 1, and 1 known cycles of length 4, 5, 6, 8, 9, and 28, respectively [44, 85, 86, 84]. As far as we know, BORHO [13] is the only one who has given *rules* for constructing aliquot cycles of length > 2, and 8 of the 37 known 4-cycles were constructed by means of one of his rules. The starting values of the smallest cycles of length 4, 5, 6, 8, 9 and 28 are 1264460, 12496, 21548919483, 1095447416, 805984760 and 14316, respectively. It is not known whether or not there exist aliquot 3-cycles.

5.2. Generalizations of aliquot sequences

If, instead of summing *all* the divisors of n, one would sum the *unitary* divisors of n (i.e., the divisors d of n for which $\gcd(d, n/d) = 1$), we can adapt the ideas of aliquot sequence to obtain *unitary* aliquot sequences [50, Problems B3 and B8]. This has been generalized [109] to *aliquot f-sequences* where f is an arithmetic function which determines *which* divisors are to be summed when we go from n_i to n_{i+1} in an aliquot f-sequence. Various theoretical and computational results have been derived in [109], like proofs of the existence of aliquot f-sequences with arbitrarily many monotonically increasing terms, and of the existence of unbounded sequences for certain choices of f. For example, if f is the multiplicative function defined by $f(p^e) = p^e + p^{e-1}$, p prime, $e \in \mathbb{N}$, and if we start with $n_0 = 9870 = 2.3.5.7.47$, we find $n_1 = f(n_0) - n_0 = 17778 = 2.3.2963, \ldots, n_{19} = 266490 = 2.3^4 5.7.47$, $n_{20} = 480006 = 2.3^4 2963, \ldots,$ where the omitted terms are monotonically increasing. It is not difficult to prove that the terms $n_0, \ldots, n_{18}$ are repeated as the next 19 terms after multiplication by the factor 3^3, and so on, so that this is an unbounded aliquot f-sequence.

6. FOUR SMALLER PROJECTS

6.1. The Goldbach conjecture(s)

The Goldbach conjecture, expressed by Goldbach in a letter to Euler in 1742, says that every even number can be expressed as the sum of two primes (if we consider 1 a prime, as Goldbach did). In fact, this conjecture is a big "understatement": experiments show that the *number of representations* of an even number n as the sum of two primes grows quickly with n (albeit not monotonically), so a proof of the Goldbach conjecture would only provide a very poor lower bound, namely 1, for the number of representations. In 1988–1989 we have verified the Goldbach conjecture on a Cyber 205 vector computer up to 2×10^{10} [48]. This extended Stein and Stein's previous bound 10^8 [130]. Recently, SINISALDO [128] has extended our bound to 4×10^{11}.

The principle of how we verified the Goldbach conjecture on the Cyber 205 vector computer is as follows. In order to verify the Goldbach conjecture for the even numbers in a given interval $[N_1, N_2]$ (assume N_1 and N_2 to be even), a straightforward approach is to start with $n = N_1$ and find the smallest prime p such that $n - p$ is also a prime. Next, do the same for $n+2$, $n+4, \ldots$, until N_2 is reached. A disadvantage of this approach is that *repeatedly* primality has to be checked of the same number. Moreover, vectorization is not possible. To overcome this, one prepares a table of the primes between $N_1 - p$ and $N_2 - 3$, inclusive, where p is a suitably chosen prime. This can be done quickly, with the help of the Sieve of Eratosthenes. One then starts to check primality (by table look-up) of the odd numbers $N_1 + 2i - 3$ for $i = 0, 1, \ldots, (N_2 - N_1)/2$. This finds *all* even numbers in the interval $[N_1, N_2]$ which can be written as the sum of 3 and some other prime. This step can easily be vectorized on a vector computer. In the next step, primality is checked of the numbers $N_1 + 2i - 5$ for $i = 0, 1, \ldots, (N_2 - N_1)/2$ (except for those values of i for which $N_1 + 2i - 3$ was recognized to be prime in the previous step). This step is repeated with the primes $7, 11, \ldots, p$. The possibility to vectorize these steps gradually decreases, because the number of even numbers in $[N_1, N_2]$ for which no representation as a sum of two primes has been found, also decreases as the number of steps increases. Therefore, at a certain point the remaining even numbers are treated with the straightforward approach described above. Walter Lioen assisted us with the optimization of our program, by the inclusion of several machine-dependent technical refinements, for which we refer to [48]. Let $p = p(n)$ be the smallest prime such that $n - p$ is prime. We have verified the Goldbach conjecture for the even numbers up to 2×10^{10} at the expense of about 20 CPU-hours on the Cyber 205. The largest $p(n)$-value we found is $p(12{,}703{,}943{,}222) = 2029$. We also included some statistics and results based on the Prime k-tuplets Conjecture of Hardy and Littlewood, supporting these statistics. The largest $p(n)$-value known at present is $p(244{,}885{,}595{,}672) = 3163$ [128].

The correspondence between Goldbach and Euler contains a few other "Goldbach conjectures". One of them, dating back to 1752, reads

$$2n + 1 = p + 2k^2, \quad p \text{ prime}, \quad k \geq 0.$$

However, in 1856 Stern found that $2n+1 = 5777$ and $2n+1 = 5993$ are exceptions, and thereafter this conjecture (or, rather, its remains) has not received any noteworthy attention. Since no other exceptions have ever been found, it seems reasonable to save the plausibility of the conjecture by adding the clause "with at most finitely many exceptions" (FE, for short). With this in mind, the second author and Walter Lioen have tried to generalize this as follows: for any fixed *odd* $m \geq 1$ one has

$$2n + 1 = p + 2^m k^2, \quad p \text{ prime}, \quad k \geq 0 \quad \text{(FE)}. \tag{20}$$

A numerical check for $2n + 1 < 10^9$ resulted in Table 7. Similarly, for fixed $m \geq 1$, $3 \nmid m$, they conjecture that

$$2n + 1 = p + 2^m k^3, \quad p \text{ prime}, \quad k \geq 0 \quad \text{(FE)}. \tag{21}$$

The corresponding observations are given in Table 8. Further generalizations

m	number	largest found
1	2	5993
3	38	39167
5	530	1224647
7	3762	9020117
9	23121	54183467
11	132904	483642707

TABLE 7. Exceptions to (20)

m	number	largest found
1	317	9843745
2	969	17691293
4	8071	367803655

TABLE 8. Exceptions to (21)

along these lines do not seem plausible.

In 1775 Lagrange conjectured that

$$2n+1 = p + 2q, \quad p \text{ and } q \text{ odd primes,}$$

the only exceptions being $2n+1 = 3$, 5, and 7. Some experiments were carried out by the second author and Walter Lioen in order to check the plausibility of the following more general conjecture: for any fixed integer $m \geq 1$ one has

$$2n+1 = p + 2^m q, \quad p \text{ and } q \text{ odd primes (FE).} \tag{22}$$

The corresponding observations are given in Table 9. We conclude this section with a problem. Let θ be the supremum of all real α's for which

$$2n+1 = p + 2[k^\alpha], \quad p \text{ prime}, \quad k \geq 0 \text{ (FE).}$$

Is it true that $3 < \theta < 4$?

6.2. The constant of De Bruijn-Newman

Recently, CSORDAS ET. AL. [35] have introduced the so-called *De Bruijn-Newman constant* Λ as follows. Let the function $H_\lambda(x), \lambda \in \mathbb{R}$, be defined by

$$H_\lambda(x) := \int_0^\infty e^{\lambda t^2} \Phi(t) \cos(xt) dt, \tag{23}$$

where

m	number	largest found	m	number	largest found
1	3	7	9	2749	101581
2	8	77	10	6337	327857
3	16	89	11	14193	699373
4	37	473	12	31789	1847093
5	89	1951	13	70117	4030051
6	222	7571	14	153769	10726943
7	520	10793	15	334804	20368637
8	1226	37393	16	724769	63367757

TABLE 9. Exceptions to (22)

$$\Phi(t) = \sum_{n=1}^{\infty} (2\pi^2 n^4 e^{9t} - 3\pi n^2 e^{5t}) \exp(-n^2 \pi e^{4t}). \tag{24}$$

We mention the following properties of the function Φ:
i) $\Phi(z)$ is analytic in the strip $-\pi/8 < \Im z < \pi/8$;
ii) $\Phi(t) = \Phi(-t)$, and $\Phi(t) > 0 \quad (t \in \mathbb{R})$;
iii) for any $\epsilon > 0, \lim_{t\to\infty} \Phi^{(n)}(t) \exp[(\pi - \epsilon)e^{4t}] = 0$, for each $n = 0, 1, \ldots$.
The function H_λ is an entire function of order one, and $H_\lambda(x)$ is real for real x. From results of DE BRUIJN [26] it follows that if the Riemann hypothesis is true, then $H_\lambda(x)$ must possess only real zeros for any $\lambda \geq 0$. C.M. Newman has shown [92] that there exists a real number Λ, $-\infty < \Lambda \leq \frac{1}{2}$, such that $H_\lambda(x)$ has only real zeros when $\lambda \geq \Lambda$, and $H_\lambda(x)$ has some non-real zeros when $\lambda < \Lambda$. This number Λ was baptized the *De Bruijn-Newman constant* in [35]. The truth of the Riemann hypothesis would imply that $\Lambda \leq 0$, whereas NEWMAN [92] conjectures that $\Lambda \geq 0$. In [35] it was proved that $\Lambda > -50$ and in [118] the first named author gave strong numerical evidence that $\Lambda > -5$. For this result, high-precision floating-point computations with an accuracy of 250 decimal digits were required. A rough estimate showed that a formal *proof* of the bound $\Lambda > -5$ would require an extension of that precision to 2600 decimal digits. The lower bound -5 has been improved further to -0.385 in [93], -0.0991 in [37], -4.379×10^{-6} in [38] and to -5.895×10^{-9} in [36]. Here, we shall describe how the result of [118] was obtained, and how the result of [36] depends on the computations carried out in [78].

If we expand the cosine in (23) in its Taylor series, we obtain

$$H_\lambda(x) = \sum_{m=0}^{\infty} \frac{(-1)^m b_m(\lambda) x^{2m}}{(2m)!}, \tag{25}$$

where

$$b_m(\lambda) = \int_0^\infty t^{2m} e^{\lambda t^2} \Phi(t) dt,$$

$m = 0, 1, \ldots$; $\lambda \in \mathbb{R}$. The n-th degree Jensen polynomial $G_n(t; \lambda)$ associated with H_λ is defined by

$$G_n(t; \lambda) := \sum_{k=0}^{n} \binom{n}{k} \frac{k! b_k(\lambda)}{(2k)!} t^k, \tag{26}$$

and it was shown in [35] that if there exists a positive integer m and a real number $\hat{\lambda}$ such that $G_m(t; \hat{\lambda})$ possesses a complex zero, then $\hat{\lambda} < \Lambda$. The problem is to find m, given $\hat{\lambda}$. In [35] the bound $\Lambda > -50$ was derived from the computation of very accurate approximations of *all* the zeros of $G_{16}(t, -50)$, of which two zeros were found to be complex. The sensitivity of the zeros of polynomials to errors in their coefficients required that the computations were performed with an accuracy of 110 decimal digits. As a partial check, the first named author repeated the computations of CSORDAS et al. [35] with an accuracy of only 20 decimal digits, and the complex zero of $G_{16}(t, -50)$ was reproduced with about the same accuracy. This illustrates the large amount of extra work needed to provide a formal *proof* of the existence of complex zeros of the Jensen polynomial $G_n(t; \lambda)$.

In order to improve $\Lambda > -50$, we noticed that the degree of the Jensen polynomial $G_n(t; \lambda)$ which possesses complex zeros, grows quickly with λ. Consequently, finding *all* the zeros of G_n, $n = 1, 2, \ldots$ (in order to prove the existence of complex ones) becomes very expensive. Instead, we used *Sturm sequences* [57], [118, p. 663] by which it is possible to find the *numbers* of real and complex zeros of a given polynomial. The principle of the method we used in [118] is as follows. Suppose we know λ_0 and the smallest value $n(\lambda_0)$ of n for which $G_n(t; \lambda_0)$ has complex zeros (to start with, we took $\lambda_0 = -50$ and $n = 16$ from [35]). Then for a new value of λ which is somewhat larger than λ_0 we compute $b_i(\lambda)$, $i = 0, 1, \ldots$, and for each new b_i we compute the coefficients of the associated Jensen polynomial $G_i(t; \lambda)$. By means of the associated Sturm sequence, we check whether this polynomial has complex zeros with negative real part. If not, the next $b_i(\lambda)$ is computed, together with the associated Jensen polynomial and Sturm sequence, until we have found an i for which $G_i(t; \lambda)$ indeed has complex zeros (as said above, if $\lambda_0 < \lambda$ then $n(\lambda_0) \leq n(\lambda)$). Then we actually compute a complex zero of this polynomial by means of the Newton process; the starting value is chosen in the neighborhood of the complex zero of the *previous* Jensen polynomial $G_{n(\lambda_0)}(t; \lambda_0)$ [118, pp. 663–664]. In this way we found (accurate approximations of) complex zeros of $G_{n(\lambda)}(t; \lambda)$ for $\lambda = -50(1) - 40$, -30, -20, -10, and -5. We found that $G_{406}(t; -5) = 0$ for $t \approx -24.34071458 + 0.031926616\, i$. Our computations did not provide a formal proof of the existence of this complex zero, because we worked with (250D) *approximations* of the coefficients of the Jensen polynomials. However, a first order error analysis showed that the distance of this complex number to the exact zero is less than 10^{-221}.

The currently best known lower bound for Λ was derived in [36] by means of an ingenious other method, which uses extremely close (with respect to the length of the corresponding Gram interval) *pairs* of complex zeros of the Riemann zeta function. The closest known pair, found in [78], has normalized difference 0.00031, and gives rise to the lower bound -5.895×10^{-9}. The one but closest pair, found during the computations reported in [78] but not published there, has normalized difference 0.00055, and induces the lower bound -1.8×10^{-8} [94].

6.3. The Erdős-Moser equation

The Erdős-Moser Diophantine equation [91]

$$1^k + 2^k + \ldots + (x-1)^k = x^k \tag{27}$$

has one solution $(x,k) = (3,1)$ for $k = 1$, but for $k \geq 2$ no solution is known, and Erdős and Moser conjectured that indeed there are no solutions for $k \geq 2$. From now on we assume that $k \geq 2$. Moser [91] proved that $x > 10^{1000000}$ if a solution exists. The relation between x and k for solutions of (27) has been studied extensively in [74, 79, 10]. One consequence is that for every k there is at most one x satisfying (27).

Let B_r be the r-th Bernoulli number ($B_0 = 1$, $B_1 = -1/2$, $B_2 = 1/6$, $B_n = 0$ if $n \geq 3$ and odd). An odd prime p is said to be *regular* if p is not a divisor of B_r for all even integers r in the interval $[0, p-3]$. Otherwise, p is called *irregular*. Moser proved that k is even and that x should be odd. In [90] further divisibility properties of (27) have been established. Based on these properties and on numerical searches with the help of an SGI workstation, it was proved that if (x,k) is a solution of (27) then

1. k must be divisible by the number $M = 2^8 3^5 5^4 7^3 11^2 13^2 17^2 19^2 23 \cdots 199$ with $\log_{10} M = 94.359\ldots$, and
2. if p is a prime divisor of x, then p must be an irregular prime > 10000.

This provides strong support for the Erdős-Moser conjecture, particularly because these divisibility results can easily be extended if more computer time would be invested. Here, we shall illustrate the principle of the proof of 1. by showing that k must be divisible by $2^3 5.7$. For details of the proof of 1. and for the proof of 2., see [90].

In [90] a method is given to find pairs (r,q), with r even, q prime, and $r \in [2, q-3]$, such that the equation (27) has no solution (x,k) with $k \equiv r \bmod (q-1)$. We shall not describe how these pairs can be found, but Table 10 lists a number of such pairs which we need here.

$r=$	2	2, 4	2, 6	4, 12	16	18, 24	18, 24	180	120	300
$q=$	5	7	11	17	29	31	43	211	281	421

TABLE 10. Pairs (r,q) for which (27) has no solution with $k \equiv r \bmod (q-1)$

We start with Moser's result that k is even. The pair $(2,5)$ from Table 10 says that $k \not\equiv 2 \bmod 4$, so that $k \equiv 0 \bmod 4$. Together with $(4,17)$ and $(12,17)$ this implies that $k \equiv 0 \bmod 8$. From $(2,7)$ and $(4,7)$ it follows that $k \equiv 0 \bmod 6$. Combining the last two results gives $k \equiv 0 \bmod 24$.

Now we prove that $k \equiv 0 \bmod 120$ by eliminating the residues 24, 48, 72, and 96 mod 120 using the pairs $(2,11)$, $(6,11)$, $(18,31)$, and $(24,31)$ from Table 10. The pair $(2,11)$ implies that $k \not\equiv 2 \bmod 10$, which eliminates the residue 72, and the pair $(6,11)$ implies that $k \not\equiv 6 \bmod 10$, which eliminates the residue 96. The pair $(18,31)$ implies that $k \not\equiv 18 \bmod 30$, which eliminates the residue 48, and the pair $(24,31)$ implies that $k \not\equiv 24 \bmod 30$, which eliminates the residue 24. This proves that if (x,k) is a solution of (27), then $k \equiv 0 \bmod 120$.

To derive from this result that $k \equiv 0 \bmod (7 \times 120)$, we have to eliminate the residues 120, 240, 360, 480, 600, and 720 mod 840. This follows if we realize that $120 \equiv 120 \bmod 280$, $240 \equiv 16 \bmod 28$, $360 \equiv 24 \bmod 42$, $480 \equiv 18 \bmod 42$, $600 \equiv 180 \bmod 210$, and $720 \equiv 300 \bmod 420$, and use the pairs $(120,281)$, $(16,29)$, $(24,43)$, $(18,43)$, $(180,211)$, and $(300,421)$ from Table 10.

In a similar way, we proved that the primes $11, 13, \ldots, 199$ must be divisors of k if (x,k) is a solution of equation (27).

6.4. The equation $x^3 + y^3 + z^3 = k$

Consider the Diophantine equation

$$x^3 + y^3 + z^3 = k, \tag{28}$$

where k is a fixed positive integer, and x, y, and z can be any integers. It is easily seen that equation (28) has no solution at all if $k \equiv \pm 4 \bmod 9$. There is no known reason for excluding any other values of k although there are still many values of k for which no solution has been found so far. Those below 100 (and $\not\equiv \pm 4 \bmod 9$) are [46, 56, 32, 62]:

$$k = 30, 33, 42, 52, 74, \quad \text{and} \quad 75.$$

For some values of k infinitely many solutions are known. For example, we have

$$(9t^4)^3 + (-9t^4 + 3t)^3 + (-9t^3 + 1)^3 = 1,$$

and

$$(6t^3 + 1)^3 + (-6t^3 + 1)^3 + (-6t^2)^3 = 2.$$

These relations give a solution of (28) for each $t \in \mathbb{Z}$. For $k = 1$ many other solutions are known which do *not* satisfy the above parametric form (e.g., $(64, 94, -103)$).

In [83] and [46] solutions of (28) were computed by means of a straightforward algorithm which for given z and k checks whether any of the possible combinations of values of x and y in a chosen range satisfies (28). The range chosen in [46] (which includes the one chosen in [83]) was:

$$0 \le x \le y \le 2^{16},$$

$$0 < N \leq 2^{16}, N = z - x,$$
$$0 < |k| \leq 999.$$

This algorithm requires $\mathcal{O}(N^2)$ steps, but it finds solutions of (28) for a *range* of values of k. The implied $\mathcal{O}$-constant depends on that range.

Recently, Heath-Brown presented a new algorithm which takes $\mathcal{O}_k(N \log N)$ steps, where the implied $\mathcal{O}$-constant depends on k [54]. This algorithm is given explicitly for the case $k = 3$, but significant changes have to be made for other values of k, depending mainly on the class number of $\mathbb{Q}(\sqrt[3]{k})$.

For $k = 3$, Heath-Brown's algorithm can be described as follows. If $k \equiv 3 \bmod 9$ then $x \equiv y \equiv z \equiv 1 \bmod 3$. If x, y and z all have the same sign, then $x = y = z = 1$. Otherwise, let x and y have the same sign, and z the other, then we have $|x + y| \geq |z| \geq 1$. Now let $n := x + y$ and solve the equation $z^3 \equiv 3 \bmod n$ with z and n having different sign and $1 \leq |z| \leq |n|$. In [54] it is derived by factoring in $\mathbb{Q}(\sqrt[3]{3})$ (which has class number equal to 1) that $\gcd(n, 3) = 1$ and that

$$n = a^3 + 3b^3 + 9c^3 - 9abc$$

for some integers a, b, c such that

$$z \equiv (3c^2 - ab)(b^2 - ac)^{-1} \bmod n \tag{29}$$

(with z and n having different sign and $\gcd(b^2 - ac, n) = 1$). This gives a unique value of z. We can then solve the equations $x^3 + y^3 + z^3 = 3$ and $x + y = n$ to find x and y. This yields

$$x = \frac{n+d}{2}, \quad y = \frac{n-d}{2}$$

$$\text{with } \ d = \sqrt{D} \ \text{ and } \ D = \frac{1}{3}\left[4\left(\frac{3 - z^3}{n}\right) - n^2\right].$$

Here, D should be the square of an integer to yield integral x and y. If we choose $a = -1$, $b = 0$ and $c = 1$, we get $n = 8$, $z = -5$, $D = 0$ and $x = y = 4$ ($(1, 1, 1)$ and $(4, 4, -5)$ are the only known solutions for $k = 3$).

Walter Lioen and the first author have implemented Heath-Brown's algorithm on a Cyber 205 vector computer [56] for $k = 2, 3, 20, 30, 39$ and 42. In particular, Lioen was able to vectorize the Euclidean algorithm for the computation of $(b^2 - ac)^{-1} \bmod n$ in (29) using standard Fortran. Vectorized routines were written for double precision vector addition, subtraction, multiplication, division, and modular multiplication. The cases $k = 3$ and $k = 30$ probably are the most intensively studied ones. For $k = 2$ the parametric solution given above was known, but we wanted to check whether other solutions exist. For $k = 20$ the density of adèlic points is rather high, and relatively many integer points are known. This case was used as a (partial) check of the correctness of our program. The smallest value of $k > 30$ for which no solution was known is $k = 33$. However, the fundamental unit of $\mathbb{Q}(\sqrt[3]{33})$ is enormous, and in this case the algorithm becomes very inefficient. Therefore, we selected the next two cases $k = 39$ and $k = 42$. In [56] precise descriptions are given of the algorithms for the various chosen values of k. No (new) solutions were found for $k = 3, 30$, and 42. The upperbound on the checked values of $|x|$, $|y|$, and $|z|$ was 1.35×10^8 for $k = 3$, and 1.64×10^6 for $k = 30$. For $k = 2$ the first solution was found which is *not* of the parametric form given above, namely $(1214928, 3480205, -3528875)$. For $k = 20$ eight new solutions were found (the largest being $(-89598233, -374850480, 376549093)$) and, finally, for $k = 39$ we found the first solution $(134476, 117367, -159380)$, so this case could be removed from the list of values of k for which no solution was known. We remark that this solution was also found, independently, by CONN and VASERSTEIN [32], and by K. KOYAMA [62].

$k = 3$	denominator D	xD	yD	zD
	3	191554	198873	−246040
	6	10510	155511	−155527
	14	−224067217	−510955663	524932898
	21	−9526505	−15665580	16761452
$k = 30$	denominator D	xD	yD	zD
	2	362264	−113380	1121345
	2	−601438	−11299015	11299583
	3	2215240	5369951	−5492781
	6	−35146503	−40659593	48006104

TABLE 11. Some rational solutions of (28) for $k = 3$ and $k = 30$

Recently, the first named author has implemented Heath-Brown's algorithm for $k = 3$ and $k = 30$ on a Cray C90 vector computer. This, and also the work in [56] was stimulated by Heath-Brown's conjecture [53, p. 623] that there are *infinitely many solutions* of (28) for each value of $k \not\equiv \pm 4 \bmod 9$. Lioen again vectorized the Euclidean algorithm and Dik Winter wrote a vectorized double precision multiplication routine. Peter Montgomery speeded up the search algorithm by showing that $x^3 + y^3 + z^3 = 3$ (or 30) implies that $x + y + z \equiv 3 \bmod 9$. This is seen as follows. If $k = 3$ or $k = 30$ in (28) then $x \equiv y \equiv z \equiv 1 \bmod 3$. Let $x = 3a + 1$, $y = 3b + 1$, and $z = 3c + 1$; then

$$0 = x^3 + y^3 + z^3 - k \equiv 27(a^3 + b^3 + c^3 + a^2 + b^2 + c^2) + 9(a + b + c) \bmod 27.$$

It follows that $a+b+c \equiv 0 \bmod 3$ so that $x+y+z = 3(a+b+c)+3 \equiv 3 \bmod 9$. We have combined this with the necessary condition $x+y+z \equiv k \bmod 6$, which follows from $t^3 \equiv t \bmod 6$ and (28). With our Cray C90-implementation, the upper bound on the checked values of $|x|$, $|y|$, $|z|$ mentioned above was extended for $k = 3$ to 5.0×10^9 and for $k = 30$ to 4.4×10^7. Unfortunately, no new solutions were found.

Peter Montgomery, while visiting CWI in 1994, looked for *rational* solutions of (28) for $k = 3$ and $k = 30$ with the help of the Cray C90 vector computer. He found many such solutions, a small selection of which is given in Table 11. Notice that any rational solution x, y, z of (28) with common denominator D gives an integer solution xD, yD, zD of (28) with k replaced by kD^3.

7. Acknowledgements

Dik Winter and Walter Lioen have given programming and vectorization support to virtually all the projects described in this paper. Their expert knowledge of the hardware and software of the various computers used, and their extensive experience, were indispensable for the success of these projects. We thank Peter Montgomery for reviewing an early draft of the manuscript. We are grateful to the 70 CWI workstation "owners" for making available the idle time of their machines for our projects.

The work on the Cyber 205, NEC SX-2, Cray Y-MP and Cray C90 vector computers was supported by the Stichting Nationale Computerfaciliteiten (National Computing Facilities, NCF), with financial support from the Nederlandse Organisatie voor Wetenschappelijk Onderzoek (Netherlands Organization for Scientific Research, NWO). IBM Nederland provided generous access to the IBM SP1. We acknowledge the operational and technical support of the staff of SARA (Academic Computing Centre Amsterdam).

References

1. L. Adleman, C. Pomerance, and R. Rumely. On distinguishing prime numbers from composite numbers. *Ann. of Math.*, 117:173–206, 1983.
2. J. Alanen, O. Ore, and J. Stemple. Systematic computations on amicable numbers. *Mathematics of Computation*, 21:242–245, 1967.
3. W.R. Alford and Carl Pomerance. Implementing the self initializing quadratic sieve on a distributed network. Manuscript, received Nov. 11, 1993.
4. A.O.L. Atkin and F. Morain. Elliptic curves and primality proving. *Mathematics of Computation*, 61:29–68, 1993.
5. Derek Atkins, Michael Graff, Arjen K. Lenstra, and Paul C. Leyland. THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE. In *Proceedings of Asiacrypt '94*, Lecture Notes in Computer Science, Berlin. Springer–Verlag. To appear.
6. D.H. Bailey. Multiprecision translation and execution of Fortran programs. *ACM Transactions on Mathematical Software*, 19:288–319, 1993.
7. S. Battiato. Über die Produktion von 37803 neuen befreundeten Zahlenpaaren mit der Brütermethode. Master's thesis, Bergische Universität Gesamthochschule Wuppertal, June 1988.

8. C. Batut, D. Bernardi, H. Cohen, and M. Olivier. *User's Guide to PARI-GP*. This Guide and the package can be obtained by anonymous ftp from the sites `ftp.inria.fr` and `math.ucla.edu`.
9. L. Bernstein. *The modified algorithm of Jacobi–Perron*. Memoirs of the Amer. Math. Soc., vol. 67, 1966.
10. M.R. Best and H.J.J. te Riele. On a conjecture of Erdős concerning sums of powers of integers. Technical Report NW 23/76, Mathematisch Centrum, Amsterdam, May 1976.
11. Henk Boender and Herman te Riele. Factoring integers with large prime variants of the quadratic sieve. In preparation.
12. H. Bohr. *Almost periodic functions*. Chelsea, New York, 1947.
13. W. Borho. Über die Fixpunkte der k-fach iterierten Teilersummenfunktion. *Mitt. Math. Gesells. Hamburg*, 9:34–48, 1969.
14. W. Borho. Some large primes and amicable numbers. *Mathematics of Computation*, 36:303–304, 1981.
15. W. Borho and H. Hoffmann. Breeding amicable numbers in abundance. *Mathematics of Computation*, 46:281–293, 1986.
16. Wieb Bosma and Marc-Paul van der Hulst. *Primality proving with cyclotomy*. PhD thesis, University of Amsterdam, December 1990.
17. P. Bratley and J. McKay. More amicable numbers. *Mathematics of Computation*, 22:677–678, 1968.
18. Richard P. Brent and Graeme L. Cohen. A new lower bound for odd perfect numbers. *Mathematics of Computation*, 53:431–437, 1989.
19. R.P. Brent. A Fortran multiple precision arithmetic package. *ACM Transactions on Mathematical Software*, 4:57–70, 1978.
20. R.P. Brent. On the zeros of the Riemann zeta function in the critical strip. *Mathematics of Computation*, 33:1361–1372, 1979.
21. R.P. Brent, G.L. Cohen, and H.J.J. te Riele. Improved techniques for lower bounds for odd perfect numbers. *Mathematics of Computation*, 57:857–868, 1991.
22. R.P. Brent, J. van de Lune, H.J.J. te Riele, and D.T. Winter. On the zeros of the Riemann zeta function in the critical strip. II. *Mathematics of Computation*, 39:681–688, 1982.
23. R.P. Brent and H.J.J. te Riele. Factorizations of $a^n \pm 1$, $13 \leq a < 100$. Technical Report NM-R9212, Centrum voor Wiskunde en Informatica, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands, June 1992.
Available by anonymous ftp from:
`nimbus.anu.edu.au: pub/Brent/rpb134t.txt.Z`, `rpb134.dvi.Z`.
Update 1 to this report has appeared as CWI Report NM–R9419, September 1994, with P.L. Montgomery as additional author.
24. J. Brillhart, D.H. Lehmer, J.L. Selfridge, B. Tuckerman, and S.S. Wagstaff, Jr. *Factorizations of* $b^n \pm 1, b = 2,3,5,6,7,10,11,12$ *up to high powers*, volume 22 of *Contemporary Mathematics*. American Mathematical Society, second edition, 1988.
Updates to this second edition, with new lists of most and more wanted

numbers, are distributed regularly by the fifth author.

25. John Brillhart and J.L. Selfridge. Some factorizations of $2^n \pm 1$ and related results. *Mathematics of Computation*, 21(97):87–96, January 1967. Corrigendum, *ibid.*, p. 751.
26. N.G. de Bruijn. The roots of trigonometric integrals. *Duke Math. J.*, 17:197–226, 1950.
27. Graeme L. Cohen, Stephen F. Gretton, and Peter Hagis, Jr. Multiamicable numbers. Manuscript, received Febr. 15, 1994.
28. H. Cohen. On amicable and sociable numbers. *Mathematics of Computation*, 24:423–429, 1970.
29. H. Cohen and H.W. Lenstra, Jr. Primality testing and Jacobi sums. *Mathematics of Computation*, 42:297–330, 1984.
30. H. Cohen and A.K. Lenstra. Implementation of a new primality test. *Mathematics of Computation*, 48:103–121, 1987.
31. Henri Cohen. *A Course in Computational Algebraic Number Theory*, volume 138 of *Graduate Texts in Mathematics*. Springer–Verlag, Berlin, 1993.
32. W. Conn and L.N. Vaserstein. On sums of three integral cubes. Technical Report PM-131, Department of Mathematics, Pennsylvania State University, 1992. To appear in the Proceedings of a Conference honoring H. Rademacher, AMS Contemporary Mathematics Series.
33. B. Conrey. More than two-fifth of the zeros of the Riemann zeta function are on the critical line. *J. reine angew. Math.*, 399:1–26, 1989.
34. Wolfgang Creyaufmüller. Private communication, August 1994.
35. G. Csordas, T.S. Norfolk, and R.S. Varga. A lower bound for the De Bruijn-Newman constant λ^*. *Numer. Math.*, 52:483–497, 1988.
36. G. Csordas, A.M. Odlyzko, W. Smith, and R.S. Varga. A new Lehmer pair of zeros and a new lower bound for the De Bruijn-Newman constant Λ. *Electronic Transactions on Numerical Analysis*, 1:104–111, December 1993.
37. G. Csordas, A. Ruttan, and R.S. Varga. The Laguerre inequalities with applications to a problem associated with the Riemann hypothesis. *Numerical Algorithms*, 1:305–330, 1991.
38. George Csordas, Wayne Smith, and Richard S. Varga. Lehmer pairs of zeros, the De Bruijn-Newman constant Λ, and the Riemann hypothesis. *Constructive Approximation*, 10:107–129, 1994.
39. J.A. Davis, D.B. Holdridge, and G.J. Simmons. Status report on factoring (at the Sandia National Laboratories). In *Advances in Cryptology*, pages 183–215. Lecture Notes in Computer Science, **209**, 1985.
40. T. Denny, B. Dodson, A. K. Lenstra, and M. S. Manasse. On the factorization of RSA-120. In D.R. Stinson, editor, *Advances in Cryptology – CRYPTO '93*, volume 773 of *Lecture Notes in Computer Science*, pages 166–174, Berlin, 1994. Springer–Verlag.
41. L.E. Dickson. Amicable number triples. *The Amer. Math. Monthly*, 20:84–91, 1913.
42. François Dress. Fonction sommatoire de la fonction de Möbius, 1: Majo-

rations expérimentales. *Experimental Mathematics*, 2:89–98, 1993.

43. H.M. Edwards. *Riemann's Zeta Function.* Academic Press, New York and London, 1974.
44. Achim Flammenkamp. New sociable numbers. *Mathematics of Computation*, 56:871–873, 1991.
45. W. Gabcke. *Neue Herleitung und explizite Restabschätzung der Riemann-Siegel-Formel.* Dissertation, Universität Göttingen, 1979.
46. V.L. Gardiner, R.B. Lazarus, and P.R. Stein. Solutions of the Diophantine equation $x^3+y^3=z^3-d$. *Mathematics of Computation*, 18:408–413, 1964.
47. J.-P. Gram. Sur les zéros de la fonction $\zeta(s)$ de Riemann. *Acta. Math.*, 27:289–304, 1903.
48. A. Granville, J. van de Lune, and H.J.J. te Riele. Checking the Goldbach conjecture on a vector computer. In R.A. Mollin, editor, *Number Theory and Applications*, pages 423–433. Kluwer, 1989.
49. Andrew W.P. Guy and Richard K. Guy. A record aliquot sequence. In Walter Gautschi, editor, *Mathematics of Computation 1943–1993: a Half-Century of Computational Mathematics.* Proceedings of Symposia in Applied Mathematics, American Mathematical Society, 1994. To appear.
50. R.K. Guy. *Unsolved problems in number theory*, volume I of *Unsolved Problems in Intuitive Mathematics.* Springer-Verlag, New York, etc., second edition, 1994.
51. J.L. Hafner and A. Ivić. On the mean-square of the Riemann zeta-function on the critical line. *J. Number Theory*, 32:151–191, 1989.
52. C.B. Haselgrove. A disproof of a conjecture of Pólya. *Matematika*, 5:141–145, 1958.
53. D.R. Heath-Brown. The density of zeros of forms for which weak approximation fails. *Mathematics of Computation*, 59:613–623, 1992.
54. D.R. Heath-Brown. Searching for solutions of $x^3+y^3+z^3=k$. In D. Sinnou, editor, *Sém. Théorie des Nombres, Paris 1989–1990*, pages 71–76. Birkhäuser, 1992.
55. D.R. Heath-Brown. Sign changes of $E(T)$, $\Delta(x)$, and $P(x)$. *J. Number Theory*, 49:73–83, 1994.
56. D.R. Heath-Brown, W.M. Lioen, and H.J.J. te Riele. On solving the Diophantine equation $x^3+y^3+z^3=k$ on a vector computer. *Mathematics of Computation*, 61:235–244, 1993.
    This is a revised version of CWI Report NM-R9121, December 1991.
57. P. Henrici. *Applied and Computational Complex Analysis*, volume I. Wiley, New York, 1977.
58. Marije Huizing. Experiments with the number field sieve. In preparation.
59. A.E. Ingham. On two conjectures in the theory of numbers. *Amer. J. Math.*, 64:313–319, 1942.
60. A. Ivić and H.J.J. te Riele. On the zeros of the error term for the mean square of $|\zeta(\frac{1}{2}+it)|$. *Mathematics of Computation*, 56:303–328, 1991.
61. W. Jurkat and A. Peyerimhoff. A constructive approach to Kronecker approximations and its application to the Mertens conjecture. *J. reine*

angew. Math., 286/287:332–340, 1976.
62. K. Koyama. Review of Kenji Koyama's "Tables of solutions of the Diophantine equation $x^3 + y^3 + z^3 = n$" deposited in the journal's UMT file. *Mathematics of Computation*, 62:941–942, 1994.
63. M. Kraitchik. *Théories des Nombres, Tome II.* Gauthiers-Villars, Paris, 1926.
64. R. Sherman Lehman. On the difference $\pi(x) - \mathrm{li}(x)$. *Acta Arithm.*, 11:397–410, 1966.
65. A.K. Lenstra and H.W. Lenstra, Jr., editors. *The Development of the Number Field Sieve*, volume 1554 of *Lecture Notes in Mathematics.* Springer–Verlag, Berlin, 1993.
66. A.K. Lenstra, H.W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982.
67. A.K. Lenstra, H.W. Lenstra, Jr., M.S. Manasse, and J.M. Pollard. The factorization of the Ninth Fermat number. *Mathematics of Computation*, 61(203):319–349, July 1993.
68. A.K. Lenstra and M.S. Manasse. Factoring with two large primes. *Mathematics of Computation*, 63:785–798, 1994.
69. Arjen K. Lenstra and Mark S. Manasse. Factoring by electronic mail. In J.-J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology — EUROCRYPT '89*, volume 434 of *Lecture Notes in Computer Science*, pages 355–371, Berlin, 1990. Springer–Verlag.
70. H.W. Lenstra, Jr. An iterated divisor function. *The Amer. Math. Monthly*, 84:580, 1977. Solution of Problem 6064.
71. H.W. Lenstra, Jr. Factoring with elliptic curves. *Ann. Math.*, 126:649–673, 1987.
72. Walter Lioen, Herman te Riele, and Dik Winter. Optimization of the MPQS-factorization algorithm on the Cyber 205 and the NEC SX-2. *Supercomputer*, 26:42–50, July 1988.
73. W.M. Lioen and J. van de Lune. Systematic computation of number-theoretic functions by vectorized sieving. To appear, 1995.
74. J. van de Lune. On a conjecture of Erdős, 1. Technical Report ZW 54/75, Mathematisch Centrum, Amsterdam, 1975.
75. J. van de Lune. *Sums of equal powers of positive integers.* PhD thesis, Vrije Universiteit Amsterdam, May 1984.
76. J. van de Lune and H.J.J. te Riele. Explicit computation of special zeros of partial sums of Riemann's zeta function. Technical Report NW 44/77, Mathematisch Centrum, Amsterdam, September 1977.
77. J. van de Lune and H.J.J. te Riele. On the zeros of the Riemann zeta function in the critical strip. III. *Mathematics of Computation*, 41:759–767, 1983.
78. J. van de Lune, H.J.J. te Riele, and D.T. Winter. On the zeros of the Riemann zeta function in the critical strip. IV. *Mathematics of Computation*, 46:667–681, 1986.
79. J. van de Lune and H.J.J. te Riele. On a conjecture of Erdős, 2. Technical

Report ZW 56/75, Mathematisch Centrum, Amsterdam, 1975.

80. J. van de Lune and H.J.J. te Riele. Recent progress on the numerical verification of the Riemann hypothesis. *CWI Newsletter*, 2:35–37, March 1984.

81. J. van de Lune and E. Wattel. Systematic computations on Gauss' lattice point problem (in commemoration of Johannes Gualtherus van der Corput, 1890-1975). Technical Report AM-R9008, Centrum voor Wiskunde en Informatica, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands, 1990.

82. J. van de Lune and E. Wattel. Systematic computation on Dirichlet's divisor problem. To appear, 1995.

83. J.C.P. Miller and M.F.C. Woollett. Solutions of the Diophantine equation $x^3 + y^3 + z^3 = k$. *J. London Math. Soc.*, 30:101–110, 1955.

84. David Moews. Private communication, August 1994.

85. David Moews and Paul C. Moews. A search for aliquot cycles below 10^{10}. *Mathematics of Computation*, 57:849–855, 1991.

86. David Moews and Paul C. Moews. A search for aliquot cycles and amicable pairs. *Mathematics of Computation*, 61:935–938, 1993.

87. H.L. Montgomery. Zeta zeros on the critical line. *The Amer. Math. Monthly*, 86:43–45, 1979.

88. H.L. Montgomery. Zeros of approximations to the zeta function. In P. Erdős, L. Alpár, G. Halász, and P. Turán, editors, *Studies in Pure Mathematics*, pages 497–506. Birkhäuser, Basel, 1983.

89. Peter L. Montgomery. A survey of modern integer factorization algorithms. *CWI Quarterly*, 1994. This Issue.

90. P. Moree, H.J.J. te Riele, and J. Urbanowicz. Divisibility properties of integers x, k satisfying $1^k + 2^k + \cdots + (x-1)^k = x^k$. *Mathematics of Computation*, 63:799–816, 1994.

91. L. Moser. On the Diophantine equation $1^n + 2^n + \cdots + (m-1)^n = m^n$. *Scripta Math.*, 19:84–88, 1953.

92. C.M. Newman. Fourier transforms with only real zeros. *Proc. Amer. Math. Soc.*, 61:245–251, 1976.

93. T.S. Norfolk, A. Ruttan, and R.S. Varga. A lower bound for the De Bruijn-Newman constant Λ. II. In A.A. Gonchar and E.B. Saff, editors, *Progress in Approximation Theory*, pages 403–418, New–York, 1992. Springer–Verlag.

94. A. Odlyzko. Private communication, November 5, 1994.

95. A. M. Odlyzko. The 10^{20}-th zero of the Riemann zeta function and 175 million of its neighbors. Manuscript in preparation.

96. A.M. Odlyzko and A. Schönhage. Fast algorithms for multiple evaluations of the Riemann zeta function. *Trans. Amer. Math. Soc.*, 309:797–809, 1988.

97. A.M. Odlyzko and H.J.J. te Riele. Disproof of the Mertens conjecture. *J. reine angew. Math.*, 357:138–160, 1985.

98. Andrew M. Odlyzko. Analytic computations in number theory. In Walter Gautschi, editor, *Mathematics of Computation 1943–1993: a Half-Century*

of Computational Mathematics. Proceedings of Symposia in Applied Mathematics, American Mathematical Society, 1994. To appear.

99. J. Pintz. An effective disproof of the Mertens conjecture. *Astérisque*, 147/148:325–333, 1987. (Journées arithmétiques, Besançon/France, 1985).
100. C. Pomerance, J.W. Smith, and R. Tuler. A pipeline architecture for factoring large integers with the quadratic sieve algorithm. *SIAM J. Comput.*, 17:387–403, 1988.
101. Carl Pomerance. The quadratic sieve factoring algorithm. In T. Beth, N. Cot, and I. Ingemarsson, editors, *Advances in Cryptology, Proceedings of EUROCRYPT 84*, volume 209 of *Lecture Notes in Computer Science*, pages 169–182, New York, 1985. Springer–Verlag.
102. Herman J.J. te Riele, Walter M. Lioen, and Dik T. Winter. New factorization records on supercomputers. *CWI Newsletter*, 10:40–42, March 1986.
103. Herman J.J. te Riele, Dik T. Winter, and Jan van de Lune. Numerical verification of the Riemann hypothesis on the Cyber 205. In A.H.L. Emmen, editor, *Supercomputer Applications (Proceedings of International Symposium, Amsterdam, Nov. 7–9, 1984)*, pages 33–38. North-Holland, 1985.
104. Herman te Riele, Walter Lioen, and Dik Winter. Factoring with the quadratic sieve on large vector computers. *J. Comp. Appl. Math.*, 27:267–278, 1989.
105. Herman te Riele, Walter Lioen, and Dik Winter. Factorization beyond the googol with MPQS on a single computer. *CWI Quarterly*, 4:69–72, March 1991.
106. H.J.J. te Riele. An amicable pair method for finding amicable triples. In preparation.
107. H.J.J. te Riele. A note on the Catalan-Dickson conjecture. *Mathematics of Computation*, 27:189–192, 1973.
108. H.J.J. te Riele. Four large amicable pairs. *Mathematics of Computation*, 28:309–312, 1974.
109. H.J.J. te Riele. *A theoretical and computational study of generalized aliquot sequences.* PhD thesis, University of Amsterdam, January 1976.
110. H.J.J. te Riele. Computations concerning the conjecture of Mertens. *J. reine angew. Math.*, 311/312:356–360, 1979.
111. H.J.J. te Riele. Tables of the first 15000 zeros of the Riemann zeta function to 28 significant digits, and related quantities. Technical Report NW 67/79, Mathematisch Centrum, Amsterdam, June 1979.
112. H.J.J. te Riele. Iteration of number-theoretic functions. *Nieuw Archief voor Wiskunde (4)*, 1:345–360, 1983.
113. H.J.J. te Riele. New very large amicable pairs. In H. Jager, editor, *Number Theory Noordwijkerhout 1983*, pages 210–215. Springer-Verlag, 1984.
114. H.J.J. te Riele. On generating new amicable pairs from given amicable pairs. *Mathematics of Computation*, 42:219–223, 1984.
115. H.J.J. te Riele. Some historical and other notes about the Mertens conjec-

ture and its recent disproof. *Nieuw Archief voor Wiskunde(4)*, 3:237–243, 1985.

116. H.J.J. te Riele. Computation of all the amicable pairs below 10^{10}. *Mathematics of Computation*, 47:361–368, S9–S40, 1986.
117. H.J.J. te Riele. On the sign of the difference $\pi(x) - \mathrm{li}(x)$. *Mathematics of Computation*, 48:323–328, 1987.
118. H.J.J. te Riele. A new lower bound for the De Bruijn-Newman constant. *Numer. Math.*, 58:661–667, 1991.
119. H.J.J. te Riele. On the history of the function $M(x)/\sqrt{x}$ since Stieltjes. In Gerrit van Dijk, editor, *Thomas Jan Stieltjes – Collected Papers (two volumes)*, pages 69–79 in Vol. 1. Springer-Verlag, 1993.
120. H.J.J. te Riele. A new method for finding amicable pairs. In Walter Gautschi, editor, *Mathematics of Computation 1943–1993: a Half-Century of Computational Mathematics.* Proceedings of Symposia in Applied Mathematics, American Mathematical Society, 1994. To appear.
121. H.J.J. te Riele, W. Borho, S. Battiato, H. Hoffmann, and E.J. Lee. Table of amicable pairs between 10^{10} and 10^{52}. Technical Report NM-N8603, Centrum voor Wiskunde en Informatica, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands, September 1986.
122. B. Riemann. Üeber die Anzahl der Primzahlen unter einer gegebenen Grösse. *Monatsber. Königl. Preuss. Akad. Wiss. Berlin aus den Jahre 1859*, pages 671–680, 1860. Also in "Gesammelte Werke", Teubner, Leipzig, 1892; reprinted by Dover Books, New York, 1953.
123. Hans Riesel. *Prime numbers and computer methods for factorization.* Birkhäuser, Boston, etc., second edition, 1994.
124. R.L. Rivest, A. Shamir, and L. Adelman. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 21:120–126, 1978.
125. H.L. Rolf. Friendly numbers. *Mathematics Teacher*, 60:157–160, 1967.
126. J.W. Sander. Die Nullstellen der Riemannschen Zetafunktion. *Mathematische Semesterberichte*, 39:185–194, 1992.
127. Robert D. Silverman. The multiple polynomial quadratic sieve. *Mathematics of Computation*, 48:329–339, 1987.
128. Matti K. Sinisaldo. Checking the Goldbach conjecture up to 4×10^{11}. *Mathematics of Computation*, 61:931–934, 1993.
129. R. Spira. Zeros of sections of the zeta function. II. *Mathematics of Computation*, 22:163–173, 1968.
130. M.L. Stein and P.R. Stein. Experimental results on additive 2-bases. *Mathematics of Computation*, 19:427–434, 1965.
131. G. Szekeres. Multidimensional continued fractions. *Ann. Univ. Sc. Budapest. de Rolando Eőtvős nom.*, 13:113–140, 1970.
132. E.C. Titchmarsh. *The theory of the Riemann Zeta-function.* Clarendon Press, Oxford, 1986. Second edition, revised by D.R. Heath-Brown.
133. J. Tromp. More computations on Gauss' lattice point problem. Technical Report CS-R9017, Centrum voor Wiskunde en Informatica, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands, 1990.

134. P. Turan. On some approximative Dirichlet polynomials in the theory of the zeta function of Riemann. *Danske Vid. Selsk. Mat. Fys. Medd.*, 24:3–36, 1948.
135. Richard S. Varga. *Scientific computation on mathematical problems and conjectures.* SIAM, Philadelphia, Pennsylvania, 1990.
136. J.H. Wilkinson. *Rounding errors in algebraic processes.* Prentice–Hall, 1963.
137. Dik Winter and Herman te Riele. Optimization of a program for the verification of the Riemann hypothesis. *Supercomputer*, 5, January 1985.
138. S.Y. Yan and T.H. Jackson. A new large amicable pair. *Computers Math. Applics.*, 27:1–3, 1994.