

Grootschalig rekenen in de getaltheorie

Herman te Riele, CWI Amsterdam

KWG Wintersymposium

Utrecht, 7 januari 2012

Outline

- Perfect numbers
- Amicable numbers
- Factorization of large numbers and crypto
- The Riemann hypothesis (RH)
- The 3-Primes Theorem
- Some assertions equivalent with RH
- The Mertens conjecture

Perfect numbers

A **perfect** number is a positive integer equal to the sum of its divisors other than itself. For example,

$$6 = 1 + 2 + 3, 28 = 1 + 2 + 4 + 7 + 14.$$

Equivalent definition: n is **perfect** iff $\sigma(n) = 2n$, where $\sigma(n)$ denotes the sum of the divisors of n .

Find more perfect numbers.

By trial and error, suggests the following:

Theorem (Euclid-Euler) An **even** number n is perfect iff it is of the form $n = 2^{q-1}M_q$, where $M_q = 2^q - 1$ is (a Mersenne) prime.

Currently, 47 even perfect numbers are known, the largest occurring for $q = 43112609$. **GIMPS** Great Internet Mersenne Prime Search, now runs on $\approx 74,000$ computers.

Any **odd** perfect numbers?

Amicable numbers

A pair of numbers (m, n) is called **amicable** if each of them is the sum of the proper divisors of the other, i.e.,

$n = \sigma(m) - m, m = \sigma(n) - n$, for example

$(220, 284) = (2^2 \cdot 5 \cdot 11, 2^2 \cdot 71)$, because

$$\sigma(220) - 220 = 7 \cdot 6 \cdot 12 - 220 = 284 \quad \text{and}$$

$$\sigma(284) - 284 = 7 \cdot 72 - 284 = 220.$$

Find more of them.

By trial and error, with help of computers, suggests the following:

Rule of Thabit ibn Kurrah (9th century)

$2^k pq$ and $2^k r$ form an amicable pair if $p = 3 \cdot 2^{k-1} - 1$,

$q = 3 \cdot 2^k - 1$ and $r = 9 \cdot 2^{2k-1} - 1$ are all primes and $k > 1$.

Works for $k = 2, 4, 7$ and no other value of $k \leq 191600$, **but many more amicable pairs, different from Thabit's form, are known...**

Exhaustive counts

Let $a(X)$ be the number of amicable pairs (m, n) , with $m \leq X$.

From Table of known APs:

X	$a(X)$	$\log(a(X))/\log(X)$ (4 decimals)
10^5	13	0.2228
10^6	42	0.2705
10^7	108	0.2905
10^8	236	0.2966
10^9	586	0.3075
10^{10}	1427	0.3154
10^{11}	3340	0.3203
10^{12}	7642	0.3236
10^{13}	17519	0.3264
10^{14}	39374	0.3282

$a(X)$ taken from <http://amicable.homepage.dk/knwnc2.htm>, which lists

11,994,387 amicable pairs, known on Sept 28, 2007.

Factorization of large numbers and crypto

- The **RSA cryptosystem** was introduced by Rivest, Shamir, and Adleman in 1978; the security of RSA depends on the difficulty to factor large numbers
- the best published factoring result in 1978 was a 39-digit number factored in two CPU-hours ($2^{128} + 1$ by Morrison and Brillhart, Sept. 13, 1970); extrapolation predicted about 62 billion years of CPU time to factor a 512-bit number with 1978 technology
- improved algorithms, much faster computers, **and the very invention of RSA (!)** have pushed us from 118 bits/39 decimals in 1970 to 512 bits/155 decimals in 1999 to 768 bits/232 decimals in 2009

Typical factorization

$n = 1649$. Try to write n as a **difference of squares**. $\sqrt{n} = 40.6 \dots$

$$41^2 = 1681 \equiv 32 \pmod{1649}$$

$$42^2 = 1764 \equiv 115 \pmod{1649}$$

$$43^2 = 1849 \equiv 200 \pmod{1649}$$

Multiply the first and the third congruence:

$$(41 \cdot 43)^2 \equiv 6400 \equiv 80^2 \pmod{1649}$$

$$1763^2 \equiv 114^2 \pmod{1649}, \text{ so}$$

$$114^2 \equiv 80^2 \pmod{1649}, \text{ and}$$

$$\gcd(114 - 80, 1649) = 17 \text{ and } 1649 = 17 \cdot 97.$$

RSA

Every participant has a public and a private key, defined as follows.

Take two large primes, p and q , and compute their product $n = pq$, called the **modulus**.

Choose a number e with

$$1 < e < n \text{ and } \gcd(e, (p - 1)(q - 1)) = 1.$$

Find a number d such that

$$ed \equiv 1 \pmod{(p - 1)(q - 1)}.$$

The public key is the pair (n, e) and the private key is the pair (n, d) (or vice versa).

The primes p and q may be kept secret with the private key, or destroyed.

RSA encryption

Suppose Alice wants to send a message m to Bob.

Alice takes Bobs public key (n, e) from the public-key directory, **encrypts** her message by computing $c = m^e \bmod n$ and sends c to Bob.

Bob **decrypts** with the help of his private key (n, d) by computing $c^d \bmod n$.

By the following theorem of Euler:

$$\text{if } \gcd(m, n) = 1, \text{ then } m^{\phi(n)} \equiv 1 \pmod{n},$$

we have $c^d \equiv (m^e)^d \equiv m^{ed} \equiv m^{k\phi(n)+1} \equiv m \pmod{n}$.

If m was chosen such that $1 < m < n$ then it follows that

$$c^d \bmod n = m.$$

If one would know the factors p and q of n , then finding d would be easy.

Mathematics of public-key cryptosystems

Various mathematical problems arising in the study of public-key cryptosystems:

- factoring large numbers, primality testing
- computing discrete logarithms
- elliptic curves analysis
- analysis of complexity

From these:

- finding polynomials with unusually many smooth values
- solving large sparse systems of linear equations over finite fields
- numerical analysis
- computing square roots of large algebraic numbers
- modular arithmetic, multiprecision arithmetic
- cache optimization, parallel programming
- efficient handling of large amount of data

...

Literature

R. Crandall, Carl Pomerance, *Prime Numbers, A Computational Perspective*, Springer-Verlag, New York, etc., 2001.

A.K. Lenstra, H.W. Lenstra, Jr. (Eds.), *The development of the number field sieve*, Springer-Verlag, Berlin, etc., 1993.

The Riemann hypothesis

The **Riemann zeta function** $\zeta(s)$ is the analytic function of $s = \sigma + it$ defined by:

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

for $\sigma > 1$, and by analytic continuation for $\sigma \leq 1, \sigma \neq 1$. Apart from “trivial” zeros at the negative even integers, all zeros of $\zeta(s)$ lie in the so-called **critical strip** $0 < \sigma < 1$ and symmetric around the line $\sigma = 1/2$ and symmetric around the line $t = 0$.

The **Riemann hypothesis** is the conjecture that all nontrivial zeros of $\zeta(s)$ lie on the so-called **critical line** $\sigma = 1/2$.

History of the Riemann hypothesis

1903	15	Gram
1914	79	Backlund
1925	138	Hutchinson
1935	1,041	Titchmarsh
1953	1,104	Turing
1956	25,000	Lehmer
1958	35,337	Meller
1966	250,000	Lehman
1968	3,502,500	Rosser, Yohe, Schoenfeld
1979	81,000,001	Brent
1982	200,000,001	Brent, Van de Lune, Te Riele, Winter
1983	300,000,001	Van de Lune, Te Riele
1986	1,500,000,001	Van de Lune, Te Riele, Winter
2001	10,000,000,000	Van de Lune
2004	900,000,000,000	Wedeniwski
2004	10,000,000,000,000	Gourdon en Demichel

Some “zeros” of $\zeta(s)$ with Mathematica

```
In[39]:= FindRoot[Zeta[s] == 0, {s, 0}]
```

```
Out[39]= {s → -2.}
```

```
{s → -1.99999999999999973`}
```

```
In[40]:= FindRoot[Zeta[s] == 0, {s, 0.4 + 12 I}]
```

```
Out[40]= {s → 0.5 + 14.1347 i}
```

```
{s → 0.50000000000000071` + 14.134725141734693` i}
```

From complex to real: the Riemann- Siegel function $Z(t)$

$\zeta(s)$ satisfies a functional equation which may be written in the form

$$\xi(s) = \xi(1-s), \quad \text{with} \quad \xi(s) = \pi^{-s/2} \Gamma(s/2) \zeta(s).$$

It follows that, if

$$\theta(t) = \arg \left(\pi^{-\frac{1}{2}it} \Gamma\left(\frac{1}{4} + \frac{1}{2}it\right) \right) = \Im[\log \Gamma\left(\frac{1}{4} + \frac{1}{2}it\right)] - \frac{t}{2} \log \pi,$$

then

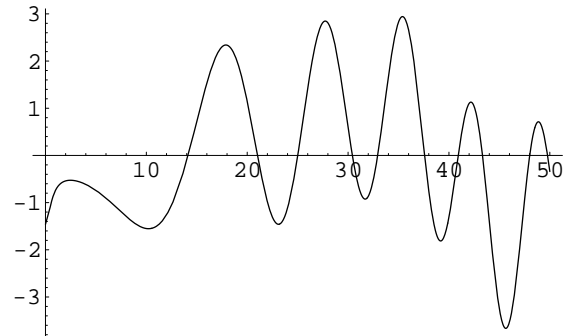
$$Z(t) = e^{i\theta(t)} \zeta\left(\frac{1}{2} + it\right)$$

is **real** (for real t). Since $|Z(t)| = |\zeta(\frac{1}{2} + it)|$, the zeros of Z are the **imaginary parts** of the zeros of $\zeta(s)$ on the **critical line**.

$Z(t)$ is known as the **Riemann-Siegel** function.

Some plots of $Z(t)$ with Mathematica

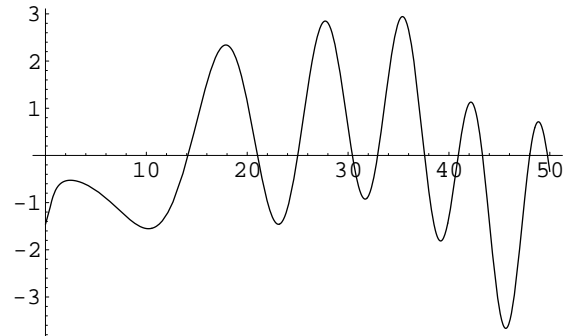
```
In[63]:= Plot[RiemannSiegelZ[t], {t, 0, 50}]
```



```
Out[63]= - Graphics -
```

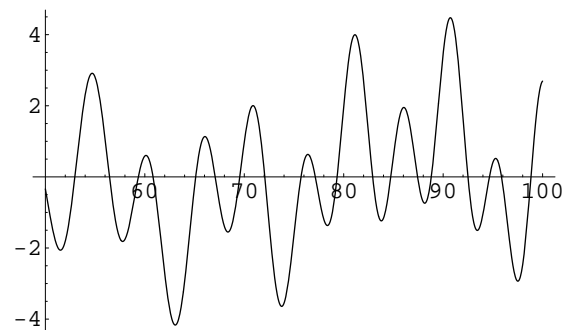
Some plots of $Z(t)$ with Mathematica

```
In[63]:= Plot[RiemannSiegelZ[t], {t, 0, 50}]
```



```
Out[63]= - Graphics -
```

```
In[64]:= Plot[RiemannSiegelZ[t], {t, 50, 100}]
```

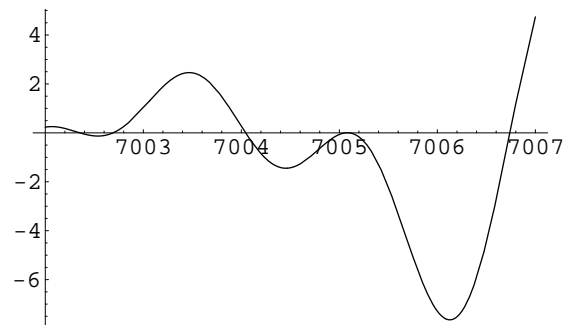


```
Out[64]= - Graphics -
```

Another plot of $Z(t)$

Close zeros: **Lehmer phenomenon**

```
In[61]:= Plot[RiemannSiegelZ[t], {t, 7002, 7007}]
```

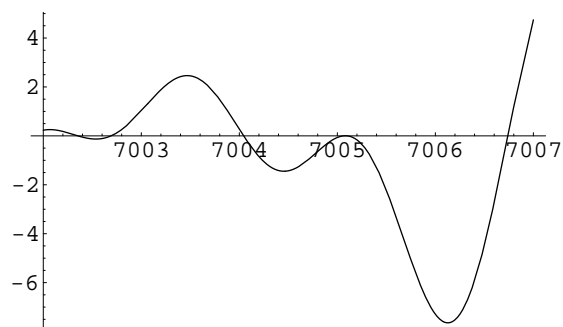


```
Out[61]= - Graphics -
```

Another plot of $Z(t)$

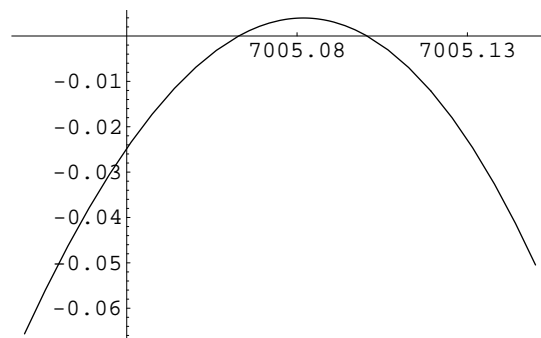
Close zeros: **Lehmer phenomenon**

```
In[61]:= Plot[RiemannSiegelZ[t], {t, 7002, 7007}]
```



```
Out[61]= - Graphics -
```

```
In[62]:= Plot[RiemannSiegelZ[t], {t, 7005, 7005.15},  
  Ticks -> {{7005.03, 7005.08, 7005.13}, Automatic}]
```



```
Out[62]= - Graphics -
```

Total number of zeros in a given part of the critical strip

Backlund proved around 1912 that the total number $N(T)$ of complex zeros ρ of $\zeta(s)$ with $0 < \Im(\rho) < T$ (counting multiplicities) can be expressed as

$$N(T) = \frac{\theta(T)}{\pi} + 1 + \frac{1}{\pi} \Im \left\{ \int_C \frac{\zeta'(s)}{\zeta(s)} ds \right\},$$

where C is the broken line segment from $1 + \epsilon$ (for some $\epsilon > 0$) to $1 + \epsilon + iT$ to $\frac{1}{2} + iT$.

Backlund observed that if $\Re \zeta \neq 0$ on C , then this formula suffices to determine $N(T)$ as **the nearest integer** to $\theta(T)/\pi + 1$.
Expansion:

$$\theta(t) = \frac{t}{2} \log \frac{t}{2\pi} - \frac{t}{2} - \frac{\pi}{8} + \frac{1}{48t} + \mathcal{O}(t^{-3}), \quad \text{as } t \rightarrow \infty.$$

Example: $\theta(100)/\pi + 1 = 29.0024\dots$

The Euler-Maclaurin formula for $\zeta(s)$

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

where

$$T_{k,n} = \frac{B_{2k}}{(2k)!} n^{1-s-2k} \prod_{j=0}^{2k-2} (s+j), \quad |E_{m,n}| < \left| T_{m+1,n} \left(\frac{s+2m+1}{\sigma+2m+1} \right) \right|$$

for all $m \geq 0$, $n \geq 1$ en $\sigma = \Re(s) > -(2m+1)$.

B_{2k} , $k = 1, 2, \dots$ are the Bernoulli-numbers:

$$B_2 = 1/6, B_4 = -1/30, B_6 = 1/42, \dots$$

For $s = \frac{1}{2} + it$ a good choice for m, n is: $m \approx \sqrt{n}$ and $n \approx t/(2\pi)$.

Complexity: $\mathcal{O}(t)$.

The Riemann-Siegel formula for $Z(t)$

Let $\tau := t/(2\pi)$, $m := \lfloor \tau^{1/2} \rfloor$, and $z := 2(\tau^{1/2} - m) - 1$, then

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

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

with $\Phi(z) = \dots$ and $R_n(\tau) = \mathcal{O}(\tau^{-(2n+3)/4})$, $n \geq -1$, $\tau > 0$.

For $\tau > 32$ ($t > 200$) we have $|R_n(\tau)| < d_n \tau^{-(2n+3)/4}$ with

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

(Doctor's Thesis **Gabcke**). **Complexity: $\mathcal{O}(\sqrt{t})$.**

Gram points and Gram's "Law"

The **Gram point** $g_m, m = -1, 0, 1, \dots$, is the unique solution in $[7, \infty)$ of the equation

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

The value of the first term $2 \cos(\theta(t))$ in the Riemann-Siegel formula in the Gram point $t = g_m$ equals

$$2 \cos(\theta(g_m)) = 2 \cos(m\pi) = 2(-1)^m.$$

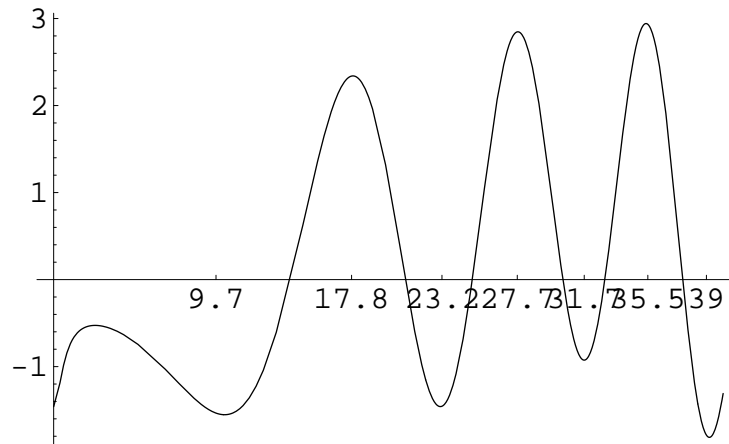
Gram's "Law" is the tendency of the **zeros** of $Z(t)$ to **alternate with the Gram points** (based on the expectation that the first term in the RS formula dominates).

Unfortunately, this "Law" fails infinitely often, but it is known that **on average there is precisely one zero of $Z(t)$ in between two consecutive Gram points.**

Illustration of Gram's “Law”

$g_{-1}, g_0, g_1, g_2, g_3, g_4, g_5 =$
 $9.7, 17.8, 23.2, 37.7, 31.7, 35.5, 39.0$

```
In[88]:= Plot[RiemannSiegelZ[t], {t, 0, 40},
  Ticks -> {{9.7, 17.8, 23.2, 27.7, 31.7, 35.5, 39.0, 42.34}, Automatic}]
```



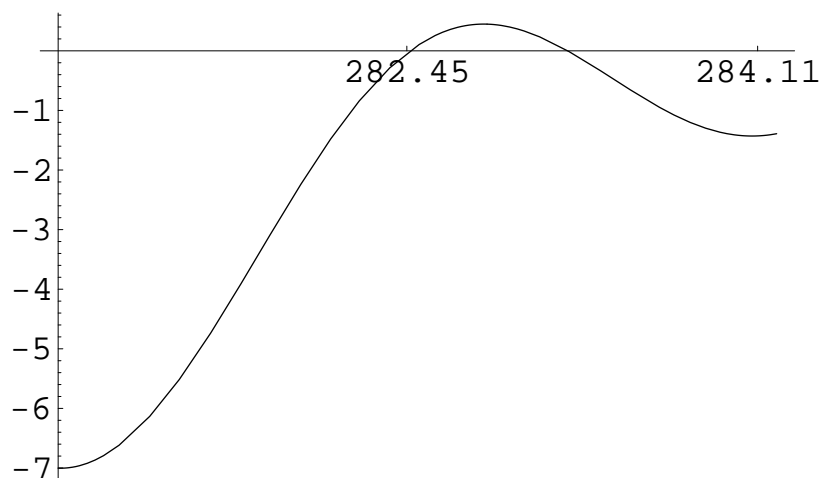
```
Out[88]= - Graphics -
```

First violation of Gram's "Law"

$g_{125}, g_{126}, g_{127} =$
280.80, 282.45, 284.11

`In[112]:=`

```
Plot[RiemannSiegelZ[t], {t, 280.8, 284.2}, Ticks -> {{280.8, 282.45, 284.11}, Automatic}]
```



`Out[112]=`

- Graphics -

Literature

H.M. Edwards, *Riemann's Zeta Function*, Academic Press, New York and London, 1974.

E.C. Titchmarsh, *The Theory of the Riemann Zeta-function*, Second edition, revised by D.R. Heath-Brown, Clarendon Press, Oxford, 1986.

R. van der Veen, J. van de Craats, *De Riemann-hypothese, een miljoenenprobleem*, Epsilon-uitgaven, deel 69, 2011.

The 3-Primes Theorem

Theorem (Deshouillers, Effinger, tR, Zinoviev, 1997)

If the Generalized Riemann Hypothesis holds, then **every odd number > 5 can be written as a sum of three primes.**

GRH: all non-trivial zeros of all Dirichlet L -functions have real part equal to $1/2$.

Unconditionally: every odd number $> 10^{43000}$ can be written as a sum of three primes (Chen and Wang, 1989).

The **Goldbach conjecture** (GC) states that every even number ≥ 4 can be written as a sum of two primes.

It implies the 3-Primes Theorem, but the converse does not hold.

The 3-Primes Theorem, 2

The 3-Primes Theorem is a consequence of the following three lemmas.

Lemma 1 (Zinoviev, 1997)

Assuming GRH, every odd number $> 10^{20}$ is a sum of three prime numbers.

Lemma 2 Assuming GRH, if $6 \leq n \leq 10^{20}$, then there exists a prime number p such that $4 \leq n - p \leq 1.615 \times 10^{12}$.

Lemma 3 (Deshouillers and tR, 1997)

Every even number $4 \leq m \leq 10^{13}$ is a sum of two prime numbers (improving the bound 4×10^{11} of Sinisalo, 1993).

Currently, the Goldbach conjecture has been proved to be true for all even numbers $\leq 2.6 \times 10^{18}$ (Oliveira e Silva).

Usual approach to verify GC

Let p_i be the i th odd prime number. The usual approach to verify GC on a given interval $[a, b]$ is to find, for every even $e \in [a, b]$, the smallest odd prime p_i such that $e - p_i$ is a prime.

An efficient way to do this is to generate the set of primes

$$Q(a, b) = \{q \mid q \text{ prime and } a - \epsilon_a \leq q \leq b\},$$

where ϵ_a is chosen in a suitable way, and to generate the sets of even numbers $\mathcal{E}_0 \subset \mathcal{E}_1 \subseteq \mathcal{E}_2 \subseteq \dots$, defined by $\mathcal{E}_0 = \emptyset$,

$$\mathcal{E}_{i+1} = \mathcal{E}_i \cup (Q(a, b) + p_{i+1}), i = 0, 1, \dots$$

until, for some j , \mathcal{E}_j covers **all** the even numbers in $[a, b]$.

The set of primes $Q(a, b)$ is generated with the sieve of Eratosthenes. The number ϵ_a must exceed the largest odd prime used in the generation of the sets \mathcal{E}_i .

Alternative approach to verify GC

Find, for every even $e \in [a, b]$, a prime q , close to a , for which $e - q$ is prime. To that end a set of k consecutive primes q_1, q_2, \dots, q_k close to a is generated, for suitably chosen k , and a large set \mathcal{P} of all the odd primes up to about $b - a$ is precomputed (with the sieve of Eratosthenes) in order to check the numbers $e - q$ for primality.

For the actual check we generate the sets of even numbers $\mathcal{F}_0 \subset \mathcal{F}_1 \subseteq \mathcal{F}_2 \subseteq \dots$, defined by $\mathcal{F}_0 = \emptyset$,

$$\mathcal{F}_{i+1} = \mathcal{F}_i \cup (\mathcal{P} + q_{i+1}), i = 0, 1, \dots$$

until, for some j , \mathcal{F}_j covers **all** the even numbers in $[a, b]$.

Comparison

In the **first** approach a **small** set of small primes up to 5000, say, has to be generated and for each interval $[a, b]$ treated **all** the primes in $[a, b]$ have to be generated.

In the **second** approach, a **large** set of small primes up to about $10^8 + 10^4$, say, has to be generated (only once for all intervals $[a, b]$ treated), and for each interval $[a, b]$ one has to find the k largest primes $\leq a$. This of course is much cheaper than the first approach.

The difference is that the first approach finds for each even number e the **smallest** odd prime for which $e - p$ is prime. In the second approach **some** prime p is found for which $e - p$ is prime but in general this p is neither the smallest neither the largest such prime.

Experiments to verify GC up to 10^{13}

We chose the length of the interval $[a, b]$ equal to 10^8 . The largest prime we may need in the set \mathcal{P} lies close to $b - q_1$. How large can we expect k to be in practice? The density of the odd primes among the odd numbers up to 10^8 is about 0.115 (there are 5761454 odd primes below 10^8 and 5×10^7 odd numbers below 10^8). So a proportion of about 0.885 of the even numbers in $[a, b]$ is **not covered** by the set $\mathcal{F}_1 = \mathcal{P} + q_1$; assuming uniform distribution of the primes, about 0.885^2 of the even numbers would not be covered by \mathcal{F}_2 , and so on. After 151 steps this proportion is reduced to 10^{-8} . For our experiments $k = 360$ turned out to be sufficient. For $a \approx 10^{13}$ this implies that the largest prime in the set \mathcal{P} lies close to $10^8 + 10^4$. Total CPU time on a Cray C98 vector computer was about 50 CPU hours.

With this approach we also verified GC in $[10^{10i}, 10^{10i} + 10^9]$, for $i = 20, 21, \dots, 30$, in about 1000 CPU hours on the Cray C98.

Literature

J.-M. Deshouillers, G. Effinger, H. te Riele, D. Zinoviev, A complete Vinogradov 3-primes theorem under the generalized Riemann hypothesis, *Electr. Research Announcements of the Amer. Math. Soc.* 3 (1997), 99–104 (Sept. 17, 1997).

J.-M. Deshouillers, H.J.J. te Riele, Y. Saouter, *New experimental results concerning the Goldbach conjecture*, Proc. of ANTS III, Portland, Oregon, USA, June 21–25, 1998, LNCS 1423, Springer (also appeared as Report MAS-R9804, March 1998, CWI Amsterdam).

Some assertions equivalent with RH, 1

For given $x > 1$ consider the rational numbers which, when expressed in lowest terms, have the denominators $< x$ and lie in $(0, 1]$. This is called the **Farey sequence corresponding to x** . For $x = 7\frac{1}{2}$, this is:

$$\frac{1}{7}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{2}{7}, \frac{1}{3}, \frac{2}{5}, \frac{3}{7}, \frac{1}{2}, \frac{4}{7}, \frac{3}{5}, \frac{2}{3}, \frac{5}{7}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{6}{7}, 1.$$

Let $A(x)$ be the number of terms in this sequence.

Let δ_j , $j = 1, 2, \dots, A(x)$, be the amount by which the j th term of the Farey sequence differs from $j/A(x)$.

The Riemann hypothesis is equivalent to the statement that for every $\epsilon > 0$ the function $(|\delta_1| + |\delta_2| + \dots + |\delta_{A(x)}|)/x^{1/2+\epsilon}$ tends to zero as $x \rightarrow \infty$.

Some assertions equivalent with RH, 2

The Riemann hypothesis is equivalent to the statement that for every $\epsilon > 0$ the function $M(x)/x^{1/2+\epsilon}$ tends zero as $x \rightarrow \infty$.

Here, $M(x) = \sum_{1 \leq n \leq x} \mu(n)$ and $\mu(n)$ is the **Möbius function** defined by $\mu(1) = 1$, $\mu(n) = (-1)^k$ if n is the product of k distinct primes, and $\mu(n) = 0$ otherwise.

There is some numerical evidence that $M(x)/x^{1/2}$ grows like $\sqrt{\log \log \log x}$ (Kotnik and van de Lune).

The Mertens conjecture

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

The *Mertens conjecture (1897)* states that

$|M(x)|/\sqrt{x} < 1$ for all $x > 1$. This – but also the weaker assumption $|M(x)|/\sqrt{x} < C$ for all $x > 1$ and some $C > 1$ – would imply the truth of the Riemann hypothesis.

The Mertens conjecture, 2

The Mertens conjecture was shown to be false by Odlyzko and Te Riele in 1985 with help of the lattice basis reduction (L^3) algorithm of A.K. Lenstra, H.W. Lenstra, Jr., and L. Lovász (1982) for finding short vectors in lattices.

OtR proved the **existence** of some x for which $M(x)/\sqrt{x} > 1.06$, and of some other x for which $M(x)/\sqrt{x} < -1.009$.

In 1987, Pintz gave an **effective** disproof of the Mertens conjecture in the sense that he proved that $|M(x)|/\sqrt{x} > 1$ for some $x \leq \exp(3.21 \times 10^{64})$.

Nowadays, it is generally believed that the function $M(x)/\sqrt{x}$ is **unbounded**, both in the positive and in the negative direction.

Notation

The complex zeros of the Riemann zeta function are denoted by $\rho_j = \frac{1}{2} + i\gamma_j$ (we work in the range where the Riemann hypothesis is known to be true) with $\gamma_1 = 14.1347\dots$ and

$$\gamma_j < \gamma_{j+1}, j = 1, 2, \dots$$

Furthermore, we write $\psi_j = \arg \rho_j \zeta'(\rho_j)$ and $\alpha_j = |\rho_j \zeta'(\rho_j)|^{-1}$.

We also consider the zeros ρ_j ordered according to

non-increasing values of α_j , and denote them by $\rho_j^* = \frac{1}{2} + i\gamma_j^*$

with the corresponding quantities $\psi_j^*, \alpha_j^*, j = 1, 2, \dots$

For example, the first five ρ_j^* 's coincide with the first five ρ_j 's, but

$$\rho_6^* = \rho_7, \rho_7^* = \rho_{10}, \text{ and } \rho_8^* = \rho_6$$

(with $\alpha_6^* = \alpha_7 = 0.0163\dots, \alpha_7^* = \alpha_{10} = 0.0141\dots$ and

$$\alpha_8^* = \alpha_6 = 0.0137\dots).$$

The first ten γ_j 's

j	γ_j	ψ_j	α_j	γ_j^*
1	14.1347	1.6933	0.0891	14.1347
2	21.0220	1.3264	0.0418	21.0220
3	25.0109	1.8851	0.0291	25.0109
4	30.4249	1.0169	0.0252	30.4249
5	32.9351	2.1297	0.0220	32.9351
6	37.5862	1.2636	0.0137	40.9187
7	40.9187	1.3540	0.0164	49.7738
8	43.3271	2.2052	0.0126	37.5862
9	48.0052	0.7096	0.0133	48.0052
10	49.7738	2.0372	0.0142	43.3271

Direct approach

Systematic computations of $M(x)$ for all $x \in [1, X]$ by Mertens and many others have not led to a disproof of the Mertens conjecture. For $X = 10^{14}$, Kotnik and Van de Lune found the largest **positive** value of $M(x)/\sqrt{x}$ to be 0.571 for $x = 7\,766\,842\,813$ and the largest **negative** value to be -0.525 for $x = 71\,578\,936\,427\,177$.

Another approach

Another approach is based on the following theorem of Titchmarsh (1951):

Theorem 1 *If all the zeros of the Riemann zeta-function are simple, then there is an increasing sequence $\{T_n\}$ such that*

$$(1) \quad M(x) = \lim_{n \rightarrow \infty} \sum_{|\gamma| < T_n} \frac{x^\rho}{\rho \zeta'(\rho)} - R(x) + \sum_{n=1}^{\infty} \frac{(-1)^{n-1} (2\pi/x)^{2n}}{(2n)! n \zeta(2n+1)}$$

where $R(x) = 2 - \frac{\mu(x)}{2}$ if x is an integer, and $R(x) = 2$ otherwise.

On the Riemann hypothesis, we have $\rho = \frac{1}{2} + i\gamma$, giving:

$$(2) \quad \frac{M(x)}{\sqrt{x}} = 2 \lim_{n \rightarrow \infty} \sum_{0 < \gamma < T_n} \frac{\cos(\gamma \log x - \psi_\gamma)}{|\rho \zeta'(\rho)|} + O(x^{-1/2}).$$

Hence, as n increases, the sum in (2) will eventually converge to $M(x)/\sqrt{x}$, with error on the order of magnitude of $1/\sqrt{x}$. However, very little is known about the rate of this convergence, as the coefficients $|\rho_j \zeta'(\rho_j)|^{-1}$ do not form a monotonically decreasing sequence, but instead behave quite irregularly. For some values of x up to 10^{14} , this rate of convergence has been studied computationally by Kotnik and Van de Lune: several thousands of terms generally suffice to bring the error below 1%, but for much larger x this approach is not feasible.

Ingham's tric

The tric of Ingham was to consider, instead of (2), a **weighted average of the function** $M(x)/\sqrt{x}$. In that case the terms of the sum in (2) are multiplied by a function of bounded support, and the series in (1) is transformed into a finite sum. Two such cases will appear in what follows.

We write $x = e^y$, $-\infty < y < \infty$, and define

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

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

Ingham's tric, 2

Then we have the following

Theorem 2 *Let*

$$h(y, T) := 2 \sum_{0 < \gamma < T} \left[\left(1 - \frac{\gamma}{T}\right) \cos\left(\pi \frac{\gamma}{T}\right) + \pi^{-1} \sin\left(\pi \frac{\gamma}{T}\right) \right] \frac{\cos(\gamma y - \psi_\gamma)}{|\rho \zeta'(\rho)|}$$

where $\rho = \beta + i\gamma$ are the complex zeros of the Riemann zeta function which satisfy $\beta = \frac{1}{2}$ and which are simple. Then **for any real y_0** we have

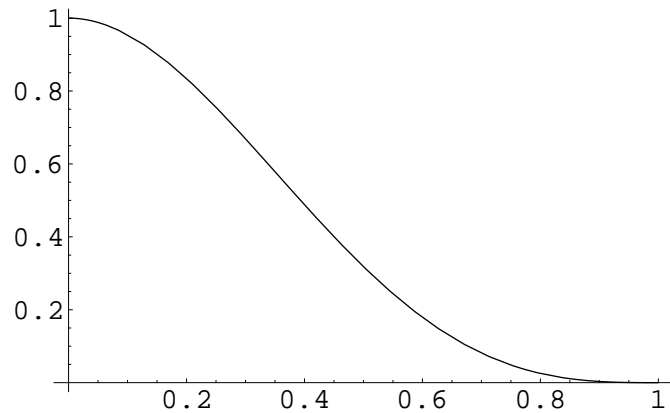
$$\underline{m} \leq h(y_0, T) \leq \overline{m}$$

and **any value $h(y, T)$ is approximated arbitrarily closely, and infinitely often, by $M(x)/\sqrt{x}$.**

Notice that also **negative** values of y_0 are allowed.

Graph of $(1 - t) \cos(\pi t) + \pi^{-1} \sin(\pi t)$

```
Plot[(1 - t) * Cos[Pi * t] + Sin[Pi * t] / Pi, {t, 0, 1}]
```



An inhomogeneous Diophantine approximation problem

Since

$$(1 - t) \cos(\pi t) + \pi^{-1} \sin(\pi t) > 0 \text{ for } 0 < t < 1$$

and since it is known that $\sum_{\rho} |\rho \zeta'(\rho)|^{-1}$ diverges, the sum of the **coefficients** of $\cos(\gamma y - \psi_{\gamma})$ in Theorem 2 can be made arbitrarily large by choosing T large enough. Consequently, if we could find a value of y such that **all of the $\gamma y - \psi_{\gamma}$ are close to integer multiples of 2π** , then we could make $h(y, T)$ arbitrarily large. This would contradict, by Theorem 2, the conjecture of Mertens or any weaker form given above.

An inhomogeneous ..., 2

If the γ 's were linearly independent over the rationals, then by Kronecker's theorem there would indeed exist, for any $\epsilon > 0$, integer values of y satisfying

$$|\gamma y - \psi_\gamma - 2\pi m_\gamma| < \epsilon$$

for all $\gamma \in (0, T)$ and certain integers m_γ . This would show that $h(y, T)$, and hence $M(x)/\sqrt{x}$, can be made arbitrarily large. On the same assumptions, a similar argument can be given to imply that $h(y, T)$, and hence $M(x)/\sqrt{x}$, can be made arbitrarily large on the negative side.

No good reason is known why among the γ 's there should exist any linear dependencies over the rationals.

The lattice basis reduction algorithm

The approach which actually led to a disproof of the Mertens conjecture was based on the now well-known **lattice basis reduction (L^3 -) algorithm of Lenstra (A.K.), Lenstra (H.W.) and Lovász for finding short vectors in lattices.**

With this algorithm, the inhomogeneous Diophantine approximation problem could be solved for a much larger number of terms than before the time that L^3 was known.

The **“prize” to pay** was that any value of y that would come out was quite large. Therefore, the first 2000 γ 's were (and had to be) computed with an accuracy of about 100 decimal digits.

The best lower and upper bounds found in 1985 for \overline{m} and \underline{m} were **1.06** and **-1.009**, respectively.

How is L^3 applied?

In order to find a y such that each of the numbers

$$(3) \quad (\gamma_j^* y - \psi_j^*) \bmod 2\pi, \quad 1 \leq j \leq n,$$

is small, we transform this problem into a problem about short vectors in lattices as follows. The lattice L used is generated by the columns $\underline{v}_1, \underline{v}_2, \dots, \underline{v}_{n+2}$ of the following $(n+2) \times (n+2)$ matrix (here $[x]$ means the greatest integer $\leq x$):

The input matrix for L^3

$$\begin{array}{ccccccc}
 -[\sqrt{\alpha_1^*} \psi_1^* 2^\nu] & [\sqrt{\alpha_1^*} \gamma_1^* 2^{\nu-10}] & [2\pi \sqrt{\alpha_1^*} 2^\nu] & 0 & \dots & 0 \\
 -[\sqrt{\alpha_2^*} \psi_2^* 2^\nu] & [\sqrt{\alpha_2^*} \gamma_2^* 2^{\nu-10}] & 0 & [2\pi \sqrt{\alpha_2^*} 2^\nu] & \dots & 0 \\
 \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
 \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
 \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
 -[\sqrt{\alpha_n^*} \psi_n^* 2^\nu] & [\sqrt{\alpha_n^*} \gamma_n^* 2^{\nu-10}] & 0 & 0 & \dots & [2\pi \sqrt{\alpha_n^*} 2^\nu] \\
 2^\nu n^4 & 0 & 0 & 0 & \dots & 0 \\
 0 & 1 & 0 & 0 & \dots & 0
 \end{array}$$

where ν is an integer satisfying $2n \leq \nu \leq 4n$.

The L^3 algorithm produces a reduced basis $\underline{v}'_1, \underline{v}'_2, \dots, \underline{v}'_{n+2}$ for the lattice L , where each new basis vector is a linear combination of the $n + 2$ given basis vectors.

Now the $(n + 1)$ -st coordinate of \underline{v}'_1 , which has value $2^\nu n^4$, is very large compared to all the other entries of the original basis. Since the reduced basis is a basis for the lattice L , it should contain **precisely one vector \underline{w} which has a nonzero coordinate in the $(n + 1)$ -st position and that coordinate should be $\pm 2^\nu n^4$.** Without loss of generality this may be taken to be $2^\nu n^4$.

Given the original lattice basis, the j -th coordinate of this vector \underline{w} equals, for $1 \leq j \leq n$:

$$z \left[\sqrt{\alpha_j^*} \gamma_j^* 2^{\nu-10} \right] - \left[\sqrt{\alpha_j^*} \psi_j^* 2^\nu \right] - m_j \left[2\pi \sqrt{\alpha_j^*} 2^\nu \right]$$

and the $(n+2)$ -nd coordinate is z , for some integers z, m_1, m_2, \dots, m_n . If the length of \underline{w} is small, all of the

$$z \sqrt{\alpha_j^*} \gamma_j^* 2^{\nu-10} - \sqrt{\alpha_j^*} \psi_j^* 2^\nu - m_j 2\pi \sqrt{\alpha_j^*} 2^\nu$$

will be small, i.e., all of the

$$\beta_j = \sqrt{\alpha_j^*} (y \gamma_j^* - \psi_j^* - 2\pi m_j)$$

will be very small, where $y = z/1024$.

The reason for the presence of the numbers α_j^* in the lattice basis is that we want to make the sum

$$\sum_{j=1}^n \alpha_j^* \cos(\gamma_j^* y - \psi_j^* - 2\pi m_j)$$

large. If the cos-arguments are all close to zero, this sum will approximately be equal to:

$$\sum_{j=1}^n \alpha_j^* - \frac{1}{2} \sum_{j=1}^n [\sqrt{\alpha_j^*} (\gamma_j^* y - \psi_j^* - 2\pi m_j)]^2,$$

and therefore we want the second sum to be small. This corresponds to minimizing the euclidean norm of the vector $(\beta_1, \beta_2, \dots, \beta_n)$ which is what the L^3 algorithm attempts to do.

Example

$$n = 4, \nu = 8, L = \begin{bmatrix} -129 & 1 & 480 & 0 & 0 & 0 \\ -69 & 1 & 0 & 328 & 0 & 0 \\ -82 & 1 & 0 & 0 & 274 & 0 \\ -41 & 1 & 0 & 0 & 0 & 255 \\ 65536 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$L' = \begin{bmatrix} 1 & -51 & -55 & -66 & -213 & -65 \\ 1 & -51 & -55 & -262 & 61 & -5 \\ 1 & -51 & 219 & -66 & 7 & -18 \\ 1 & 204 & -55 & -66 & -12 & 23 \\ 0 & 0 & 0 & 0 & 0 & 65536 \\ 1 & -51 & -55 & -66 & -267 & 64 \end{bmatrix}$$

$$z = 64, y = z/1024 = 0.0625$$

Example, cont.

norms of vectors of L :

2.236, 255, 274, 328, 480, 65536.227

product= 1.6×10^{15}

norms of vectors of L' :

2.236, 228.079, 245.073, 293.373, 347.235, 65536.070

product= 8.3×10^{14}

j	α_j^*	$\cos(\gamma_j^* y - \psi_j^*)$	$\alpha_j^* \cos(\gamma_j^* y - \psi_j^*)$
1	0.0891	0.6896	0.0614
2	0.0418	0.9999	0.0418
3	0.0291	0.9486	0.0276
4	0.0252	0.6336	0.0160
sum:	0.1852		0.1468

Application of L^3

We (Kotnik and HtR) have applied the L^3 algorithm with the matrix (4) as input, for all the combinations (ν, n) in the range $\nu = 8, 9, \dots, 400$, $n = \lceil \nu/4 \rceil, \lceil \nu/4 \rceil + 1, \dots, \lceil \nu/2 \rceil$. To this end we used the function `qflll` from the PARI/GP package. For a given ν , the **precision** by which the computations were carried out was chosen to be **$\log_{10}(2^{2\nu})$ decimal digits**. For each combination of ν and n a number $z = z(\nu, n)$ was generated as described above and we computed the local maximum of $h(y, T)$ as defined above with y in the neighborhood of $z/1024$, and $T = \gamma_{10000}$. The γ_j 's were computed to an accuracy of **about 250 decimal digits** using the Mathematica package, and, as a check, using the PARI/GP package. The computing time was about **600 CPU hours** on the SGI Altix 3700 Aster system of the Academic Computing Centre Amsterdam (SARA).

Scatter plot of the large positive values of h

Figure 1 gives for each $\nu = 8, 9, \dots, 400$ and for each value of $z(\nu, n)$ which was found by the L^3 algorithm, a scatter plot of the positive values of

$$h(z(\nu, n)/1024, \gamma_{2000}).$$

For increasing values of ν , the corresponding h -values are increasing on average, but at a rate that seems to decrease. For the negative values of h the pattern is very similar. Reaching 1.3 and -1.3 would likely require a value of ν in the neighborhood of 800.

*Large positive values of h ,
hence of $M(x)/\sqrt{x}$*

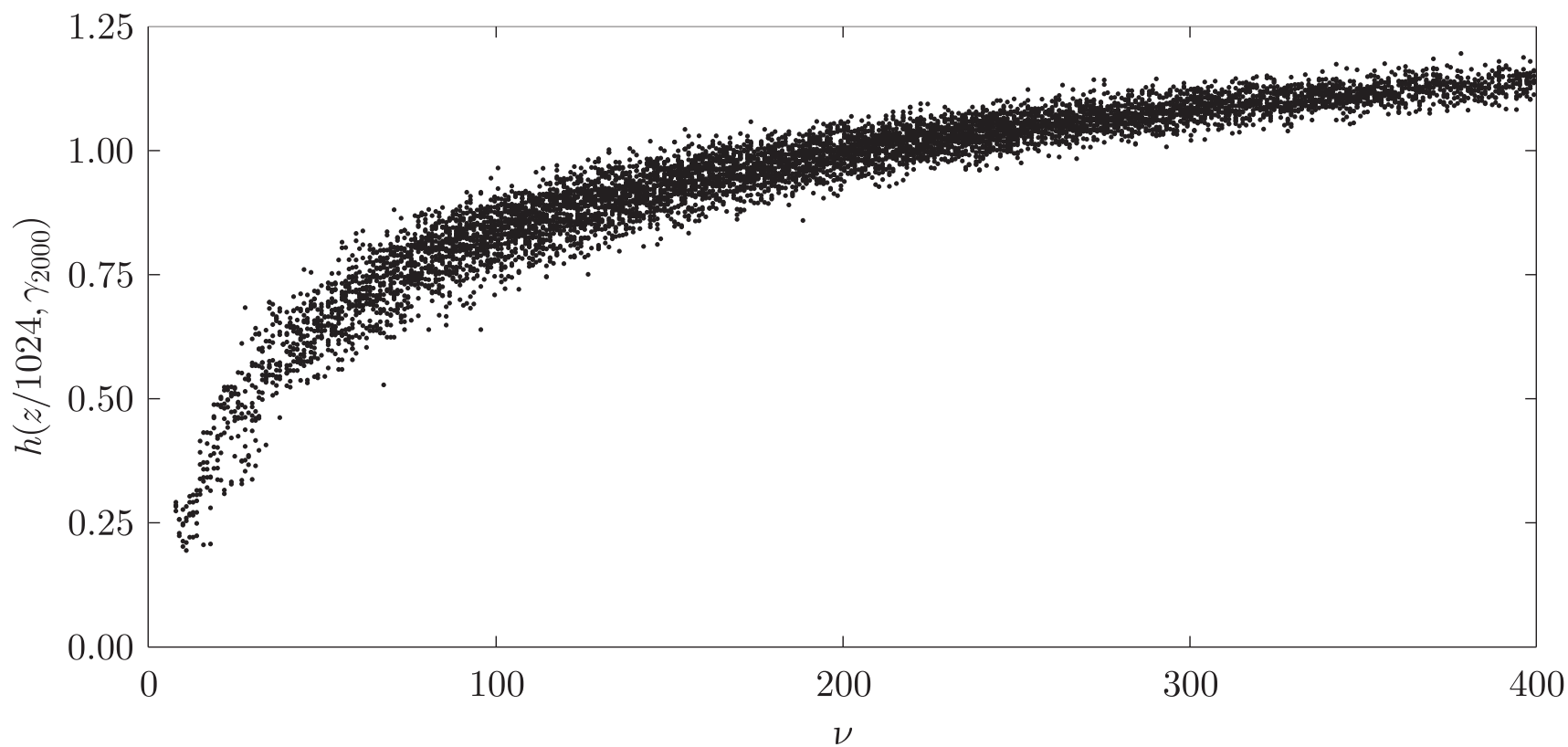


FIGURE 1

Champions

For the most promising values of h obtained, we computed the local maximum resp. minimum of $h(y, \gamma_{10000})$ in the neighborhood of $y = z/1024$. On the positive side, our champion (found with $\nu = 379, n = 98$) is

$y = -233029271\ 5134531215\ 0140181996\ 7723401020\ 4456785091\ \backslash$
 $6681557518\ 6743434036\ 9240230890\ 8933261706\ 9029233958\ \backslash$
 2730162362.807965 ($\log_{10} |y| = 108.3 \dots$)

with $h(y, \gamma_{10000}) = 1.218429$

and on the negative side, our champion (found with $\nu = 396, n = 102$) is

$y = -1608\ 7349754400\ 0919817483\ 9640165505\ 4685212472\ \backslash$
 $2284778177\ 5539303027\ 5350690810\ 7957194829\ 6433602695\ \backslash$
 $1442102295\ 3212754000.679958$ ($\log_{10} |y| = 113.2 \dots$)

with $h(y, \gamma_{10000}) = -1.229385$.

Behaviour of $M(e^y)/e^{y/2}$ near the cham-pions

Figure 2 compares the typical behaviour of $M(e^y)/e^{y/2}$ (top) with the behaviour of $h(y, \gamma_{10000})$ around the 1.218–spike (middle) and around the -1.229 –spike (bottom).

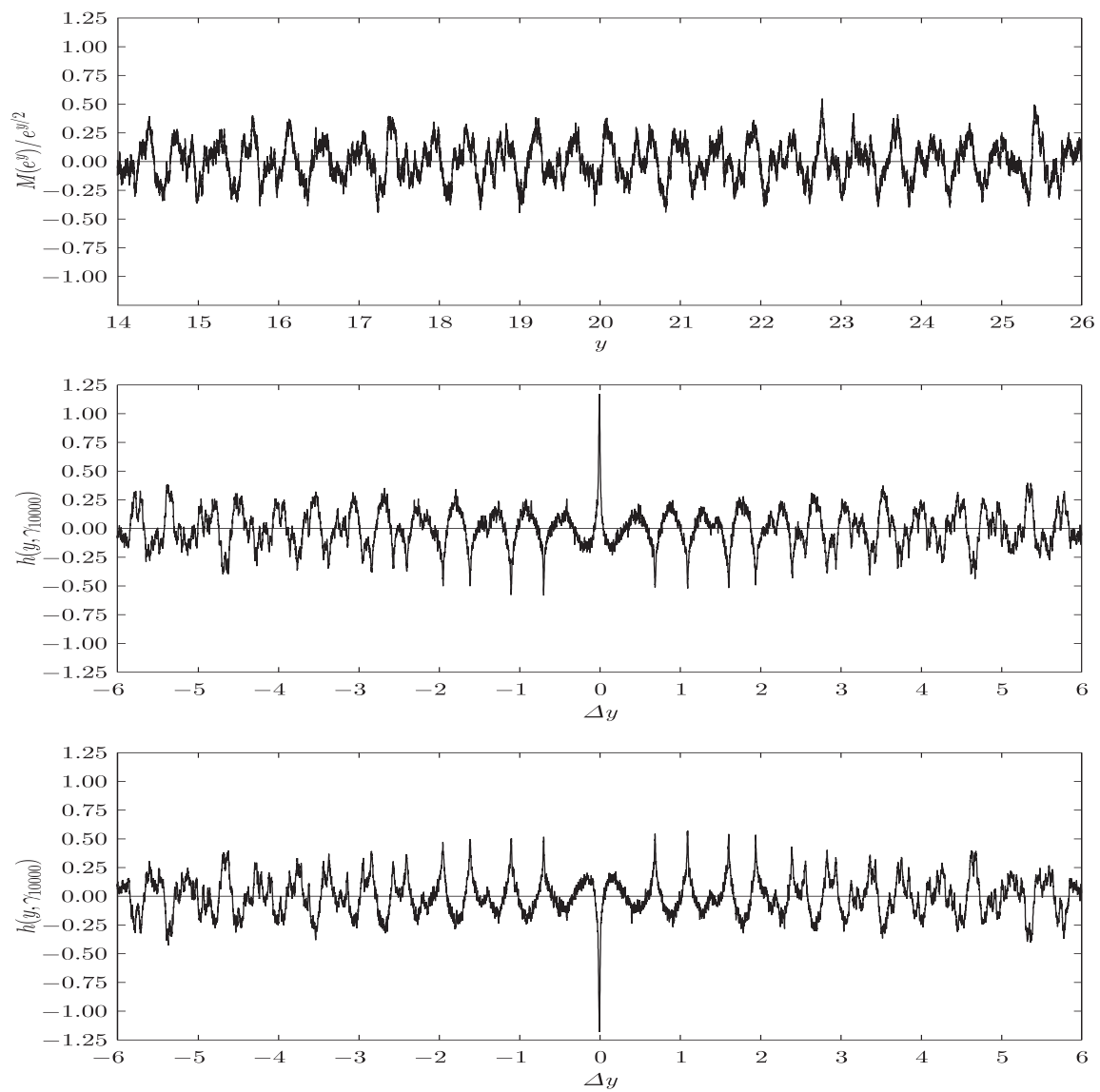


FIGURE 2

Literature

A.K. Lenstra, H.W. Lenstra, L. Lovasz, Factoring polynomials with rational coefficients, *Math. Ann.*, **261**, pp. 513–534, 1982.

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

J. Pintz, An effective disproof of the Mertens conjecture, *Astérisque*, **147–148**, pp. 325–333, 1987.

Conclusions

- Many problems and conjectures in number theory can profit from the availability of fast and large computers, e.g., the evidence for the truth of the Riemann hypothesis has been enlarged considerably with help of fast computers since Riemann formulated his hypothesis.
- Fast computers have helped to validate the strength of number-theory based cryptosystems like RSA considerably.
- Fast computers have helped to prove results like the three-primes theorem by covering a large interval of numbers for which the theorem could not be proved by theoretical means.
- Fast computers have very much helped to increase our knowledge about special numbers like perfect and amicable numbers.