Centrum voor Wiskunde en Informatica

REPORT*RAPPORT*

# Computational sieving applied to some classical number-theoretic problems

H.J.J. te Riele

Modelling, Analysis and Simulation (MAS)

**MAS-R9821 October 1998**

Report MAS-R9821
ISSN 1386-3703

CWI
P.O. Box 94079
1090 GB Amsterdam
The Netherlands

# Computational Sieving Applied to some Classical Number-Theoretic Problems

Herman te Riele
*CWI, P.O. Box 94079, 1090 GB Amsterdam, The Netherlands*
*Herman.te.Riele@cwi.nl*

ABSTRACT

Many problems in computational number theory require the application of some sieve. Efficient implementation of these sieves on modern computers has extended our knowledge of these problems considerably. This is illustrated by three classical problems: the Goldbach conjecture, factoring large numbers, and computing the summatory function of the Möbius function.

*1991 Mathematics Subject Classification:* Primary 11N35. Secondary 11P32, 11Y05, 11Y70.
*1991 Computing Reviews Classification System:* F.2.1.
*Keywords and Phrases:* Sieving, Goldbach conjecture, factoring large numbers, Möbius function.
*Note:* To appear in the Proceedings of the International Number Theory Conference held in Zakopane-Kościelisko, Poland, June 30 – July 9, 1997.
Work carried out under project MAS2.5 "Computational number theory and data security".

## 1. Introduction

In many problems in number theory like in prime counting, sieving plays a crucial role. Modern computers have made it possible to implement sieving in a very efficient way with the help of bit and vector operations, enabling us to extend the boundaries of our knowledge of these problems substantially. After discussing the arch-sieve of Eratosthenes and generalizations, we shall illustrate the progress in the past two decades with the following examples: the binary Goldbach conjecture which states that every even number $\geq 6$ can be expressed as a sum of two odd primes and the ternary Goldbach conjecture which states that every odd number $\geq 9$ can be expressed as a sum of three primes; factoring large numbers with modern sieve methods; computing the summatory function of the Möbius function.

## 2. The sieve of Eratosthenes and its generalizations

The best known sieve is the sieve of Eratosthenes (3rd century B.C.). It may be used to generate a table of prime numbers (and count them) up to some given bound B as follows. From the integers in the interval $[2, B]$ all the multiples of 2 are marked; next, all the multiples of the smallest *unmarked* number are marked, and this is repeated until all the multiples of the primes $\leq \sqrt{B}$ have been marked. The numbers left unmarked are the primes $\leq B$.

By repeating the application of this sieve to the numbers in the interval $[B, B^2]$ we may find all the primes in that interval. One may also use this sieve to generate the primes in a given interval $[C, D]$ by sieving with all the primes $\leq \sqrt{D}$; this requires a small amount of additional work, viz. to find the smallest multiple of a sieving prime in $[C, D]$.

To illustrate this sieve, we generate the primes in $[100, 140]$. We start by writing down the odd numbers in that interval (so the sieving with 2 has been done already) and we mark multiples of 3, 5, 7, and 11 to get:

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| multiples of 3 : | 101 | 103 | $\underline{105}$ | 107 | 109 | $\underline{111}$ | 113 | 115 | $\underline{117}$ | 119 |
| | 121 | $\underline{123}$ | 125 | 127 | $\underline{129}$ | 131 | 133 | $\underline{135}$ | 137 | 139 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| multiples of 5 : | 101 | 103 | $\underline{\underline{105}}$ | 107 | 109 | $\underline{111}$ | 113 | $\underline{\underline{115}}$ | $\underline{117}$ | 119 |
| | 121 | $\underline{123}$ | $\underline{\underline{125}}$ | 127 | $\underline{129}$ | 131 | 133 | $\underline{\underline{135}}$ | 137 | 139 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| multiples of 7 : | 101 | 103 | $\underline{\underline{\underline{105}}}$ | 107 | 109 | $\underline{111}$ | 113 | $\underline{\underline{115}}$ | $\underline{117}$ | $\underline{119}$ |
| | 121 | $\underline{123}$ | $\underline{\underline{125}}$ | 127 | $\underline{129}$ | 131 | $\underline{133}$ | $\underline{\underline{135}}$ | 137 | 139 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| multiples of 11 : | 101 | 103 | $\underline{\underline{\underline{105}}}$ | 107 | 109 | $\underline{111}$ | 113 | $\underline{\underline{115}}$ | $\underline{117}$ | $\underline{119}$ |
| | $\underline{121}$ | $\underline{123}$ | $\underline{\underline{125}}$ | 127 | $\underline{129}$ | 131 | $\underline{133}$ | $\underline{\underline{135}}$ | 137 | 139 |

The remaining, unmarked, numbers are prime because $139 < 13^2$. We notice that after the marking of multiples of some prime, these numbers *remain* in the list. If instead one would *drop* these numbers, we obtain *lucky numbers* [24, sequence # M2616], [11]; their density is higher than the density of the primes.

The sieve of Eratosthenes allows one to compute the *number* of primes $\leq x$, denoted by $\pi(x)$. According to the Prime Number Theorem, we have $\pi(x) \sim x/\log x$, so with a sieve like that of Eratosthenes we cannot compute $\pi(x)$ with less than about $x/\log x$ operations. Various authors, starting with the astronomer Meissel in the 19th century, have studied faster methods. The best practical results have been obtained by Deléglise and Rivat [5], [6] who have computed various values of $\pi(x)$ for $x$ up to $10^{20}$ with an algorithm which has time complexity $\mathcal{O}(x^{2/3}/\log^2 x)$ and space complexity $\mathcal{O}(x^{1/3}\log^3 x)$.

An essential feature of the sieve of Eratosthenes is that it is concerned with counting the number of elements in a set that do *not* possess certain prescribed properties. This has been generalized in various directions: we mention here the books by Halberstam and Richert [12] and by Hooley [13] which treat numerous sieves which have the objective to *estimate* the number of unsifted elements in a set after the elements satisfying certain properties have been striked out.

One particular generalization is known as the Generalized Sieving Problem (GSP) [16]: suppose we are given

1. an interval $[C, D]$;
2. $k$ moduli $m_1, m_2, \ldots, m_k$, all $> 1$, relatively prime in pairs;
3. $k$ sets $\mathcal{R}_i = \{r_{ij} \mid 0 \leq r_{ij} < m_i\}$ $\quad(i = 1, \ldots, k)$ of *acceptable residues.*

The question now is to determine all the integers $x \in [C, D]$ such that

$$x \pmod{m_i} \in \mathcal{R}_i \ \text{ for } \ i = 1, \ldots, k.$$

Let $m_i = p_i$, the $i$-th prime number. The instance $C = 1$, $D = p_{k+1}^2$ for some positive integer $k$, and $\mathcal{R}_i = \{1, 2, \ldots, p_i - 1\}$ $(i = 1, \ldots, k)$, is the problem to find all the primes $< p_{k+1}^2$.

Another example of a GSP is the following. Let $f_A(x)$ denote the quadratic polynomial $x^2 + x + A$ ($x \in \mathbb{N} \cup \{0\}, A \in \mathbb{Z}$). Euler discovered that $f_{41}(x)$ is prime for forty *consecutive* values of $x$, namely, for $x = 0, 1, \ldots, 39$. Let $P_A(n)$ denote the number of prime values assumed by $f_A(x)$ for $0 \leq x \leq n$, so we have $P_{41}(39) = 40$.[1] Another example is $f_{27941}(x)$, discovered by N.G.W.H. Beeger in 1938 [2]: we have $P_{27941}(39) = 30$, and $P_{27941}(1000000) = 286128$, whereas $P_{41}(1000000) = 261080$, so it seems that $P_{27941}(x)$ assumes more prime values than $P_{41}(x)$, albeit not for small $x$. The problem to find values of $A$ such that the density of prime values taken by $f_A(x)$ is high, can be formulated as a GSP. In order to find the polynomial $f_{27941}(x)$ Beeger computed all the positive integers $N < 10^6$ of the form $8t + 3$ such that the Legendre symbol $(-N/q) = -1$ for all odd primes $q \leq 43$. A simple example is the problem of finding the least positive $X < 8 \cdot 3 \cdot 5 \cdot 7 = 840$ such that

$$\begin{array}{lcl} X & \equiv & 3 \pmod{8}, \\ X & \equiv & 1 \pmod{3}, \\ X & \equiv & 2 \text{ or } 3 \pmod{5}, \\ X & \equiv & 1,\ 2,\ \text{or } 4 \pmod{7}. \end{array}$$

The solution is $X = 43$.

## 3. The Goldbach conjecture

### *3.1 The binary Goldbach conjecture*

The usual way to verify the binary Goldbach conjecture on a given interval $[A, B]$ is to mark those even $n \in [A, B]$ for which $n - p_i$ is prime, for $i = 2, 3, \ldots,$ until all even $n \in [A, B]$ have been marked. This requires the availability of the primes in $[A, B]$ and a few small odd primes. As an example, we take $[A, B] = [100, 138]$. Let

$$\mathcal{P} = \{3, 5, 7, 11, 13, 17, 19\}$$

and let

$$\mathcal{Q} = \{89, 97, 101, 103, 107, 109, 113, 127, 131, 137\}$$

be the set of primes on the interval $[100, 138]$ (and a few more). We start with writing down the even numbers in $[100, 138]$ and mark (by underlining) those belonging to the set $3 + \mathcal{Q}$:

$$\begin{array}{cccccccccc} \underline{100} & 102 & \underline{104} & \underline{106} & 108 & \underline{110} & \underline{112} & 114 & \underline{116} & 118 \\ 120 & 122 & 124 & 126 & 128 & \underline{130} & 132 & \underline{134} & 136 & 138 \end{array}$$

Next, we mark those in $5 + \mathcal{Q}$ to get:

$$\begin{array}{cccccccccc} \underline{100} & \underline{102} & \underline{104} & \underline{\underline{106}} & \underline{108} & \underline{110} & \underline{\underline{112}} & \underline{114} & \underline{116} & \underline{118} \\ 120 & 122 & 124 & 126 & 128 & \underline{130} & \underline{132} & \underline{134} & \underline{136} & 138 \end{array}$$

After marking, subsequently, the numbers which belong to $7 + \mathcal{Q}$, $11 + \mathcal{Q}$, $13 + \mathcal{Q}$, we obtain:

$$\begin{array}{cccccccccc} \underline{\underline{100}} & \underline{\underline{102}} & \underline{\underline{104}} & \underline{\underline{106}} & \underline{\underline{\underline{108}}} & \underline{\underline{\underline{110}}} & \underline{\underline{\underline{112}}} & \underline{\underline{\underline{\underline{114}}}} & \underline{\underline{\underline{116}}} & \underline{\underline{118}} \\ \underline{\underline{\underline{120}}} & \underline{122} & \underline{\underline{124}} & \underline{126} & 128 & \underline{130} & \underline{132} & \underline{\underline{134}} & \underline{136} & \underline{\underline{138}} \end{array}$$

[1] It is known that $P_A(A - 2) = A - 1$ can only happen for $A = 2, 3, 5, 11, 17, 41$.

Finally, 128 is marked since it belongs to $19 + \mathcal{Q}$.[2]

Notice that we have been building up the sum $\mathcal{P} + \mathcal{Q}$ to cover the even numbers in $[A, B]$. The set $\mathcal{P}$ contains a few small odd primes and the set $\mathcal{Q}$ contains the primes in $[A, B]$ (and a few more). An alternative approach is to choose for $\mathcal{P}$ the set of odd primes $\leq B - A$ and for $\mathcal{Q}$ a small set of large primes $< A$.

So, for $[A, B] = [100, 138]$ we start with the set $\mathcal{P}$ of odd primes $< 38$ (and a few more):

$$\mathcal{P} = \{3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59\}$$

and

$$\mathcal{Q} = \{79, 83, 89, 97\}.$$

We start again with writing down the even numbers in $[100, 138]$ but we now mark those belonging to the set $\mathcal{P} + 97$ to get:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| $\underline{100}$ | $\underline{102}$ | $\underline{104}$ | 106 | $\underline{108}$ | $\underline{110}$ | 112 | $\underline{114}$ | $\underline{116}$ | 118 |
| $\underline{120}$ | 122 | 124 | $\underline{126}$ | $\underline{128}$ | 130 | 132 | $\underline{134}$ | 136 | $\underline{138}$ |

Doing the same for the sets $\mathcal{P} + 89$ and $\mathcal{P} + 83$ we obtain:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| $\underline{\underline{\underline{100}}}$ | $\underline{\underline{\underline{102}}}$ | $\underline{104}$ | $\underline{\underline{106}}$ | $\underline{\underline{108}}$ | $\underline{110}$ | $\underline{\underline{112}}$ | $\underline{\underline{114}}$ | $\underline{116}$ | $\underline{118}$ |
| $\underline{\underline{\underline{120}}}$ | 122 | $\underline{124}$ | $\underline{\underline{\underline{126}}}$ | $\underline{128}$ | $\underline{\underline{130}}$ | $\underline{132}$ | $\underline{134}$ | $\underline{\underline{136}}$ | $\underline{138}$ |

Finally, 122 is marked since it lies in the set $\mathcal{P} + 79$.

The advantage of the second approach is that we have to generate the set of odd primes $\mathcal{P}$ below some given bound $B - A$ *once*; in addition, for each interval $[A, B]$ we have to find some primes smaller than but close to $A$. If we keep the length of the intervals $[A, B]$ fixed, we make optimal use of the set $\mathcal{P}$. In the first approach, one essentially has to generate *all the primes in the intervals* $[A, B]$ which we want to treat, and this is much more expensive than the work required in the second approach.

With this idea of using a large set of "small" odd primes (namely the odd primes $< 10^9$), and a small set of large primes near each interval $[A, B]$ to be checked, Deshouillers, Saouter, and the present author have verified the binary Goldbach conjecture up to $10^{14}$, partly on a Cray C90, partly on a cluster of workstations [9]. This extends similar work by Sinisalo up to $4 \times 10^{11}$ [23]. In addition, in [9] the binary Goldbach conjecture has been verified on the intervals $[10^{5k}, 10^{5k} + 10^8]$, for $k = 3, 4, \ldots, 20$ and $[10^{10k}, 10^{10k} + 10^9]$, for $k = 20, 21, \ldots, 30$. For each interval several hundred large primes close to the power of ten at the beginning of that interval were generated. Primality of these numbers was proved rigorously with the help of codes of François Morain [17, 1] and of Bosma and Van der Hulst [3].

### *3.2 The ternary Goldbach conjecture*

The ternary Goldbach conjecture states that every odd number $\geq 9$ can be written as a sum of three primes. Recently, a proof of this conjecture was announced on the condition of the truth of the Generalized Riemann hypothesis [8]. In this proof use is made of the fact that the binary Goldbach conjecture is true for all even numbers $\leq 1.615 \times 10^{12}$, a result implied by [9].

[2] So $128 - p$ is composite for $p = 3, 5, 7, 11, 13, 17$, but prime for $p = 19$.

The (unconditional) truth of the ternary Goldbach conjecture up to $10^{20}$ was shown recently by Saouter [22], who, by using [23], constructed a sequence of about $2.5 \times 10^8$ increasing prime numbers $q_i$, $0 \le i \le P$ such that $q_0 < 4 \times 10^{11}$, $q_{i+1} - q_i < 4 \times 10^{11}$ for all $0 \le i \le P-1$ and $q_P > 10^{20}$.

## 4. Factoring by sieving

The problem of finding the prime factors of a given integer $N$ is old and well-known and many different factoring algorithms are known to day. The best algorithms for general numbers are based on finding integers $a$ and $b$ such that $a^2 \equiv b^2 \bmod N$, and ideas in this direction go back to Fermat, Legendre, Gauss and many others [10]. The *quadratic sieve* [19] and the *number field sieve* [14] are the modern versions of such algorithms, and they have been used to factor the largest general numbers up to 130 decimal digits [4]. In these methods many $B$-*smooth* numbers have to be found, i.e., numbers whose prime factors are all $\le B$. These $B$-smooth numbers are searched among numbers which are themselves *values of polynomials* and this makes it possible to use sieve methods for this purpose. We shall illustrate this with a simple example.

We want to factor $N$. Choose (e.g.) the quadratic polynomial

$$f(x) = (x + \lfloor N^{1/2} \rfloor)^2 - N, \quad x = 0, \pm 1, \pm 2, \dots$$ [3]

Find $f(x)$–values that factor into primes less than some given bound $B$. If $f(x_i)$, $i = 1, 2, \dots$ are such values, we have

$$(x_i + \lfloor N^{1/2} \rfloor)^2 \equiv f(x_i) \bmod N$$

and we try to find a subset of the $x_i$'s such that the product of the corresponding $f(x_i)$–values is a *square*. If we succeed, we have found a congruence of the form $a^2 \equiv b^2 \bmod N$. We could try to find $B$-smooth $f(x)$–values by trial and error, but we can do much better by using the fact that any polynomial $p(x)$ enjoys the property that

$$p(c) \equiv 0 \bmod d \implies p(c + kd) \equiv 0 \bmod d \text{ for any } k \in \mathbb{Z}.$$

For $N = 1633$, $f(x) = (x + 40)^2 - 1633$, a small table of $f(x)$–values for $x$ near zero looks as follows:

| $x$ | $f(x)$ | |
|---|---|---|
| $-3$ | $-264 =$ | $-2^3 3 \cdot 11$ |
| $-2$ | $-189 =$ | $-3^3 \cdot 7$ |
| $-1$ | $-112 =$ | $-2^4 7$ |
| $0$ | $-33 =$ | $-3 \cdot 11$ |
| $1$ | $48 =$ | $2^4 3$ |
| $2$ | $131 =$ | prime |
| $3$ | $216 =$ | $2^3 3^3$ |

We may find small prime divisors by *sieving* with the primes $\le 11$, (i.e., taking $B = 11$) using:

$$\begin{array}{lcl} f(x) \equiv 0 \bmod 2 & \to & x \equiv 1 \bmod 2 \\ f(x) \equiv 0 \bmod 3 & \to & x \equiv 0,\ 1 \bmod 3 \\ f(x) \equiv 0 \bmod 5 & & \text{impossible} \\ f(x) \equiv 0 \bmod 7 & \to & x \equiv -1,\ -2 \bmod 7 \\ f(x) \equiv 0 \bmod 11 & \to & x \equiv -3,\ 0 \bmod 11. \end{array}$$

[3] By $\lfloor x \rfloor$ we denote the largest integer $\le x$.

In general, $f(x) \equiv 0 \bmod p$ implies that

$$(x + \lfloor N^{1/2} \rfloor)^2 \equiv N \bmod p$$

and this is solvable if $N$ is a quadratic residue of $p$ i.e., if the Legendre symbol $(N/p) = 1$ (see, e.g., [21, Appendix 3]).

To complete the algorithm for the above example, multiplying the above congruence relations corresponding to $x = -2, -1, 1$, namely, $38^2 \equiv -3^3 \cdot 7$, $39^2 \equiv -2^4 7$, and $41^2 \equiv 2^4 3$, gives $(38 \cdot 39 \cdot 41)^2 \equiv (2^4 3^2 7)^2 \bmod 1633$, $341^2 \equiv 1008^2 \bmod 1633$, 1633 divides $341^2 - 1008^2$, $\gcd(341 + 1008, 1633) = 71$, and $1633 = 23 \cdot 71$.

## 5. Computing arithmetic functions by sieving

Another example where computational sieving plays a role is found in the problem of computing the values of an arithmetic function $f(n)$ for all $n$ in a given interval $[A, B]$, where $f(n)$is a function of the prime factors of $n$. In addition, one may be interested in the behaviour of the summatory function $\sum_{1 \le n \le x} f(n)$.

We will illustrate this with $f(n) = \mu(n)$, the Möbius function, defined by

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

The function $M(x) = \sum_{1 \le n \le x} \mu(n)$ plays an important role in analytic number theory. The boundedness of $M(x)/\sqrt{x}$ implies the truth of the Riemann hypothesis. Since Mertens, who conjectured that $M(x)/\sqrt{x} < 1$, it has long been believed [20] that indeed $M(x)/\sqrt{x}$ is bounded, but nowadays one generally believes that this function is *unbounded*. This was supported by the disproof of Mertens' conjecture [18].

Lioen and Van de Lune [15] have found an efficient vectorized sieving algorithm for computing $\mu(n)$ for $n = 1, \ldots, N$:

**for** $n = 1$ **to** $N$: $\mu(n) = 1$
**for all** $p \le \sqrt{N}$: (**for all** $n$, $p|n$: $\mu(n) = -p \cdot \mu(n)$)
**for all** $p \le \sqrt{N}$: (**for all** $n$, $p^2|n$: $\mu(n) = 0$)
**for** $n = 1$ **to** $N$: (**if** $|\mu(n)| \ne n$ **then** $\mu(n) = -\mu(n)$)
**for** $n = 1$ **to** $N$: $\mu(n) = \mathrm{sign}(\mu(n))$

In Table 1 we illustrate this for $N = 30$. The algorithm fills an array corresponding to $\mu(n)$ for $n = 1, \ldots, 30$. The first column gives the indices (1–30). The algorithm starts by initializing the array with 1 (column headed 1); next, every *second* element of this array is multiplied by $-2$ (column headed 2), every *third* element by $-3$ (column headed 3), and every fifth element by $-5$ (column headed 4). In the next three steps array elements with index divisible by the *square* of the primes 2, 3, and 5, respectively, are made zero (columns headed 5–7). In step 8, an adjustment is made for array elements with index divisible by a prime $\ge 7$. In step 9, each entry in the table is replaced by its sign-function, so the last column lists $\mu(n)$ for $n = 1, \ldots, 30$.

Lioen and Van de Lune [15, 25] have applied this algorithm to compute $M(x)$ *for all* $x \le 1.7889 \times 10^{13}$ on a Cray C90 vector computer, establishing the bounds

$$-0.513 < \frac{M(x)}{\sqrt{x}} < 0.571.$$

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | | | | | | | | +1 |
| 2 | 1 | −2 | | | | | | | −1 |
| 3 | 1 | | −3 | | | | | | −1 |
| 4 | 1 | −2 | | | 0 | | | | 0 |
| 5 | 1 | | | −5 | | | | | −1 |
| 6 | 1 | −2 | +6 | | | | | | +1 |
| 7 | 1 | | | | | | | −1 | −1 |
| 8 | 1 | −2 | | | 0 | | | | 0 |
| 9 | 1 | | −3 | | | 0 | | | 0 |
| 10 | 1 | −2 | | +10 | | | | | +1 |
| 11 | 1 | | | | | | | −1 | −1 |
| 12 | 1 | −2 | +6 | | 0 | | | | 0 |
| 13 | 1 | | | | | | | −1 | −1 |
| 14 | 1 | −2 | | | | | | +2 | +1 |
| 15 | 1 | | −3 | +15 | | | | | +1 |
| 16 | 1 | −2 | | | 0 | | | | 0 |
| 17 | 1 | | | | | | | −1 | −1 |
| 18 | 1 | −2 | +6 | | | 0 | | | 0 |
| 19 | 1 | | | | | | | −1 | −1 |
| 20 | 1 | −2 | | +10 | 0 | | | | 0 |
| 21 | 1 | | −3 | | | | | +3 | +1 |
| 22 | 1 | −2 | | | | | | +2 | +1 |
| 23 | 1 | | | | | | | −1 | −1 |
| 24 | 1 | −2 | +6 | | 0 | | | | 0 |
| 25 | 1 | | | −5 | | | 0 | | 0 |
| 26 | 1 | −2 | | | | | | +2 | +1 |
| 27 | 1 | | −3 | | | 0 | | | 0 |
| 28 | 1 | −2 | | | 0 | | | | 0 |
| 29 | 1 | | | | | | | −1 | −1 |
| 30 | 1 | −2 | +6 | −30 | | | | | −1 |

Table 1: *Vectorized computing of* $\mu(n)$ *for* $n = 1, \ldots, 30$

The time complexity of this algorithm is $\mathcal{O}(x \log\log x)$ and the space complexity is $\mathcal{O}(x)$. Deléglise and Rivat [7] have given an algorithm to compute *isolated* values of $M(x)$ in time complexity $\mathcal{O}(x^{2/3}(\log\log x)^{1/3})$ and space complexity $\mathcal{O}(x^{1/3}(\log\log x)^{2/3})$. They list values of $M(a \times 10^b)$ for $a = 1(1)9$ and $b = 10(1)15$ and they give $M(10^{16}) = -3195437$. The corresponding $M(x)/\sqrt{x}$–bounds do not exceed those found by Lioen and Van de Lune.

# References


1. A.O.L. Atkin and F. Morain. Elliptic curves and primality proving. *Mathematics of Computation*, 61:29–68, 1993. *MR* **93m**:11136, *Zbl* **792**.11056.
2. N.G.W.H. Beeger. Report on some calculations of prime numbers. *Nieuw Archief voor Wiskunde*, 20(2):48–50, 1939. *MR* **1** 65g.
3. Wieb Bosma and Marc-Paul van der Hulst. *Primality proving with cyclotomy*. PhD thesis, University of Amsterdam, December 1990.
4. James Cowie, Bruce Dodson, R.-Marije Elkenbracht-Huizing, Arjen K. Lenstra, Peter L. Montgomery, and Jörg Zayer. A world wide number field sieve factoring record: on to 512 bits. In Kwangjo Kim and Tsutomu Matsumoto, editors, *Advances in Cryptology – Asiacrypt '96*, volume 1163 of *Lecture Notes in Computer Science*, pages 382–394, Berlin, etc., 1996. Springer–Verlag.
5. M. Deléglise and J. Rivat. Computing $\pi(x)$: the Meissel, Lehmer, Lagarias, Miller, Odlyzko method. *Mathematics of Computation*, 65(213):235–245, 1996. *MR* **96d**:11139, *Zbl* **960**.26198.
6. Marc Deléglise. Some new values of $\pi(x)$. Submitted for publication.
7. Marc Deléglise and Joël Rivat. Computing the summation of the Möbius function. *Experimental Mathematics*, 5(4):291–295, 1996.
8. J.-M. Deshouillers, G. Effinger, H. te Riele, and D. Zinoviev. A complete Vinogradov 3-primes theorem under the Riemann hypothesis. *Electronic Research Announcements of the AMS*, 3:99–104, September 17, 1997. URL: `http://www.ams.org/journals/era/home-1997.html` .
9. J.-M. Deshouillers, H.J.J. te Riele, and Y. Saouter. New experimental results concerning the Goldbach conjecture. In J.P. Buhler, editor, *Algorithmic Number Theory (Third International Symposium, ANTS-III, Portland, Oregon, USA, June 1998)*, volume 1423 of *Lecture Notes in Computer Science*, pages 204–215, Berlin etc., 1998. Springer. A preliminary version of this paper has appeared as CWI–Report MAS-R9804, March 1998, available as postscript file from `ftp://ftp.cwi.nl/pub/CWIreports/MAS/MAS-R9804.ps.Z` .

10. R.-M. Elkenbracht-Huizing. Historical background of the number field sieve. *Nieuw Archief voor Wiskunde*, 14(3):375–389, 1996. *Zbl* **970**.31229.

11. Vera Gardiner and R. Lazarus. On certain sequences of integers defined by sieves. *Math. Mag.*, 29:117–122, 1955.

12. H. Halberstam and H.-E. Richert. *Sieve Methods*. Academic Press, 1974. *MR* **54** #12689, *Zbl* **298**.10026.

13. C. Hooley. *Applications of sieve methods to the theory of numbers*. Cambridge University Press, 1976. *MR* **53** #7976.

14. 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. *MR* **96m**:11116, *Zbl* **777**.00017.

15. Walter M. Lioen and Jan van de Lune. Systematic computations on Mertens' conjecture and Dirichlet's divisor problem by vectorized sieving. In Krzysztof Apt, Lex Schrijver, and Nico Temme, editors, *From universal morphisms to megabytes: a Baayen space Odyssey*, pages 421–432. CWI, Amsterdam, 1994. *Zbl* **846**.11068.

16. R.F. Lukes, C.D. Patterson, and H.C. Williams. Numerical Sieving Devices: Their History and Some Applications. *Nieuw Archief voor Wiskunde, Series IV*, 13(1):113–139, 1995. *MR* **96m**:11082, *Zbl* **856**.11048.

17. François Morain. *Courbes Elliptiques et Tests de Primalité*. PhD thesis, L'Université Claude Bernard, Lyon I, September 1990. Introduction in French, body in English.

18. A.M. Odlyzko and H.J.J. te Riele. Disproof of the Mertens conjecture. *J. reine angew. Math.*, 357:138–160, 1985. *MR* **86m**:11070, *Zbl* **544**.10047.

19. Carl Pomerance. Analysis and comparison of some integer factoring algorithms. In H.W. Lenstra, Jr. and R. Tijdeman, editors, *Computational Methods in Number Theory, Part I*, pages 89–139. Mathematisch Centrum, Amsterdam, 1982. Math. Centrum Tract 154, *MR* **84i**:10005.

20. Herman J.J. te Riele. On the history of the function $M(x)/\sqrt{x}$ since Stieltjes. In Gerrit van Dijk, editor, *Thomas Jan Stieltjes Œuvres Complètes—Collected Papers (two volumes)*, pages 69–79 in Volume I. Springer-Verlag, 1993. *MR* **95g**:01033.

21. Hans Riesel. *Prime numbers and computer methods for factorization*. Birkhäuser, Boston, etc., second edition, 1994. *MR* **95h**:11142, *Zbl* **821**.11001.

22. Yannick Saouter. Checking the odd Goldbach conjecture up to $10^{20}$. *MathComp*, 67(222):863–866, 1998.

23. Matti K. Sinisalo. Checking the Goldbach conjecture up to $4 \times 10^{11}$. *Mathematics of Computation*, 61:931–934, 1993. *MR* **94a**:11157, *Zbl* **783**.11037.

24. N.J.A. Sloane and Simon Plouffe. *The Encyclopedia of Integer Sequences*. Academic Press, 1995. *MR* **96a**:11001, *Zbl* **845**.11001.

25. H.J.J. te Riele and J. van de Lune. Computational Number Theory at CWI in 1970–1994. *CWI Quarterly*, 7(4):285–335, 1994. *MR* **96g**:11147.