AN INTRODUCTION TO FAST GENERATION OF LARGE PRIME NUMBERS

by C. COUVREUR and J. J. QUISQUATER

Abstract
In this paper we present in the form of a survey a detailed analysis of prime distribution, sieving methods, compositeness and some primality tests. This study is aimed at adapting recent methods for generating large random primes such as needed in public-key cryptosystems. An algorithm has been implemented. It will be presented in a subsequent paper.

1. Introduction
The use of large prime numbers has revealed to be very important in modern cryptography. This has motivated an increasing interest in the subject of prime number generation. As an illustration let us briefly describe the public-key cryptosystem proposed by Rivest, Shamir and Adleman (usually referred to as the RSA or M.I.T. cryptosystem\(^1\)). An encryption key consists of a pair of positive integers \((e, n)\). The message \(M\), which is an integer between 0 and \(n - 1\), is encrypted into

\[ C = M^e \pmod{n}. \]

Thus the cryptogram \(C\) is the remainder in the division of the \(e\)th power of \(M\) by \(n\). Similarly, a decryption key is a pair of positive integers \((d, n)\). The message \(M\) is obtained by decrypting \(C\) as follows

\[ M = C^d \pmod{n}. \]

The modulus \(n\) is the product of two large prime numbers, \(p\) and \(q\). The integers \(e\) and \(d\) are multiplicative inverses modulo the least common multiple of \(p - 1\) and \(q - 1\), i.e.

\[ ed \equiv 1 \pmod{lcm(p - 1, q - 1)}. \]

The security of the RSA public-key cryptosystem is known to be crucially based on the difficulty of finding the factorization \(n = pq\) of the given modulus \(n\) (see Williams\(^2\); Williams and Schmid\(^3\) and Couvreur and Goethals\(^4\)). Some constraints must be put on \(p\) and \(q\) to create secure keys. In fact,
the process of devising suitable values for \( p \) and \( q \) requires first a method for finding large random primes between \( 10^{60} \) and \( 10^{100} \).

Many methods for verifying that a number is a prime have been proposed. Let us now review some of them:

- **Sieve** (Eratosthenes, circa 250 b.c.) and **trial division** (Leonardo Pisano Fibonacci, 1202). These are the first known methods. Their practical limit is for numbers with a maximum of 15 to 20 digits. But combined with other tests these techniques have proved to be very powerful (see sec. 5 of the present paper).

- **Factoring.** One can test a number for primality by attempting to factorize it. Good accounts of this method are given by Guy\(^5\), Knuth and Pardo\(^6,7\), Monier\(^8\) and Wunderlich\(^9\).

- **Wilson’s theorem** (published in 1770 by Waring). It characterizes the number \( n \) as being a prime if and only if the congruence \((n - 1)! \equiv -1 \pmod{n}\) holds (see Hardy and Wright\(^10\, p.68\)).

- **Recognition of primes by automata.** There exists an automaton recognizing the set of primes and having a memory which grows linearly with the input length (see Hartmanis and Shank\(^11\)).

- **Use of Pascal’s arithmetic triangle.** The number \( n \) is a prime if and only if all binomial coefficients \( \binom{n}{k} \) are divisible by \( k \) (see Mann and Shanks\(^12\) and Harborth\(^13\)).

- **Prime representing polynomials.** Certain multivariable polynomials have been explicitly determined with the following property. The set of primes is identical with the set of positive values assumed by a given polynomial as the variables range over the natural numbers (see Davis, Matijasevic and Robinson\(^14\)).

- **Succinct prime certification.** To show that a number \( n \) is composite, it suffices to write it as a product of two nontrivial factors. There also exist analogous certificates showing that a number \( n \) is prime. However no fast way is known to find them (see Pratt\(^15\)).

- **Exponentiation.** It is proven that there exists a certain number \( A \) greater than 1 but not an integer, such that \( A^x \) is prime for \( x = 1, 2, 3, \ldots \) Alas \( A \) is not known (see Mills\(^16\)).

- The set of all integers which can be written as the sum of at least three consecutive positive integers is the set of all positive integers which are neither prime nor a power of 2 (see de la Rosa\(^17\)).

However these methods, although interesting from a theoretical viewpoint, are not efficient for the practical problem of generating large prime numbers.

Four other basic methods for testing the primality of a number \( s \) have been developed and extensively studied. Table 1 summarizes their principal charac-
<table>
<thead>
<tr>
<th>Method of primality testing</th>
<th>gives a rigorous proof of primality</th>
<th>depends on factorization</th>
<th>ease of implementation</th>
<th>speed of execution</th>
<th>references</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. special functions</td>
<td>yes</td>
<td>yes</td>
<td>from easy to very difficult</td>
<td>from slow to very rapid</td>
<td>Lehmer $^{79,90}$&lt;br&gt;Brillhart and al. $^{22}$&lt;br&gt;Williams and al. $^{23,25}$&lt;br&gt;Morrison and al. $^{91,92}$&lt;br&gt;Adleman and Leighton $^{93}$</td>
</tr>
<tr>
<td>2. extension fields</td>
<td>yes</td>
<td>no</td>
<td>very difficult</td>
<td>rapid</td>
<td>Adleman and Rumely $^{94}$&lt;br&gt;Pomerance $^{95}$&lt;br&gt;Lenstra $^{96,97}$&lt;br&gt;Cohen $^{98}$</td>
</tr>
<tr>
<td>3. probabilistic (Monte-Carlo)</td>
<td>no</td>
<td>no</td>
<td>easy</td>
<td>very rapid</td>
<td>Miller $^{66,67}$&lt;br&gt;Rabin $^{68,69}$&lt;br&gt;Solovay and Strassen $^{70}$&lt;br&gt;Malm $^{99}$</td>
</tr>
<tr>
<td>4. based on the extended Riemann's hypothesis (E.R.H.)</td>
<td>unknown</td>
<td>no</td>
<td>easy</td>
<td>rapid?</td>
<td>Miller $^{66,67}$&lt;br&gt;Lenstra $^{100}$&lt;br&gt;Vélu $^{101}$&lt;br&gt;Mignotte $^{102}$&lt;br&gt;Pajunen $^{103}$</td>
</tr>
</tbody>
</table>
C. Couvreur and J. J. Quisquater

teristics (let us note that Williams\textsuperscript{18}) presents a detailed analysis of three of these methods).

The first method requires prior knowledge of the factorization of some special functions of \( s \), like for instance \( s - 1 \), \( s + 1 \) or \( s^2 + s + 1 \).

The second method is based on pseudoprime tests performed in various extensions of the rational numbers.

The probabilistic method is based on a simple algorithm (using \( k \) random integers out of \( \{1, 2, \ldots, s - 1\} \)) which declares that a number \( s \) is prime with a probability of error bounded from above by \( 2^{-k} \).

The fourth method provides certificates of primality if the Riemann hypothesis is true.

In fact the first and the second methods are the only ones to be considered when a rigorous proof of primality is required. For the first method, the problem of factoring the special function of \( s \) can be overcome by generating random factorizations instead of random numbers to be tested for primality. Williams and Schmid\textsuperscript{3}), Buhler, Crandall and Penk\textsuperscript{19,20}, and chiefly Plaisted\textsuperscript{21} propose such a method which appears to be quite general and, with some adaptations, suitable for our purposes. Thus we have adapted their method and extended their results.

The paper is organized as follows. First a large set \( S \) is constructed which consists of large odd integers \( s \), composed from known factorizations and which are candidates for primes. The construction of the set \( S \) is described in sec. 2. Then, after discussing the distribution of primes in sec. 3, we study the average distance between two primes of \( S \) in sec. 4, thus justifying the choice of our set \( S \). Secondly most of the composite numbers in \( S \) must be eliminated by sieving out the set \( S \): the sieving process on the set \( S \) is studied in sec. 5. Finally the remaining elements of \( S \) must be tested for compositeness or primality; compositeness tests are analysed in sec. 6, whereas primality tests are discussed in sec. 8.

The following notations are used throughout this paper. By \( s \) we denote an integer whose primality is tested. All logarithms written in the form \( \log x \) are taken with respect to the base 2. Natural logarithms are written \( \ln x \).

2. Construction of the set \( S \)

The basic idea consists in constructing a set \( S \) of large odd integers \( s \), all of which are generated using a fixed random number \( F \), partially or completely factored. The set \( S \) must be easy to describe and must contain enough prime numbers. Some constraints are placed on \( F \) to make the compositeness or primality tests easier.
An introduction to fast generation of large prime numbers

The methods we have considered for testing the primality of $s$ use known factors of $s - 1$, $s + 1$, $s^2 - 1$, $s^2 + 1$, $s^2 + s + 1$ or $s^2 - s + 1$ (see Brillhart, Lehmer and Selfridge$^{22}$; Williams and Judd$^{26,24}$) and Williams and Holte$^{25}$. Only the tests based on the knowledge of a complete or partial factorization of $s \pm 1$ (see Brillhart, Lehmer and Selfridge$^{22}$) seem to be interesting here, as we do not see how to construct a family of integers $s$ from a fixed random number $F$ which would be a factor of $s^2 + 1$, or $s^2 \pm s - 1$. We find it useful to retain only the tests relative to the factorization of $s - 1$. The tests relative to the factorization of $s + 1$ have been the subject of a similar work (see Baillie and Wagstaff$^{104}$).

In great generality, the set $S$ to be considered here can be defined as follows:

$$S = \{s = kF + 1 \mid k = 1, 2, 3, \ldots, K\}, \quad (1)$$

where $F$ is a random even large number. More constraints are imposed on $F$, depending on the compositeness or primality tests to be used in the method for generating large primes. These are discussed in the next sections. The bound $K$ is proportional to the number of primes we want to generate and is examined in the next sections too.

3. Distribution of primes

The central theorem concerning the distribution of primes (see Hardy and Wright$^{10,p.9}$) states that the number of primes not exceeding $x$, noted $\pi(x)$, is asymptotic to $x/\ln x$

$$\pi(x) \sim \frac{x}{\ln x},$$

that is

$$\lim_{x \to \infty} \frac{\pi(x) \ln x}{x} = 1.$$ 

Lower and upper bounds on $\pi(x)$ have been established (see Rosser and Schoenfeld$^{27}$), namely

$$\frac{x}{\ln x} \left(1 + \frac{1}{2 \ln x}\right) < \pi(x) < \frac{x}{\ln x} \left(1 + \frac{3}{2 \ln x}\right)$$

for $x \geq 59$, and

$$\frac{x}{\ln x - \frac{1}{2}} < \pi(x) < \frac{x}{\ln x - \frac{3}{2}}$$

for $x \geq 67$. It is interesting to compare the actual count of primes with the corresponding values in these formulas (see Hardy and Wright$^{10,p.9}$); Bohman$^{28,29}$ and Mapes$^{30}$): these appear in table 2.
TABLE 2
Actual and approximate counts of primes

<table>
<thead>
<tr>
<th>$x$</th>
<th>$\frac{x}{\ln x}$</th>
<th>$\frac{x}{\ln x \left(1 + \frac{1}{2 \ln x}\right)}$</th>
<th>$\frac{x}{\ln x - \frac{1}{2}}$</th>
<th>$\pi(x)$</th>
<th>$\frac{x}{\ln x \left(1 + \frac{3}{2 \ln x}\right)}$</th>
<th>$\frac{x}{\ln x + \frac{1}{2}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10^3$</td>
<td>145</td>
<td>155</td>
<td>156</td>
<td>168</td>
<td>176</td>
<td>185</td>
</tr>
<tr>
<td>$10^4$</td>
<td>1 086</td>
<td>1 145</td>
<td>1 148</td>
<td>1 229</td>
<td>1 263</td>
<td>1 297</td>
</tr>
<tr>
<td>$10^5$</td>
<td>8 686</td>
<td>9 063</td>
<td>9 080</td>
<td>9 592</td>
<td>9 818</td>
<td>9 987</td>
</tr>
<tr>
<td>$10^6$</td>
<td>72 382</td>
<td>75 002</td>
<td>75 100</td>
<td>78 498</td>
<td>80 241</td>
<td>81 198</td>
</tr>
<tr>
<td>$10^7$</td>
<td>620 421</td>
<td>639 667</td>
<td>640 283</td>
<td>664 579</td>
<td>678 159</td>
<td>684 084</td>
</tr>
<tr>
<td>$10^8$</td>
<td>5 428 681</td>
<td>5 576 034</td>
<td>5 580 145</td>
<td>5 761 455</td>
<td>5 870 740</td>
<td>5 909 928</td>
</tr>
<tr>
<td>$10^9$</td>
<td>48 254 942</td>
<td>49 419 212</td>
<td>49 447 998</td>
<td>50 847 478</td>
<td>51 747 752</td>
<td>52 020 297</td>
</tr>
<tr>
<td>$10^{10}$</td>
<td>434 294 482</td>
<td>443 725 067</td>
<td>443 934 394</td>
<td>455 052 511</td>
<td>462 586 237</td>
<td>464 557 709</td>
</tr>
<tr>
<td>$10^{11}$</td>
<td>3 948 131 654</td>
<td>4 026 070 371</td>
<td>4 027 639 917</td>
<td>4 118 054 813</td>
<td>4 181 947 807</td>
<td>4 196 666 533</td>
</tr>
<tr>
<td>$10^{12}$</td>
<td>36 191 206 825</td>
<td>36 846 108 551</td>
<td>36 858 177 793</td>
<td>37 607 912 018</td>
<td>38 155 912 002</td>
<td>38 268 692 049</td>
</tr>
</tbody>
</table>
An introduction to fast generation of large prime numbers

Other numerical expressions are known for estimating the number of primes not exceeding \( x \). They are of an outstanding accuracy but their actual computation is not so simple as compared with the previous ones. We briefly present here the results. First the **Riemann formula** (see Knuth\(^6\), p.366))

\[
\pi(x) \sim \mu(1) \text{Li}(x) + \frac{\mu(2)}{2} \text{Li}(x^2) + \frac{\mu(3)}{3} \text{Li}(x^3) + \ldots,
\]

where \( \text{Li}(x) \) is the *integral logarithm* and \( \mu(n) \) is the *Möbius function*. Lehmer\(^31\) has shown that Riemann's formula is equivalent to

\[
\pi(x) \sim 1 + \frac{\ln x}{\zeta(2)} + \frac{(\ln x)^2}{2 \cdot 2! \zeta(3)} + \frac{(\ln x)^3}{3 \cdot 3! \zeta(4)} + \ldots,
\]

where \( \zeta(n) \) is the *Riemann zeta function*. Secondly the **Chebyshev formula** which was earlier conjectured by Gauss,

\[
\pi(x) \sim \int_{2}^{x} \frac{dx}{\ln x}.
\]

In table 3 we compare the actual prime counts with those predicted by Riemann and Chebyshev (see Jones, Lal and Blundon\(^32\); Knuth\(^6\), p.366) and Shanks\(^33\)).

In fact our interest here is in the number of primes of the form \( ka + b \), where \( a \) and \( b \) are relatively prime. **Dirichlet's theorem** (see Hardy and Wright\(^10\), p.13)

**TABLE 3**

<table>
<thead>
<tr>
<th>( x )</th>
<th>( \pi(x) )</th>
<th>Riemann count</th>
<th>Chebyshev count</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 10^3 )</td>
<td>168</td>
<td>168.36</td>
<td>177.6</td>
</tr>
<tr>
<td>( 10^4 )</td>
<td>1 229</td>
<td></td>
<td>1 246.2</td>
</tr>
<tr>
<td>( 10^5 )</td>
<td>9 592</td>
<td></td>
<td>9 629.6</td>
</tr>
<tr>
<td>( 10^6 )</td>
<td>78 498</td>
<td>78 527.40</td>
<td>78 631.7</td>
</tr>
<tr>
<td>( 10^7 )</td>
<td>664 579</td>
<td>664 667</td>
<td>664 918</td>
</tr>
<tr>
<td>( 10^8 )</td>
<td>5 761 455</td>
<td>5 761 551.9</td>
<td>5 762 208.3</td>
</tr>
<tr>
<td>( 10^9 )</td>
<td>50 847 478</td>
<td>50 847 455.4</td>
<td>50 849 233.9</td>
</tr>
<tr>
<td>( 10^{10} )</td>
<td>455 052 511</td>
<td>455 050 683.3</td>
<td>455 055 613.5</td>
</tr>
<tr>
<td>( 10^{11} )</td>
<td>4 118 054 813</td>
<td>4 118 052 494.6</td>
<td>4 118 066 399.6</td>
</tr>
<tr>
<td>( 10^{12} )</td>
<td>37 607 912 018</td>
<td>37 607 910 542.2</td>
<td>37 607 950 279.8</td>
</tr>
<tr>
<td>( 10^{13} )</td>
<td>346 065 535 898</td>
<td>346 065 531 065.8</td>
<td>346 065 645 809.0</td>
</tr>
<tr>
<td>( 10^{14} )</td>
<td>3 204 941 731 601.7</td>
<td>3 204 942 065 690.9</td>
<td></td>
</tr>
<tr>
<td>( 10^{15} )</td>
<td>29 844 570 495 886.9</td>
<td>29 844 571 475 286.5</td>
<td></td>
</tr>
</tbody>
</table>
C. Couvreur and J. J. Quisquater

asserts that there are infinitely many primes of this form. Let \( \pi(x, a, b) \) denote the number of such primes which are less than or equal to \( x \). A well-known conjecture, due to Hardy and Littlewood\(^{34}\), asserts that

\[
\pi(x, a, b) \sim \frac{\pi(x)}{\phi(a)},
\]

(2)

where \( \phi \) is the \textit{Euler totient function} (this conjecture was proved by de la Vallée Poussin, for \( x \to \infty \), see Apostol\(^{35}\)). In table 4, we have indicated the results of a comparison between the actual value of \( \pi(x, a, b) \) and its corresponding approximation (see Bays and Hudson\(^{36-38}\)). As we can read from this table, \( \pi(x)/\phi(a) \) is a good approximation to \( \pi(x, a, b) \).

4. Average distance between two primes in the set \( S \)

Let us recall that the set \( S \) to be considered consists of numbers \( s \) of the form

\[
s = kF + 1 \quad k = 1, 2, 3, \ldots,
\]

(3)

where \( F \) is a random even number, partially or completely factored.

Let us assume that the density of primes remains constant throughout the set \( S \), and examine the validity of this assumption. A first approach to the question is made by considering primes of any form. Afterwards it is particularized to primes of the form (3).

We point out the experimental observation that prime numbers are randomly and uniformly distributed in a suitable length interval: indeed, as Gauss notices, if \( x \) is large while \( \Delta \) is comparatively small, the number of primes between \( x \) and \( x + \Delta \) is observed to be approximately given by

\[
\frac{\Delta}{\ln x}
\]

(see Rouse Ball and Coxeter\(^{39}\)). In table 5, we examine the accuracy of this approximation on the basis of several examples taken from Mapes\(^{30}\), Jones, Lal and Blundon\(^{32}\), Zagier\(^{40}\) and Knuth\(^{6}\). We observe that, provided \( \Delta \) is not too small, the approximation is generally excellent. We now examine what happens to the density of primes when a given interval is subdivided into subintervals. To that end we consider the nine successive subintervals of length \( 10^7 \) from the interval \( 10^7 \leq s \leq 10^8 \): since there are 5096876 primes in \( 10^7 \leq s \leq 10^8 \), each subinterval is expected to contain approximately 566320 primes. In table 6 we compare the actual number of primes in these subintervals with the expected value and we observe that the ratio between the two quantities varies between 0.96 and 1.07. We find it also of interest to deter-
<table>
<thead>
<tr>
<th>$x$</th>
<th>$a$</th>
<th>$b$</th>
<th>$\pi(x, a, b)$</th>
<th>$\phi(a)$</th>
<th>$\pi(x)$</th>
<th>$\frac{\pi(x)}{\phi(a)} \cdot \frac{1}{\pi(x, a, b)}$</th>
<th>gap between $\frac{\pi(x)}{\phi(a)}$ and $\pi(x, a, b)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10^{10}$</td>
<td>4</td>
<td>1</td>
<td>227 523 275</td>
<td>2</td>
<td>227 526 256</td>
<td>1.000 013 102</td>
<td>2.981</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td></td>
<td>227 529 235</td>
<td></td>
<td></td>
<td>0.999 986 907 2</td>
<td>-2.979</td>
</tr>
<tr>
<td>$10^{11}$</td>
<td>6</td>
<td>1</td>
<td>2 059 018 668</td>
<td>2</td>
<td>2 059 027 407</td>
<td>1.000 004 244</td>
<td>8.739</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td></td>
<td>2 059 036 143</td>
<td></td>
<td></td>
<td>0.999 995 757 2</td>
<td>-8.736</td>
</tr>
<tr>
<td>$10^{11}$</td>
<td>24</td>
<td>1</td>
<td>514 742 404</td>
<td>8</td>
<td>514 756 852</td>
<td>1.000 028 068</td>
<td>14.448</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td></td>
<td>514 760 074</td>
<td></td>
<td></td>
<td>0.999 993 740 8</td>
<td>-3.222</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td></td>
<td>514 762 733</td>
<td></td>
<td></td>
<td>0.999 988 575 3</td>
<td>-5.881</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td></td>
<td>514 755 092</td>
<td></td>
<td></td>
<td>1.000 003 419</td>
<td>1.760</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td></td>
<td>514 757 222</td>
<td></td>
<td></td>
<td>0.000 000 001 9</td>
<td>-370</td>
</tr>
<tr>
<td></td>
<td>17</td>
<td></td>
<td>514 760 580</td>
<td></td>
<td></td>
<td>0.999 992 757 8</td>
<td>-3.728</td>
</tr>
<tr>
<td></td>
<td>19</td>
<td></td>
<td>514 756 309</td>
<td></td>
<td></td>
<td>1.000 001 055</td>
<td>543</td>
</tr>
<tr>
<td></td>
<td>23</td>
<td></td>
<td>514 760 397</td>
<td></td>
<td></td>
<td>0.999 993 113 3</td>
<td>-3.545</td>
</tr>
<tr>
<td>$10^{12}$</td>
<td>3</td>
<td>1</td>
<td>18 803 933 520</td>
<td>2</td>
<td>18 803 956 010</td>
<td>1.000 001 196</td>
<td>22.490</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td></td>
<td>18 803 978 497</td>
<td></td>
<td></td>
<td>0.999 998 804 5</td>
<td>-22.487</td>
</tr>
<tr>
<td>$10^{12}$</td>
<td>24</td>
<td>1</td>
<td>4 700 968 265</td>
<td>8</td>
<td>4 700 989 001</td>
<td>1.000 004 411</td>
<td>20.736</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td></td>
<td>4 700 998 678</td>
<td></td>
<td></td>
<td>0.999 997 941 5</td>
<td>-9.677</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td></td>
<td>4 701 001 698</td>
<td></td>
<td></td>
<td>0.999 997 299 1</td>
<td>-12.697</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td></td>
<td>4 701 004 728</td>
<td></td>
<td></td>
<td>0.999 996 654 5</td>
<td>-15.727</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td></td>
<td>4 700 973 812</td>
<td></td>
<td></td>
<td>1.000 003 231</td>
<td>15.189</td>
</tr>
<tr>
<td></td>
<td>17</td>
<td></td>
<td>4 700 983 585</td>
<td></td>
<td></td>
<td>1.000 001 152</td>
<td>5.416</td>
</tr>
<tr>
<td></td>
<td>19</td>
<td></td>
<td>4 700 989 745</td>
<td></td>
<td></td>
<td>0.999 999 841 7</td>
<td>-7.44</td>
</tr>
<tr>
<td></td>
<td>23</td>
<td></td>
<td>4 700 991 505</td>
<td></td>
<td></td>
<td>0.999 999 467 3</td>
<td>-2.504</td>
</tr>
</tbody>
</table>
TABLE 5
Prime counts in given intervals

<table>
<thead>
<tr>
<th>interval $[x, x + \Delta]$</th>
<th>$\pi(x \leq s \leq x + \Delta)$</th>
<th>$\Delta \ln x$</th>
<th>$\pi(x \leq s \leq x + \Delta)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10^7 \leq s \leq 10^9$</td>
<td>50,182,955</td>
<td>61,421,648</td>
<td>0.8170</td>
</tr>
<tr>
<td>$10^8 \leq s \leq 10^9$</td>
<td>45,086,079</td>
<td>48,858,129</td>
<td>0.9228</td>
</tr>
<tr>
<td>$10^7 \leq s \leq 2 \times 10^7$</td>
<td>606,028</td>
<td>620,421</td>
<td>0.9768</td>
</tr>
<tr>
<td>$2 \times 10^7 \leq s \leq 3 \times 10^7$</td>
<td>587,252</td>
<td>594,840</td>
<td>0.9872</td>
</tr>
<tr>
<td>$3 \times 10^7 \leq s \leq 4 \times 10^7$</td>
<td>575,795</td>
<td>580,831</td>
<td>0.9913</td>
</tr>
<tr>
<td>$4 \times 10^7 \leq s \leq 5 \times 10^7$</td>
<td>567,480</td>
<td>571,285</td>
<td>0.9933</td>
</tr>
<tr>
<td>$5 \times 10^7 \leq s \leq 6 \times 10^7$</td>
<td>560,981</td>
<td>564,094</td>
<td>0.9945</td>
</tr>
<tr>
<td>$6 \times 10^7 \leq s \leq 7 \times 10^7$</td>
<td>555,949</td>
<td>558,352</td>
<td>0.9957</td>
</tr>
<tr>
<td>$7 \times 10^7 \leq s \leq 8 \times 10^7$</td>
<td>551,318</td>
<td>553,877</td>
<td>0.9959</td>
</tr>
<tr>
<td>$8 \times 10^7 \leq s \leq 9 \times 10^7$</td>
<td>547,572</td>
<td>549,525</td>
<td>0.9964</td>
</tr>
<tr>
<td>$9 \times 10^7 \leq s \leq 10^8$</td>
<td>544,501</td>
<td>545,991</td>
<td>0.9973</td>
</tr>
<tr>
<td>$10^8 \leq s \leq 10^8 + 150,000$</td>
<td>8,154</td>
<td>8,143</td>
<td>1.0013</td>
</tr>
<tr>
<td>$10^7 \leq s \leq 10^7 + 100$</td>
<td>2</td>
<td>6</td>
<td>0.3224</td>
</tr>
<tr>
<td>$2^{24} - 167 \leq s \leq 2^{24} - 3$</td>
<td>10</td>
<td>9.9</td>
<td>1.0144</td>
</tr>
<tr>
<td>$2^{26} - 183 \leq s \leq 2^{26} - 39$</td>
<td>10</td>
<td>8.3</td>
<td>1.2034</td>
</tr>
<tr>
<td>$2^{26} - 135 \leq s \leq 2^{26} - 5$</td>
<td>10</td>
<td>7.2</td>
<td>1.3863</td>
</tr>
<tr>
<td>$2^{27} - 235 \leq s \leq 2^{27} - 39$</td>
<td>10</td>
<td>10.5</td>
<td>0.9548</td>
</tr>
<tr>
<td>$2^{28} - 273 \leq s \leq 2^{28} - 57$</td>
<td>10</td>
<td>11.1</td>
<td>0.8985</td>
</tr>
<tr>
<td>$2^{29} - 133 \leq s \leq 2^{29} - 3$</td>
<td>10</td>
<td>6.5</td>
<td>1.5463</td>
</tr>
<tr>
<td>$10^8 \leq s \leq 10^8 - 11$</td>
<td>10</td>
<td>11.0</td>
<td>0.9119</td>
</tr>
<tr>
<td>$10^8 \leq s \leq 10^8 - 63$</td>
<td>10</td>
<td>9.8</td>
<td>1.0158</td>
</tr>
</tbody>
</table>

TABLE 6
Variation of density of primes

<table>
<thead>
<tr>
<th>intervals</th>
<th>actual number of primes</th>
<th>expected number of primes</th>
<th>ratio between the actual number of primes and the expected one</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10^7 \leq s \leq 10^8$</td>
<td>5,096,876</td>
<td>566,320</td>
<td>1.0701</td>
</tr>
<tr>
<td>$10^7 \leq s \leq 2 \times 10^7$</td>
<td>606,028</td>
<td>566,320</td>
<td>1.0370</td>
</tr>
<tr>
<td>$2 \times 10^7 \leq s \leq 3 \times 10^7$</td>
<td>587,252</td>
<td>566,320</td>
<td>1.0167</td>
</tr>
<tr>
<td>$3 \times 10^7 \leq s \leq 4 \times 10^7$</td>
<td>575,795</td>
<td>566,320</td>
<td>1.0020</td>
</tr>
<tr>
<td>$4 \times 10^7 \leq s \leq 5 \times 10^7$</td>
<td>567,480</td>
<td>566,320</td>
<td>0.9906</td>
</tr>
<tr>
<td>$5 \times 10^7 \leq s \leq 6 \times 10^7$</td>
<td>560,981</td>
<td>566,320</td>
<td>0.9817</td>
</tr>
<tr>
<td>$6 \times 10^7 \leq s \leq 7 \times 10^7$</td>
<td>555,949</td>
<td>566,320</td>
<td>0.9735</td>
</tr>
<tr>
<td>$7 \times 10^7 \leq s \leq 8 \times 10^7$</td>
<td>551,318</td>
<td>566,320</td>
<td>0.9669</td>
</tr>
<tr>
<td>$8 \times 10^7 \leq s \leq 9 \times 10^7$</td>
<td>547,572</td>
<td>566,320</td>
<td>0.9615</td>
</tr>
</tbody>
</table>
An introduction to fast generation of large prime numbers

mine the average and maximum differences between two consecutive primes in a given interval \([x, x + \Delta]\). The following formula due to Cadwell\(^{41}\) gives the mean value for the largest gap

\[
2 + (\ln x - 2) \left( \frac{\Delta}{\ln x} + \gamma \right),
\]

where \(\gamma\) is Euler's constant \((\gamma = 0.57721 \ldots\), see sec. 5). The average gap is of course \(\ln x\). Some numerical results are given in table 7 (see Cadwell\(^{41}\); Knuth\(^6\); Zagier\(^{40}\) and Weintraub\(^{42-44}\)). They allow us to verify how accurately the largest gap may be estimated and to compare the average gap with the largest one.

We are now in a position to particularize this approach to primes of the form \(kF + 1\). Considering that they are also randomly and uniformly distributed in a suitable length interval, we may estimate that the number of such primes between \(x\) and \(x + \Delta\) is given by

\[
\frac{\Delta}{\phi(F) \ln x}.
\]

We have estimated the accuracy of this formula on several examples, on the basis of data from Bays and Hudson\(^{36}\) and Shanks\(^{33}\). The numerical results are reported in table 8 and allow us to conclude that (4) is a slightly overestimating, but generally excellent approximation. Let us now examine the validity of the assumption that the density of such primes remains constant throughout a considered interval. An analysis similar to that made for primes of any form has been conducted. The results are given in table 9. We consider successive subintervals from several given intervals and we compare the actual number of primes in these subintervals with the expected value. As far as the chosen examples are concerned, the ratio between the two counts varies between 0.97 and 1.05.

The preceding discussion allows us to conclude that, in the interval \([x, x + \Delta]\), the average distance between two consecutive primes of the form \(kF + 1\) may be roughly estimated by \(\phi(F) \ln x\). Hence it seems that we may estimate that the number of such primes in the set \(S\) is in a ratio of one out \(\ln x \phi(F)/F\) elements of \(S\).

Let us now have a closer look to the ratio \(\phi(F)/F\). Let \(F = p_1^{e_1} p_2^{e_2} \ldots p_n^{e_n}\) denote the complete factorization of \(F\); then

\[
\phi(F) = F \left( 1 - \frac{1}{p_1} \right) \left( 1 - \frac{1}{p_2} \right) \ldots \left( 1 - \frac{1}{p_n} \right).
\]
<table>
<thead>
<tr>
<th>interval $[x, x + \Delta]$</th>
<th>observed maximum gap</th>
<th>calculated maximum gap</th>
<th>ratio between the observed maximum gap and the calculated one</th>
<th>average gap</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10^6 \leq s \leq 10^8 + 150000$</td>
<td>168</td>
<td>159</td>
<td>1.0543</td>
<td>18</td>
</tr>
<tr>
<td>$10^8 \leq s \leq 10^9 + 150000$</td>
<td>176</td>
<td>179</td>
<td>0.9821</td>
<td>21</td>
</tr>
<tr>
<td>$10^{10} \leq s \leq 10^{10} + 150000$</td>
<td>182</td>
<td>199</td>
<td>0.9156</td>
<td>23</td>
</tr>
<tr>
<td>$10^{11} \leq s \leq 10^{11} + 150000$</td>
<td>148</td>
<td>218</td>
<td>0.6786</td>
<td>25</td>
</tr>
<tr>
<td>$10^{12} \leq s \leq 10^{12} + 150000$</td>
<td>222</td>
<td>237</td>
<td>0.9359</td>
<td>28</td>
</tr>
<tr>
<td>$10^{13} \leq s \leq 10^{13} + 150000$</td>
<td>234</td>
<td>256</td>
<td>0.9137</td>
<td>30</td>
</tr>
<tr>
<td>$10^{14} \leq s \leq 10^{14} + 150000$</td>
<td>300</td>
<td>275</td>
<td>1.0917</td>
<td>32</td>
</tr>
<tr>
<td>$10^{15} \leq s \leq 10^{15} + 150000$</td>
<td>276</td>
<td>293</td>
<td>0.9409</td>
<td>35</td>
</tr>
<tr>
<td>$10^{16} \leq s \leq 10^{16} + 150000$</td>
<td>36</td>
<td>40</td>
<td>0.8993</td>
<td>7</td>
</tr>
<tr>
<td>$10^{17} \leq s \leq 10^{17}$</td>
<td>72</td>
<td>72.4</td>
<td>0.9944</td>
<td>9</td>
</tr>
<tr>
<td>$10^{18} \leq s \leq 10^{18}$</td>
<td>114</td>
<td>115</td>
<td>0.9942</td>
<td>12</td>
</tr>
<tr>
<td>$10^{19} \leq s \leq 10^{19}$</td>
<td>154</td>
<td>167</td>
<td>0.9222</td>
<td>14</td>
</tr>
<tr>
<td>$10^{20} \leq s \leq 10^{20}$</td>
<td>220</td>
<td>229</td>
<td>0.9587</td>
<td>16</td>
</tr>
<tr>
<td>$10^{21} \leq s \leq 10^{21}$</td>
<td>292</td>
<td>302</td>
<td>0.9332</td>
<td>18</td>
</tr>
<tr>
<td>$10^{22} \leq s \leq 10^{22}$</td>
<td>354</td>
<td>385</td>
<td>0.9190</td>
<td>21</td>
</tr>
<tr>
<td>$2.24 - 167 \leq s \leq 2.24$</td>
<td>50</td>
<td>44</td>
<td>1.1380</td>
<td>17</td>
</tr>
<tr>
<td>$2.26 - 183 \leq s \leq 2.26$</td>
<td>26</td>
<td>43</td>
<td>0.6004</td>
<td>17</td>
</tr>
<tr>
<td>$2.26 - 145 \leq s \leq 2.26$</td>
<td>42</td>
<td>43</td>
<td>0.9789</td>
<td>18</td>
</tr>
<tr>
<td>$2.27 - 235 \leq s \leq 2.27$</td>
<td>52</td>
<td>51</td>
<td>1.0215</td>
<td>19</td>
</tr>
<tr>
<td>$2.28 - 273 \leq s \leq 2.28$</td>
<td>60</td>
<td>54</td>
<td>1.1112</td>
<td>19</td>
</tr>
<tr>
<td>$2.29 - 133 \leq s \leq 2.29$</td>
<td>30</td>
<td>46</td>
<td>0.6488</td>
<td>20</td>
</tr>
<tr>
<td>$10^6 - 213 \leq s \leq 10^6$</td>
<td>84</td>
<td>51</td>
<td>1.6535</td>
<td>18</td>
</tr>
<tr>
<td>$10^8 - 267 \leq s \leq 10^8 - 73$</td>
<td>86</td>
<td>56</td>
<td>1.5461</td>
<td>21</td>
</tr>
<tr>
<td>$10^{10} - 231 \leq s \leq 10^{10}$</td>
<td>48</td>
<td>59</td>
<td>0.8084</td>
<td>23</td>
</tr>
<tr>
<td>$10^{11} - 231 \leq s \leq 10^{11}$</td>
<td>52</td>
<td>65</td>
<td>0.8051</td>
<td>25</td>
</tr>
<tr>
<td>$10^7 - 100 \leq s \leq 10^7$</td>
<td>60</td>
<td>46</td>
<td>1.3128</td>
<td>16</td>
</tr>
<tr>
<td>$10^{14} \leq s \leq 10^{14} + 10^8$</td>
<td>414</td>
<td>471</td>
<td>0.8782</td>
<td>32</td>
</tr>
<tr>
<td>$10^{17} \leq s \leq 10^{17} + 10^7$</td>
<td>432</td>
<td>486</td>
<td>0.8890</td>
<td>39</td>
</tr>
<tr>
<td>$1.1 \times 10^{16} \leq s \leq 1.1 \times 10^{16} + 10^8$</td>
<td>546</td>
<td>540</td>
<td>0.9883</td>
<td>37</td>
</tr>
<tr>
<td>$1.1 \times 10^{16} + 10^8 \leq s \leq 1.1 \times 10^{16} + 2 \times 10^8$</td>
<td>468</td>
<td>540</td>
<td>1.1531</td>
<td>37</td>
</tr>
<tr>
<td>$1.1 \times 10^{16} + 2 \times 10^8 \leq s \leq 1.1 \times 10^{16} + 3 \times 10^8$</td>
<td>484</td>
<td>540</td>
<td>1.1149</td>
<td>37</td>
</tr>
<tr>
<td>$1.1 \times 10^{16} + 3 \times 10^8 \leq s \leq 1.1 \times 10^{16} + 4 \times 10^8$</td>
<td>510</td>
<td>540</td>
<td>1.0581</td>
<td>37</td>
</tr>
<tr>
<td>$1.1 \times 10^{16} + 4 \times 10^8 \leq s \leq 1.1 \times 10^{16} + 5 \times 10^8$</td>
<td>528</td>
<td>540</td>
<td>1.0220</td>
<td>37</td>
</tr>
<tr>
<td>$1.1 \times 10^{16} + 5 \times 10^8 \leq s \leq 1.1 \times 10^{16} + 6 \times 10^8$</td>
<td>504</td>
<td>540</td>
<td>1.0707</td>
<td>37</td>
</tr>
<tr>
<td>$1.1 \times 10^{16} + 6 \times 10^8 \leq s \leq 1.1 \times 10^{16} + 7 \times 10^8$</td>
<td>494</td>
<td>540</td>
<td>1.0924</td>
<td>37</td>
</tr>
<tr>
<td>$1.1 \times 10^{16} + 7 \times 10^8 \leq s \leq 1.1 \times 10^{16} + 8 \times 10^8$</td>
<td>484</td>
<td>540</td>
<td>1.1149</td>
<td>37</td>
</tr>
<tr>
<td>$1.1 \times 10^{16} + 8 \times 10^8 \leq s \leq 1.1 \times 10^{16} + 9 \times 10^8$</td>
<td>460</td>
<td>540</td>
<td>1.1731</td>
<td>37</td>
</tr>
<tr>
<td>$1.1 \times 10^{16} + 9 \times 10^8 \leq s \leq 1.1 \times 10^{16} + 10^9$</td>
<td>486</td>
<td>540</td>
<td>1.1103</td>
<td>37</td>
</tr>
</tbody>
</table>
TABLE 8
Prime counts in given intervals and forms

<table>
<thead>
<tr>
<th>interval ([x, x + \Delta])</th>
<th>(\pi(x \leq s \leq x + \Delta, 24,1))</th>
<th>(\Delta/8 \ln x)</th>
<th>(\pi(x \leq s \leq x + \Delta, 24,1)/\Delta/8 \ln x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(10^{11} \leq s \leq 2 \times 10^{11})</td>
<td>486 130 233</td>
<td>493 516 457</td>
<td>0.9850</td>
</tr>
<tr>
<td>(2 \times 10^{11} \leq s \leq 3 \times 10^{11})</td>
<td>476 410 254</td>
<td>480 370 464</td>
<td>0.9918</td>
</tr>
<tr>
<td>(3 \times 10^{11} \leq s \leq 4 \times 10^{11})</td>
<td>470 320 943</td>
<td>473 000 233</td>
<td>0.9943</td>
</tr>
<tr>
<td>(4 \times 10^{11} \leq s \leq 5 \times 10^{11})</td>
<td>465 887 425</td>
<td>467 906 650</td>
<td>0.9957</td>
</tr>
<tr>
<td>(5 \times 10^{11} \leq s \leq 6 \times 10^{11})</td>
<td>462 420 065</td>
<td>464 030 681</td>
<td>0.9965</td>
</tr>
<tr>
<td>(6 \times 10^{11} \leq s \leq 7 \times 10^{11})</td>
<td>459 568 492</td>
<td>460 911 132</td>
<td>0.9971</td>
</tr>
<tr>
<td>(7 \times 10^{11} \leq s \leq 8 \times 10^{11})</td>
<td>457 165 032</td>
<td>458 306 128</td>
<td>0.9975</td>
</tr>
<tr>
<td>(8 \times 10^{11} \leq s \leq 9 \times 10^{11})</td>
<td>455 082 970</td>
<td>456 073 257</td>
<td>0.9978</td>
</tr>
<tr>
<td>(9 \times 10^{11} \leq s \leq 10^{12})</td>
<td>453 240 447</td>
<td>454 121 708</td>
<td>0.9981</td>
</tr>
</tbody>
</table>

Thus we may conclude that the smaller \(\phi(F)/F\) is (that is, the more small prime factors \(F\) has), the more prime numbers \(S\) contains. In any case, as \(F\) is an even integer, \(\phi(F)/F\) is always less than \(1/2\). More precisely the average value of \(\phi(F)/F\) is \(3/\pi^2 \sim 0.30396\) (see Apostol\textsuperscript{35}, p.82).

5. Sieves

A \textit{sieve} is a combinatorial technique that allows one to eliminate all the unwanted members of a finite set by a finite sequence of well-defined steps (for the history of the sieve process, see Lehmer\textsuperscript{45}).
C. Couvreur and J. J. Quisquater

TABLE 9
Variations of density of primes of the form $kF + 1$

<table>
<thead>
<tr>
<th>interval $[x, x + A]$</th>
<th>$\pi(x \leq s \leq x + A, 24, 1)$</th>
<th>expected number of primes</th>
<th>ratio between the actual count and the expected one</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10^{11} \leq s \leq 10^{12}$</td>
<td>4 186 225 861</td>
<td>465 136 207 (= 4 186 225 861/9)</td>
<td>1.0451</td>
</tr>
<tr>
<td>$10^{11} \leq s \leq 2 \cdot 10^{11}$</td>
<td>486 130 233</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$2 \cdot 10^{11} \leq s \leq 3 \cdot 10^{11}$</td>
<td>476 410 254</td>
<td></td>
<td>1.0242</td>
</tr>
<tr>
<td>$3 \cdot 10^{11} \leq s \leq 4 \cdot 10^{11}$</td>
<td>470 320 943</td>
<td></td>
<td>1.0111</td>
</tr>
<tr>
<td>$4 \cdot 10^{11} \leq s \leq 5 \cdot 10^{11}$</td>
<td>465 887 425</td>
<td></td>
<td>1.0016</td>
</tr>
<tr>
<td>$5 \cdot 10^{11} \leq s \leq 6 \cdot 10^{11}$</td>
<td>462 420 065</td>
<td></td>
<td>0.9942</td>
</tr>
<tr>
<td>$6 \cdot 10^{11} \leq s \leq 7 \cdot 10^{11}$</td>
<td>459 568 492</td>
<td></td>
<td>0.9880</td>
</tr>
<tr>
<td>$7 \cdot 10^{11} \leq s \leq 8 \cdot 10^{11}$</td>
<td>457 165 032</td>
<td></td>
<td>0.9829</td>
</tr>
<tr>
<td>$8 \cdot 10^{11} \leq s \leq 9 \cdot 10^{11}$</td>
<td>455 082 970</td>
<td></td>
<td>0.9784</td>
</tr>
<tr>
<td>$9 \cdot 10^{11} \leq s \leq 10^{12}$</td>
<td>453 240 447</td>
<td></td>
<td>0.9744</td>
</tr>
</tbody>
</table>

$\pi(x \leq s \leq x + A, 8, 1)$

<table>
<thead>
<tr>
<th>interval $[x, x + A]$</th>
<th>$\pi(x \leq s \leq x + A, 8, 1)$</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$250 000 \leq s \leq 1 000 000$</td>
<td>14 079</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$250 000 \leq s \leq 500 000$</td>
<td>4 861</td>
<td>4 693</td>
<td>1.0358</td>
</tr>
<tr>
<td>$500 000 \leq s \leq 750 000$</td>
<td>4 664</td>
<td></td>
<td>0.9938</td>
</tr>
<tr>
<td>$750 000 \leq s \leq 1 000 000$</td>
<td>4 554</td>
<td></td>
<td>0.9704</td>
</tr>
</tbody>
</table>

$\pi(x \leq s \leq x + A, 10, 1)$

<table>
<thead>
<tr>
<th>interval $[x, x + A]$</th>
<th>$\pi(x \leq s \leq x + A, 10, 1)$</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$250 000 \leq s \leq 1 000 000$</td>
<td>14 122</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$250 000 \leq s \leq 500 000$</td>
<td>4 891</td>
<td>4 707</td>
<td>1.0390</td>
</tr>
<tr>
<td>$500 000 \leq s \leq 750 000$</td>
<td>4 641</td>
<td></td>
<td>0.9859</td>
</tr>
<tr>
<td>$750 000 \leq s \leq 1 000 000$</td>
<td>4 590</td>
<td></td>
<td>0.9751</td>
</tr>
</tbody>
</table>

$\pi(x \leq s \leq x + A, 12, 1)$

<table>
<thead>
<tr>
<th>interval $[x, x + A]$</th>
<th>$\pi(x \leq s \leq x + A, 12, 1)$</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$252 000 \leq s \leq 1 008 000$</td>
<td>14 211</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$252 000 \leq s \leq 504 000$</td>
<td>4 900</td>
<td>4 737</td>
<td>1.0344</td>
</tr>
<tr>
<td>$504 000 \leq s \leq 756 000$</td>
<td>4 696</td>
<td></td>
<td>0.9913</td>
</tr>
<tr>
<td>$756 000 \leq s \leq 1 008 000$</td>
<td>4 615</td>
<td></td>
<td>0.9742</td>
</tr>
</tbody>
</table>

The sieve idea plays a fundamental role in the theory of numbers. Deshoul- lers$^{46}$). Halberstam and Richert$^{47}$) and Hooley$^{48}$) describe the theoretical frame for the sieves. Here we shall only give an elementary account of sieve methods which are relevant to the problem of prime generation.

The first known method for determining primes is the sieve of Eratosthenes. It eliminates the composite numbers between $n^2$ and $n$ in the following way:
An introduction to fast generation of large prime numbers

all multiples of the first prime, i.e. 2, are removed; then all multiples of the next prime, i.e. 3, are removed, and so on. The process stops after sifting with the largest prime less than $n^4$.

The sieve of Eratosthenes is computationally fast and easily implemented since the multiples of a number may be computed by successive additions or shifts. Let $p_i$ be the $i$th prime. Then the number of "cross-out" operations, i.e. essentially the computation time, is given by

$$t = n \left( \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{p_k} \right),$$

where $p_k$ is the largest prime not exceeding $n^4$. By use of

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{p} \sim \int_2^p \frac{dp}{p \ln p} \sim \ln \ln p,$$

we obtain

$$t = \sum_{i=1}^{n(n^4)} \frac{1}{p_i} \sim n \ln \ln n^4.$$  

We conclude that, for any practical purpose, the computation time is essentially linear with respect to $n$ (for instance, for $n = 10^{10}$, $\ln \ln 10^6 \sim 2.4435$).

Nearly all prime number generators use the sieving principle. Elementary algorithms are described by Chartres $^{49}$, Singleton $^{60}$ and Wood $^{51}$. The complexity of sieve processes is studied by Mairson $^{55}$ and Gries and Misra $^{53}$. These authors give an algorithm of arithmetic complexity $O(n)$ and show that, under the RAM model of computation, this upper bound is equivalent to the theoretical lower bound. Another algorithm, the arithmetic complexity of which is only $O(n/\ln \ln n)$, is presented by Pritchard $^{61}$. Bays and Hudson $^{56}$ show how the problem of the large amount of memory required can be removed. Wells $^{66}$ and Wunderlich $^{66}$ give the most efficient methods for representing sets and discuss the programming difficulties encountered when sieving out these sets.

All published tables are computed by application of the sieve of Eratosthenes. Large or compact lists of primes may be found in Lehmer $^{51}$, Weintraub $^{67}$ and Baker and Gruenberger $^{68}$, up to the prime $104395289$. Special devices for sieving are announced or described by Lehmer $^{59,60}$ and Cantor, Estrin, Fraenkel and Turn $^{61}$ with rates of sieving up to $10^{10}$ numbers/min. Finally, let us remark that the most efficient sieves of Eratosthenes permit to generate primes up to about $10^{16}$, which is much too low for cryptographic applica-
C. Couvreur and J. J. Quisquater

tions. However, these sieves may prove useful in the preliminary generation of factors in a random factorization.

The sieving set with sieve limit \( x \), denoted by \( P_x \), is defined to be the set of all primes \( p \) with \( 2 \leq p \leq x \). Then, the function \( Q(x) \) is defined by

\[
Q(x) = \prod_{p \in P_x} \left( 1 - \frac{1}{p} \right).
\]

For an integer \( n \) much larger than \( x \) but otherwise random, we loosely interpret \( Q(x) \) as the probability for \( n \) to be relatively prime to all primes in \( P_x \).

From the approximation

\[
e^{-1/p} \sim 1 - \frac{1}{p},
\]

we find

\[
Q(x) \sim \exp \left( - \sum_{p \in P_x} \frac{1}{p} \right),
\]

and from (5) we conclude that

\[
Q(x) \sim e^{-\ln x} \sim \frac{1}{\ln x}.
\]

In fact, the Mertens theorem (see Hardy and Wright\(^{10, p.351}\)) gives the estimation

\[
Q(x) \sim \frac{e^{-\gamma}}{\ln x} \sim \frac{0.56145948...}{\ln x}, \tag{6}
\]

where \( \gamma \) is the Euler or Mascheroni constant. This constant is defined by

\[
\gamma = \lim_{n \to +\infty} \left( 1 + \frac{1}{2} + \ldots + \frac{1}{n} - \ln n \right)
\]

and is known up to at least 30 100 decimal places (see Brent and McMillan\(^{62}\)). The value \( \gamma \approx 0.577215664902 \) is sufficient for our purposes.

Table 10 displays the actual function \( Q(x) \) and its estimate (6) for some values of \( s \). Further numerical data can be found in Appel and Rosser\(^{68}\).

If a set \( P_x \) is used to sieve out the set of odd numbers

\[
S = \{ s = kF + 1 \mid 1 \leq k \leq K \},
\]

as defined in (1), the function \( 2Q(x) \) gives the average ratio of surviving numbers.

The problem of determining the most efficient sieve limit \( x \) is thus reduced to a straightforward minimization problem involving the relevant asymptotic formulas (see Crandall and Penk\(^{20}\)) for an example).
An introduction to fast generation of large prime numbers

TABLE 10
The function $Q$ and its estimation

<table>
<thead>
<tr>
<th>$x$</th>
<th>greatest prime $&lt; x = p$</th>
<th>$Q(p)$</th>
<th>$\frac{e^{-x}}{\ln p}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>7</td>
<td>0.228 571 558 192</td>
<td>0.288 533 097 9</td>
</tr>
<tr>
<td>$10^2$</td>
<td>97</td>
<td>0.120 317 304 818</td>
<td>0.122 731 137 8</td>
</tr>
<tr>
<td>$10^3$</td>
<td>997</td>
<td>0.080 965 273 159</td>
<td>0.081 314 952 89</td>
</tr>
<tr>
<td>$10^4$</td>
<td>9973</td>
<td>0.060 884 699 714</td>
<td>0.060 977 588 56</td>
</tr>
<tr>
<td>$10^5$</td>
<td>99991</td>
<td>0.048 752 923 663</td>
<td>0.048 768 132 36</td>
</tr>
<tr>
<td>$5 \times 10^6$</td>
<td>499 979</td>
<td>0.042 781 472 584</td>
<td>0.042 786 597 53</td>
</tr>
<tr>
<td>$10^6$</td>
<td>999 983</td>
<td>0.040 638 215 016</td>
<td>0.040 639 842 58</td>
</tr>
</tbody>
</table>

If a set $P_x$ is used to sieve out a small set $S = \{ s = kF + 1 \mid 1 \leq k \leq K \}$ of large numbers, the classical techniques of sieving are prohibitive. More relevant techniques are:

- successive divisions by the numbers from $P_x$,
- computation of $\gcd(s, N_x)$, for each $s \in S$, where $N_x$ is the product of first primes up to $x$. If $\gcd(s, N_x) \neq 1$, $s$ is eliminated from $S$. If $x$ is too large, it might be necessary to compute several gcd’s. If $N_x$ is a number larger than $s$, the computation of this gcd requires at most $2.078 \ln N_x$ divisions using the Euclidean algorithms (see Knuth 6, p. 343). Other efficient algorithms exist for computing gcd’s without any division (which is a relatively slow operation). We compute now the function $\ln N_x$. Let us put Chebyshev’s $\theta$-function (see Apostol 86, p. 75) defined by

$$\theta(x) = \ln \prod_{p \leq x} p.$$  

A good approximation to $\theta(x)$ is given by

$$\theta(x) = \sum_{p \leq x} \ln p \leq \pi(x) \ln x,$$

i.e., from the prime number theorem,

$$\theta(x) \sim x.$$  

Among other results about the function $\theta$, Schoenfeld 64) shows, by extensive computations, that

$$x - 2.05x^{\frac{1}{2}} < \theta(x) < x,$$

for $0 \leq x \leq 10^{11}$. Table 11 gives some values of $\theta(x)$. For $x = 500,000$, our computation confirms the value given by Johnson 65).

In conclusion this section has shown that the partial sieving is fruitful even for large numbers. A good value for the sieving limit $x$ seems to be about 1 000.

TABLE 11
The product of first primes and its estimation

<table>
<thead>
<tr>
<th>( x )</th>
<th>( p )</th>
<th>( \theta(p) )</th>
<th>( p - 2.05 p^{\frac{1}{3}} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>7</td>
<td>5.347 107 531</td>
<td>1.576 209 812</td>
</tr>
<tr>
<td>100</td>
<td>97</td>
<td>83.728 390 399</td>
<td>76.809 841 51</td>
</tr>
<tr>
<td>1 000</td>
<td>997</td>
<td>956.245 265 12</td>
<td>932.270 621 0</td>
</tr>
<tr>
<td>10 000</td>
<td>9 973</td>
<td>9 895.991 379 2</td>
<td>9 768.276 937</td>
</tr>
<tr>
<td>100 000</td>
<td>99 991</td>
<td>99 685.389 2</td>
<td>99 342.762 25</td>
</tr>
<tr>
<td>500 000</td>
<td>499 979</td>
<td>499 318.120</td>
<td>498 529.461 5</td>
</tr>
<tr>
<td>1 000 000</td>
<td>999 983</td>
<td>998 484.175</td>
<td>997 933.017 4</td>
</tr>
</tbody>
</table>

6. Compositeness tests

Miller\(^{66,67}\), Rabin\(^{68,69}\) and Solovay and Strassen\(^{70}\) have developed fast stochastic methods to recognize the compositeness of a number. These methods make no use of any factorization and allow one to build efficient probabilistic primality testing algorithms.

In this section, we first discuss some extensions of Fermat’s theorem and other number-theoretic concepts which are needed for the presentation of these tests. We refer to Baratz\(^{71}\), Chaitin and Schwartz\(^{72}\), Monier\(^{73,74}\) and Selfridge (unpublished) for an analysis of their performance. Then, as applications, we present exact and probabilistic primality tests and compositeness tests. Our treatment is closely related to Monier’s discussion and to Selfridge’s ideas presented by Williams\(^{18}\).

Let \( s = p_1^{e_1} p_2^{e_2} \ldots p_n^{e_n} \) be the prime decomposition of \( s \), and let us define the following functions:

(i) The Carmichael function \( \lambda(s) = \varphi(\varphi(p_i^{e_i})) \), also called the indicator of \( s \).

(ii) The dyadic valuation \( v_2(s) = \max \{ k \text{ such that } 2^k \mid s \} \).

(iii) The Jacobi symbol \( \left( \frac{s}{p} \right) \), for an odd integer \( s \) and any integer \( a \), where \( \left( \frac{s}{p} \right) \) is the Legendre symbol, i.e., the integer in the set \( \{0, 1, -1\} \) congruent to \( a^{(p-1)/2} \) modulo \( p \) (note that \( \left( \frac{s}{p} \right) = 0 \) if and only if \( \gcd(a,s) \neq 1 \)).

Let \( s \) be an odd prime power. Then the set of positive integers less than \( s \) and relatively prime with \( s \) is known to be of the form \( \{g^i \pmod{s} \mid 0 \leq i < \lambda(s) \} \), for a suitable integer \( g \) called a primitive root of \( s \). Thus for each \( a \) with \( \gcd(a,s) = 1 \) there exists a unique exponent \( i \) in the interval \( 0 \leq i < \lambda(s) \) such that \( g^i \equiv a \pmod{s} \); this exponent is called the index of \( a \) modulo \( s \) (relative to \( g \)) and is denoted by \( \text{ind}(a) \). The theory of indices bears certain
similarities with that of logarithms, the primitive root $g$ playing the role of the base.

The least positive integer $t$ such that $a^t \equiv 1 \pmod{s}$ is called the order of $a$ in the group of reduced residues $(\mod{s})$ and is denoted by $\text{ord}_s(a)$.

Let us now recall Fermat's theorem.

**Theorem 1.** (Fermat, 1640: see Apostol\textsuperscript{35}, p.114). If $s$ is prime and $\gcd(a, s) = 1$, then

$$a^{s-1} \equiv 1 \pmod{s}. \quad (7)$$

Therefore if $a^{s-1} \not\equiv 1 \pmod{s}$ for some $a$ with $1 < a < s$, then $s$ must be composite. It is not true that if (7) holds for some $a$, then $s$ is prime. For example, consider the composite number $341 = 11 \cdot 31$. As $2^{10} - 1 = 3 \cdot 11 \cdot 31$, we have $2^{10} \equiv 1 \pmod{341}$, hence $2^{340} \equiv 1 \pmod{341}$. We call any integer $s$ satisfying (7) for a given $a$ a "base a-pseudo-prime" or a-psp.

**Theorem 2.** (Cipolla\textsuperscript{75}): see Williams\textsuperscript{18}, p.139) and Hardy and Wright\textsuperscript{10}, P.72). For each $a > 1$, there exist infinitely many composite a-psp's.

**Proof:**

Let $p$ be an odd prime such that $\gcd(p, a^2 - 1) = 1$. The number

$$s = \frac{a^{2p} - 1}{a^2 - 1} = \frac{a^p - 1}{a - 1} \frac{a^p + 1}{a + 1}$$

is clearly a composite number. We have

$$a^{2p} \equiv s(a^2 - 1) + 1 \equiv 1 \pmod{s},$$

and

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

Since $a^{p-1} - 1$ is divisible by $p(a^2 - 1)$ and $(a^{p-1} + 1) a^2$ is always an even integer, we conclude that $s - 1$ is divisible by $2p$, whence

$$a^{r-1} \equiv 1 \pmod{s}.$$

Notice that, if (7) is satisfied for all $a$ relatively prime to $s$, then $s$ is not necessarily prime. There exist composite numbers having that property. They are called Carmichael numbers. These numbers are characterized by Carmichael\textsuperscript{28} who obtains the following result.

**Theorem 3.** The necessary and sufficient condition for a number $s$ to be a Carmichael number is that $\lambda(s) | s - 1$. A Carmichael number is odd and equal to a product of distinct primes $s = p_1 p_2 \ldots p_n$, with $n \geq 3$. 

---

The smallest Carmichael numbers are $561 = 3 \cdot 11 \cdot 17$, $1105 = 5 \cdot 13 \cdot 17$ and $1729 = 7 \cdot 13 \cdot 19$ (for $a = 2$, these numbers are not given by Cipolla’s construction). Methods for constructing Carmichael numbers are devised by Chernick (76) and Sispanov (77). A detailed account of these methods is given by Ore (78, p. 391–399). It is still not known whether infinitely many Carmichael numbers exist or not.

We denote by $CP_2(x)$ the number of composite 2-psp’s less than or equal to $x$ and by $C(x)$ the number of Carmichael numbers less than or equal to $x$. Tables of numerical values for these numbers are constructed by Lehmer (79), Poulet (80), Swift (81), Monier (73) (this last table is incomplete) and Pomerance, Selfridge and Wagstaff (82, 83). In table 12 we summarize these results, which suggest the following asymptotic relations:

$$CP_2(x) \sim \pi(x)^{0.482},$$
and

$$C(x) \sim 0.155 x^{0.4}.$$

Table 12 shows in particular that, for $x = 10^{10}$, the number of primes satisfying (7) for $a = 2$ is $30,571$ times larger than the number of non-primes with the same property.

In order to handle the Carmichael numbers, some refinement of Fermat’s theorem and some new concepts are to be introduced.

### TABLE 12
Composite 2-psp’s and Carmichael numbers

<table>
<thead>
<tr>
<th>$x$</th>
<th>$\pi(x)$</th>
<th>$CP_2(x)$</th>
<th>$\pi(x)^{0.482}$</th>
<th>$C(x)$</th>
<th>$0.155 x^{0.4}$</th>
<th>$\frac{CP_2(x)}{C(x)}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10^3$</td>
<td>168</td>
<td>3</td>
<td>12</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>$10^4$</td>
<td>1229</td>
<td>22</td>
<td>31</td>
<td>7</td>
<td>6</td>
<td>3.143</td>
</tr>
<tr>
<td>$10^5$</td>
<td>9,592</td>
<td>78</td>
<td>83</td>
<td>16</td>
<td>16</td>
<td>4.875</td>
</tr>
<tr>
<td>$10^6$</td>
<td>78,498</td>
<td>245</td>
<td>229</td>
<td>43</td>
<td>39</td>
<td>5.698</td>
</tr>
<tr>
<td>$10^7$</td>
<td>664,579</td>
<td>750</td>
<td>640</td>
<td>105</td>
<td>98</td>
<td>7.143</td>
</tr>
<tr>
<td>$10^8$</td>
<td>5,761,455</td>
<td>2,057</td>
<td>1,814</td>
<td>255</td>
<td>246</td>
<td>8.067</td>
</tr>
<tr>
<td>$10^9$</td>
<td>50,847,478</td>
<td>5,597</td>
<td>5,181</td>
<td>646</td>
<td>617</td>
<td>8.664</td>
</tr>
<tr>
<td>$10^{10}$</td>
<td>455,052,511</td>
<td>14,884</td>
<td>14,900</td>
<td>1,547</td>
<td>1,550</td>
<td>9.622</td>
</tr>
<tr>
<td>$25 \cdot 10^9$</td>
<td>21,853</td>
<td>2,163</td>
<td>2,236</td>
<td>10.103</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
An introduction to fast generation of large prime numbers

An "Euler base $a$-pseudoprime" is an odd integer $s$ such that

$$a^{(s-1)/2} \equiv \left( \frac{a}{s} \right) \pmod{s}.$$  

If $s$ is an odd prime and $\gcd(a, s) = 1$, then $s$ is an Euler $a$-pseudoprime.

Following Selfridge and Williams\(^{18}\), we define a "strong base $a$-pseudoprime" to be an odd integer $s$ such that, writing $s - 1 = 2^r s'$, $s'$ odd, one has either

$$a^{s'} \equiv 1 \pmod{s}$$

or

$$a^{2^k s'} \equiv -1 \pmod{s},$$

for some $k$, $0 < k < v_0$. Again, if $s$ is an odd prime and $\gcd(a, s) = 1$, then $s$ is a strong $a$-pseudoprime.

An odd integer $s$ satisfies the property MR (see Miller\(^{68,67}\)) for a given $a$ if

$$a^{s-1} \equiv 1 \pmod{s}$$

and for every integer $k$, $0 < k \leq v_0$,

$$a^{(s-1)/2^k} \not\equiv 1 \pmod{s}$$

implies

$$\gcd(a^{(s-1)/2^k} - 1, s) = 1.$$  

**Theorem 4.** (Selfridge, see Williams\(^{18}\)). An odd integer $s$ satisfies the property MR for a given $a$ if and only if it is a strong $a$-pseudoprime.

**Proof.**

First, suppose $s$ satisfies the property MR for a given $a$.

- If no value of $k$ exists such that $a^{(s-1)/2^k} \not\equiv 1 \pmod{s}$, then $a^{(s-1)/2^k} \equiv 1$ for all possible $k$'s and thus $a^{s'} \equiv 1 \pmod{s}$.
- Otherwise, let $k$ be the least integer such that $a^{(s-1)/2^k} \not\equiv 1 \pmod{s}$. Then

$$a^{(s-1)/2^k} \equiv 1 \pmod{s},$$

hence

$$(a^{(s-1)/2^k} - 1) (a^{(s-1)/2^k} + 1) \equiv 0 \pmod{s}.$$  

From $\gcd(s, a^{(s-1)/2^k} - 1) = 1$, we conclude that

$$a^{(s-1)/2^k} = a^{2^{v_0-k}} \equiv -1 \pmod{s}$$

and thus $s$ is a strong $a$-pseudoprime.

Conversely, suppose now that $s$ is a strong $a$-pseudoprime.

- If $a^{s'} \equiv 1 \pmod{s}$, then $a^{2^i s'} \equiv 1 \pmod{s}$, $0 \leq i \leq v_0$.
- If $a^{2^k s'} \equiv -1 \pmod{s}$ for some $k$, $0 \leq k \leq v_0$, then $a^{2^{k+i} s'} \equiv 1 \pmod{s}$.

Hence $v_0 - k$ is the value of the least positive integer $l$ such that $a^{(s-1)/2^l} \not\equiv 1 \pmod{s}$. From

$$a^{(s-1)/2^{v_0-k}} + 1 \equiv 0 \pmod{s},$$

we conclude that

$$\gcd(a^{(s-1)/2^{v_0-k}} - 1, s) = 1,$$

i.e. satisfies the property $MR$ for $a$.

We now require the following result.

**Theorem 5.** See Pocklington.\(^8\) Let $q$ be any prime such that $q^e|m$ and $q^{e+1} \mid m$. If $a^m \equiv 1 \pmod{s}$ and $\gcd(a^{m/q} - 1, s) = 1$, then any prime factor of $s$ must have the form $1 + kq^e$.

This result produces the following theorem proved by Selfridge\(^1\) and Monier\(^7,8\).

**Theorem 6.** If $s$ is a strong $a$-psp, then $s$ is an Euler $a$-psp.

**Sketched proof.**

— First, if $a^s \equiv 1 \pmod{s}$, then by Fermat's theorem and since $s'$ is odd, $a^{(p-1)/2} \equiv 1 \pmod{s}$ for each prime divisor $p$ of $s$. From this, we conclude that

$$a^{(s-1)/2} \equiv \left(\frac{a}{s}\right) \pmod{s}.$$

— Otherwise if $a^{2r} \equiv -1 \pmod{s}$ for some $r$ with $0 \leq r < v_0$, we have by theorem 5 that $d | 2^{r+1}s'$ and $d \not\mid 2^r s'$ where $d = \text{ord}_p(a)$ and $p$ is any prime divisor of $s$. Thus $d$ is an odd multiple of $2^{r+1}$ and $p = 2^{r+1} k + 1$.

By definition,

$$a^{d/2} \equiv -1 \pmod{p}$$

and

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \equiv (-1)^{(p-1)/d} \pmod{p}.$$

Thus

$$\left(\frac{a}{p}\right) = (-1)^k.$$

From the prime decomposition $s = \prod_{i=1}^{n} p_i^{e_i}$ and from $p_i = 2^{r+1} k_i + 1$, we have

$$s \equiv 1 + 2^{r+1} \sum_{i=1}^{n} e_i k_i \pmod{2^{2r+2}}.$$

Thus

$$s' 2^{v_0-1} = (s - 1)/2 \equiv 2^r \sum_{i=1}^{n} e_i k_i \pmod{2^{r+1}}$$

and

$$2^{v_0-1-r} \equiv \sum_{i=1}^{n} e_i k_i \pmod{2}.$$
An introduction to fast generation of large prime numbers

The theorem follows from
\[ a^{(r-1)/2} \equiv (-1)^{2^{r-1}-r} = (-1)^{\sum_{i=1}^{n} e_i k_i} \pmod{s} \]
and
\[ \left( \frac{a}{s} \right) = \prod_{i=1}^{n} \left( \frac{a}{p_i} \right)^{e_i} = (-1)^{\sum_{i=1}^{n} e_i k_i}. \]

For any odd composite numbers \( s \), let \( L_{MR}(s) \) denote the set of all \( a, 1 \leq a < s \), such that \( s \) is a strong \( a \)-psp. For computing the size of \( L_{MR}(s) \), we need to know the number of solutions to the equation \( x^t \equiv b \pmod{s} \) in the unknown \( x \).

Theorem 7. (see Monier 74). Let \( s \) be an odd integer, \( s = p_1^{e_1} \ldots p_n^{e_n} \) its prime factorization, \( s \) an integer such that \( \gcd(b, s) = 1 \), \( t \) a positive integer and \( \delta_i = \gcd(b, \phi(p_i^{e_i})) \). The binomial congruence \( x^t \equiv b \pmod{s} \) has solutions if and only if, for each \( i, 1 \leq i \leq n \), the index of \( b \) modulo \( p_i^{e_i} \) is a multiple of \( \delta_i \). If this condition is satisfied, the congruence has \( \prod_{i=1}^{n} \delta_i \) solutions.

Proof.
The theorem follows from the combination of two well-known theorems:
- The congruence \( x^t \equiv b \pmod{p_i^{e_i}} \) has solutions if and only if the index of \( b \) is a multiple of \( \delta_i \), in which case it has exactly \( \delta_i \) solutions (see Vinogradov 85, p.81)).
- The number of solutions of \( x^t \equiv b \pmod{s} \) is the product of the numbers of solutions to the separate congruences \( x^t \equiv b \pmod{p_i^{e_i}} \), \( 1 \leq i \leq n \) (see Vinogradov 85, p.48)).

Theorem 8. (see Monier 74). If \( s \) is composite, then the size of the set \( L_{MR}(s) \) of all \( a, 1 \leq a < s \), such that \( s \) is a strong \( a \)-psp is given by

\[ |L_{MR}(s)| = (1 + (2^{r_n} - 1)/(2^n - 1)) \prod_{u=1}^{n} \gcd(s', p_i). \]

Proof.
First let us consider the congruence \( a^{2^t} \equiv 1 \pmod{s} \). By theorem 7, the number of solutions is given by

\[ \prod_{i=1}^{n} \gcd(s', \phi(p_i^{e_i})) = \prod_{i=1}^{n} \gcd(s', p_i - 1) = \prod_{i=1}^{n} \gcd(s', p_i). \]

The other congruences \( a^{2^t 2^k} \equiv -1 \pmod{s} \), \( 0 \leq k < \nu_0 \), have solutions if and only if \( \gcd(s' 2^k, \phi(p_i^{e_i})) \) divides \( \text{ind}(-1) = \phi(p_i^{e_i})/2 = p_i^{e_i}(p_i - 1)/2 \), for any \( 1 \leq i \leq n \), i.e. \( k < \nu_i = \nu_2(p_i - 1) \) for \( i = 1, \ldots, n \), or equivalently

\[ k < \nu = \min \{ \nu_2(p_i - 1) \}. \]

The number of solutions to this congruence is then
Thus we have

\[ |L_{MR}(s)| = (1 + \sum_{k=0}^{v-1} 2^{kn}) \prod_{i=1}^{n} \gcd(s', p_i) \]

which after simplification proves the theorem.

We now derive an upper bound on \(|L_{MR}(s)|/(s - 1)|\), which we denote by \(\alpha_s\). For \(s\) prime, we have \(\alpha_s = 1\). For \(s\) composite, we distinguish three cases: \(s\) is a prime power, a Carmichael number or neither of them.

1) \(s = p^e, e \geq 2\). Thus \(n = 1\) and then

\[ \alpha_s = \frac{1}{1 + p + \ldots + p^{e-1}} \frac{\gcd(s', p^e)}{p^e} \leq \frac{1}{1 + p}. \]

From \(p \geq 3\), it follows that \(\alpha_s \leq 1/4\); equality holds only for \(s = 9\).

2) \(s\) is a Carmichael number. Then, by theorem 3, \(s\) is a product of \(n\) distinct primes, at least three. Furthermore, \(p_i' \mid s - 1\). The formula becomes

\[ \alpha_s = \left(1 + \frac{2^{vn} - 1}{2^n - 1}\right) \frac{\prod_{i=1}^{n} p_i'}{s - 1}. \]

From

\[ 2^{vn} \prod_{i=1}^{n} p_i' \leq \prod_{i=1}^{n} (p_i - 1) \leq s - 1, \]

we have

\[ \alpha_s \leq \left(1 + \frac{2^{vn} - 1}{2^n - 1}\right) \frac{1}{2^{vn}} \left(1 - \frac{1}{2^{vn}}\right) \left(1 - \frac{1}{2^n - 1}\right), \]

which is an upper bound decreasing with \(v\) and \(n\). Since \(n \geq 3\) and \(v \geq 1\), one finds that \(\alpha_s \leq \frac{1}{4}\). In fact, the limit \(\frac{1}{4}\) for \(\alpha_s\) is approached by Carmichael's numbers with exactly three prime factors, each being \(\equiv 3 \pmod{4}\). These numbers satisfy \(\alpha_s = \phi(s)/(s - 1)\) and \(p_i - 1 = 2p_i\), \(i = 1, 2, 3\). Examples given by Monier \(7^4\) are \(s = 8911\), with \(\alpha_s = 0.2\) and \(s = 1024651\) with \(\alpha_s = 0.23478\). Notice that if a prime factor of \(s\) is \(\equiv 3 \pmod{4}\) then \(\alpha_s \leq \frac{1}{4}\). An example is \(s = 561\) with \(\alpha_s = 70/561\).

3) \(s\) is not a prime power and not a Carmichael number. Then there exists a \(p_i\) such that \(p_i \mid s\) and \(\phi(p_i^e) \chi s - 1\). Therefore, three cases are to be considered:

- \(v_i > v_0\): simple computations allow us to conclude that \(\alpha_s \leq \phi(s)/4(s - 1)\)
  and thus \(\alpha_s < \frac{1}{4}\).
An introduction to fast generation of large prime numbers

— $p|\chi s'$: the conclusion is then that $\alpha_s \leq \phi(s)/6(s-1)$ and certainly $\alpha_s < \frac{1}{6}$.

— $e_1 > 1$: the bound is identical to the second case.

The bound $\frac{1}{4}$ is very likely to be the best possible. Indeed, for the numbers $s$ of the form $s = (2q + 1)(4q + 1)$, where $q$ is odd and both $(2q + 1)$ and $(4q + 1)$ are prime, the value $\alpha_s$ is given by $q/(4q + 3)$ and thus can be arbitrarily close to $\frac{1}{4}$ if the set of these numbers $s$ is infinite (open question). Monier gives as examples $s = 15, 91, 703, 1891$ and $497503$.

From this lengthy discussion, we obtain

**Theorem 9.** If $s$ is composite, then

$$\alpha_s = \frac{|L_{MR}(s)|}{s-1} \leq \frac{1}{4}.$$

7. Applications

7.1. Compositeness tests

For each odd integer $s$ and each base $a$, $1 \leq a < s$, we define the following predicates:

1) $C_{\text{psp}}(s, a) = \langle s$ is not an $a$-psp $\rangle$,
2) $C_{\text{MR}}(s, a) = \langle s$ has not the property MR for $a$ $\rangle$,
3) $C_{\text{strong}}(s, a) = \langle s$ is not a strong $a$-psp $\rangle$,
4) $C_{\text{Euler}}(s, a) = \langle s$ is not an Euler $a$-psp $\rangle$.

If $s$ is composite, then we denote the set $\{a|1 \leq a < s, C_{\text{test}}(s, a) \text{ holds}\}$ by $W_{\text{test}}(s)$. It is the set of witnesses of $s$'s compositeness. The following theorem summarizes the properties of these predicates and sets.

**Theorem 10.** For each odd integer $s$ and each base $a$, $1 \leq a < s$,

1) $C_{\text{psp}}(s, a) \Rightarrow C_{\text{Euler}}(s, a) \Rightarrow C_{\text{MR}}(s, a) \Rightarrow C_{\text{strong}}(s, a)$.
2) If any of these tests holds, then $s$ is composite.
3) If $s$ is composite, then

$$|W_{\text{psp}}(s)| \geq 0$$

(equality holds for Carmichael’s numbers),

$$|W_{\text{Euler}}(s)| > \frac{s-1}{2},$$

and

$$|W_{\text{MR}}(s)| = |W_{\text{strong}}(s)| > \frac{3}{4}(s-1).$$

**Proof.**

This theorem is a simple application of theorems 1, 4, 6 and 9. The bound on $|W_{\text{Euler}}(s)|$ is proved by Baratz and Monier (73).
The predicate \( C_{\text{Euler}}(s, a) \) is proposed by Solovay and Strassen\(^7\). Rabin uses \( C_{\text{MR}}(s, a) \). The equivalent predicate \( C_{\text{strong}}(s, a) \) is more convenient since it does not require the computation of a gcd.

### 7.2. Probabilistic primality tests

A probabilistic algorithm is based on a predicate \( C(s, a) \) defined for each odd integer \( s \) and each base \( a, 1 \leq a < s \). This predicate \( C(s, a) \) will have the following properties:

1) The number \( s \) is composite if and only if \( C(s, a) \) holds for some \( a \).
2) The running time of a program which computes \( C(s, a) \) is short, i.e. bounded by a polynomial in \( \ln s \).
3) When \( s \) is composite, let \( L(s) \) be the set of integers \( a \) for which \( C(s, a) \) does not hold. Then \[ |L(s)|/(s-1) \leq \frac{1}{2}, \] i.e. at least half the \( a \)'s must be witnesses of \( s \)'s compositeness.

Such probabilistic algorithms have the following general form. To test whether \( s \) is prime, produce a sequence of \( k \) independent random integers \( \{a_i\} \), with \( 1 \leq a_i < s \). For each \( a_i \), check whether the predicate \( C(s, a_i) \) holds. If so, then \( s \) is composite, otherwise it is not certain that \( s \) is prime but we declare \( s \) to be prime with a probability at least equal to \( 1 - 2^{-k} \).

The probabilistic primality tests of Solovay-Strassen\(^7\) and Miller-Rabin\(^6\,\!^7\,\!^8\) have this form with the use of the predicates \( C_{\text{Euler}}(s, a) \) and \( C_{\text{MR}}(s, a) \) respectively. Rabin proposes a value between 10 and 30 for \( k \).

### 7.3. Use of strong a-psp notion for small calculators

An easy primality test suitable for use on a small calculator consists in just verifying the (strong) pseudoprimitivity and then using a table of composite (strong) pseudoprimes.

Lehmer\(^7\), Norman\(^8\) and Poulet\(^9\) have constructed tables containing the composite 2-psp's up to 100000000. These tables are very lengthy.

On the other hand, Pomerance, Selfridge and Wagstaff\(^\) find, after performing exhaustive computations, that the smallest composite \( a \)-psp is

\[
N_1 = 2047 = 23 \cdot 89, \quad \text{for} \ a = 2, \\
N_2 = 1373 \, 653 = 829 \cdot 1657, \quad \text{for} \ a = 2 \text{ and } 3, \\
N_3 = 25 \, 326 \, 001 = 2 \, 251 \cdot 11 \, 251, \quad \text{for} \ a = 2, 3 \text{ and } 5, \\
N_6 = 3 \, 215 \, 031 \, 751 = 151 \cdot 751 \cdot 28 \, 351, \quad \text{for} \ a = 2, 3, 5 \text{ and } 7.
\]

Only \( N_3, N_4 = 161 \, 304 \, 001 = 7 \, 333 \cdot 21 \, 997 \) and \( N_6 = 960 \, 946 \, 321 = 11 \, 717 \cdot 82 \, 013 \) are composite strong 2, 3, 5-psp and \( < 10^9 \). The number \( N_6 \) is the only composite strong \( a \)-psp for \( a = 2, 3, 5, 7 \) which does not exceed \( 2.5 \cdot 10^{10} \).
An introduction to fast generation of large prime numbers

Using this last idea Monier (appendix) describes a program for the pocket calculator HP-41C: each number $< 10^9$ is tested for primality in less than two minutes.

8. Primality tests

We present here the results which are of interest for generating large numbers for cryptographic applications, based on the theorems of Brillhart, Lehmer and Selfridge.

Let us recall that a number $s$, which is a candidate for primality, is of the form $s = kF + 1$, where $F$ is a large even number, $k$ is very small in comparison with $s$ and $F$. The primality tests we have selected allow us to establish constraints on $F$ so as to improve the efficiency of the algorithms for generating prime numbers.

The contents of this section are as follows. The first part contains theorems in which $s - 1$ is assumed to be completely factored. The second part contains theorems which use only partial factorizations of $s - 1$. All these theorems are based on the following converse of Fermat's theorem.

**Theorem 11.** (see Carmichael, p.55). If there exists an integer $a$ such that $a^{s-1} \equiv 1 \pmod{s}$ and if further there does not exist an integer $v$ less than $s - 1$ such that $a^v \equiv 1 \pmod{s}$, then the integer $s$ is a prime number.

8.1. Theorems requiring a complete factorization of $s - 1$

The main theorem Brillhart used for primality testing is due to Lehmer.

**Theorem 12.** If there exists an $a$ such that $a^{s-1} \equiv 1 \pmod{s}$ but $a^{(s-1)/p} \not\equiv 1 \pmod{s}$ for every prime divisor $p$ of $s - 1$, then $s$ is prime.

However it is difficult to find a small base $a$ for which all the hypotheses of theorem 12 are satisfied. Selfridge observed that these hypotheses can be released to allow a change of base, if needed, for each prime factor of $s - 1$.

**Theorem 13.** Let $s - 1 = \prod p_i^{q_i}$, where the $p_i$'s are primes. If for each $p_i$ there exists an $a_i$ such that $s$ is an $a_i$-psp but $a_i^{(s-1)/p_i} \not\equiv 1 \pmod{s}$, then $s$ is prime.

**Proof.**

Let $e_i$ be the order of $a_i \pmod{s}$. The hypotheses imply $e_i | s - 1$ but $e_i \not| (s - 1)/p_i$. Hence $p_i^{q_i} | e_i$. But, for each $i$, $e_i | \phi(s)$, so that $p_i^{q_i} | \phi(s)$, that is $(s - 1) | \phi(s)$. Hence $s$ is prime.

To illustrate theorem 13 we note that the primality of

$s = (2^{104} + 1)/257 = 78\, 919\, 881\, 726\, 271\, 091\, 143\, 763\, 623\, 681$

where $s - 1 = 2^8 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 97 \cdot 193 \cdot 241 \cdot 673 \cdot 65\, 537 \cdot 22\, 253\, 377$ can be decided with $a = 3$ for $p = 3, 5, 13, 17, 97, 193, 241, 673, 65\, 537$ and 22\, 253\, 377, and with $a = 7$ for $p = 7$ and with $a = 11$ for $p = 2$ (see Brillhart and Selfridge).

For each $i$, the average number of $a_i$'s satisfying $a_i^{s-1} \equiv 1 \pmod{s}$ and $a_i^{(s-1)/p_i} \neq 1 \pmod{s}$ is $(1 - 1/p_i) (s - 1)$ if $s$ is prime. In the next theorem, the condition $a^{(s-1)/2} \equiv 1 \pmod{s}$ is used for showing that $s$ is an $a$-psp.

**Theorem 14.** Let $s - 1 = \prod p_i^{e_i}$, where the $p_i$'s are primes. If for each $p_i$ there exists an $a_i$ such that $a_i^{(s-1)/2} \equiv -1 \pmod{s}$ but, for $p_i > 2$, $a_i^{(s-1)/2p_i} \neq -1 \pmod{s}$, then $s$ is prime.

**Proof.**

Let us assume $a_i^{(s-1)/2} \equiv -1 \pmod{s}$ and let $a_i^{(s-1)/2p_i} \equiv b_i \neq -1 \pmod{s}$. Indeed we have $-1 \equiv a_i^{(s-1)/2} \equiv b_i^{p_i} \pmod{s}$, which if $b_i^2 \equiv 1 \pmod{s}$ would imply, since $p_i$ is odd, $-1 \equiv b_i^{p_i} \equiv b_i \pmod{s}$, in contradiction with the second hypothesis. Hence, by theorem 13, $s$ is prime.

This theorem is an improvement over theorem 13 in that less calculation is required to complete the primality test. However, for each $i$, the number of $a_i$'s satisfying $a_i^{(s-1)/2} \equiv -1 \pmod{s}$ and $a_i^{(s-1)/2p_i} \neq -1 \pmod{s}$ is only $(1 - 1/PI) (s - 1)$ if $s$ is prime.

Let us remark the uncomplicated nature of these two theorems. A single program can be written to carry out the primality testing without requiring much memory space. Such a program, however, requires more running time than that based on the partial factorization of $s - 1$.

### 8.2. Theorems only requiring a partial factorization of $s - 1$

In the special case where a prime factor $p$ of $s - 1$ exceeds $s^{1/2}$, the next theorem provides a primality test involving less computation than theorem 14. Only one successful choice of a base $a$ for which the hypothesis relative to $p$ holds is necessary to conclude that $s$ is prime. The other prime factors of $s - 1$ may be ignored.

**Theorem 15.** Let $s - 1 = mp$, where $p$ is an odd prime such that $2p + 1 > p^{1/2}$. If there exists an $a$ for which $a^{(s-1)/2} \equiv -1 \pmod{s}$ but $a^{(s-1)/2p} \equiv -1 \pmod{s}$, then $s$ is prime.

**Proof.**

Let $e$ be the order of $a$ modulo $s$. From $a^{s-1} \equiv 1 \pmod{s}$ and $a^{(s-1)/p} \neq 1 \pmod{s}$, we conclude $p | e$, whence $p | \phi(s)$, since $e | \phi(s)$. But $\phi(s) | s \prod (q_i - 1)$, where the $q_i$'s are the different prime factors of $s$ and $s = mp + 1$. So $p | \prod (q_i - 1)$, that is, $p | (q_i - 1)$ for some $i$, say $p | (q_1 - 1)$. Thus $q_1 \equiv 1 \pmod{2p}$, and since $s \equiv 1 \pmod{2p}$ too, we have $s/q_1 \equiv 1 \pmod{2p}$. On the other hand, since $q_1 \equiv 1 \pmod{2p}$, we have $q_1 \geq 2p + 1 > s^{1/2}$, from which it follows that $1 \leq s/q_1 < s^{1/2} > 2p + 1$. Therefore, since $s/q_1 \equiv 1 \pmod{2p}$, the only possibility for $s/q_1$ is 1, and so $s$ is prime.

Let us note that the number of $a$'s for which the hypotheses hold is
An introduction to fast generation of large prime numbers

(\frac{1}{2} - \frac{1}{2}p)(s-1), if s is prime.

Throughout the rest of this section the notation \( s-1 = F_1 R_1 \) will be used, where \( F_1 \) is the even factored portion of \( s \) and \( R_1 \) is relatively prime with \( F_1 \).

Let us mention the following version of Pocklington’s theorem which will be helpful for proving theorem 17.

**Theorem 16.** If, for each prime \( p_i \) dividing \( F_1 \), there exists an \( a_i \) such that \( s \) is an \( a_i \)-psp and \( \gcd(a_i^{(s-1)/p_i} - 1, s) = 1 \), then each prime divisor of \( s \) is \( \equiv 1 \pmod{F_1} \).

We present now another theorem, which is superior to theorem 13 in that it requires only that the factored portion \( F_1 \) exceeds \( (s/2)^{\frac{1}{2}} \).

**Theorem 17.** Assume that, for each prime \( p_i \) dividing \( F_1 \), there exists an \( a_i \) such that \( s \) is an \( a_i \)-psp and

\[
\gcd(a_i^{(s-1)/p_i} - 1, s) = 1. \tag{8}
\]

Let there be given a positive integer \( m \) such that \( \lambda F_1 + 1 \geq s \) for \( 1 \leq \lambda < m \). If

\[
s < (mF_1 + 1) [2F_1^2 + (r - m) F_1 + 1], \tag{9}
\]

where \( q \) and \( r \) are defined by \( R_1 = 2F_1 q + r, 1 \leq r < 2F_1 \), then \( s \) is prime if and only if \( q = 0 \) or \( r^2 - 8q \) is not a perfect square (note that \( r \neq 0 \) since \( R_1 \) is odd).

**Proof.**

The theorem will be proven in the following form: \( s \) is composite if and only if \( q \neq 0 \) and \( r^2 - 8q \) is a perfect square. First we prove the necessary condition. From the previous theorem all factors of \( s \) are \( \equiv 1 \pmod{F_1} \). Thus, since \( s \) is composite, we may write \( s = (cF_1 + 1)(dF_1 + 1) \) where \( c, d \geq m \) from the hypotheses, from which we obtain \( s - 1 = cdF_1^2 + (c + d) F_1 \), and thus \( R_1 = cdF_1 + (c + d) \). As \( F_1 \) is even and \( R_1 \) is odd, this implies that \( c + d \) is odd and so \( cd \) is even. From \( cdF_1 + (c + d) = R_1 = 2F_1 q + r \), we deduce \( c + d \equiv r \pmod{2F_1} \) and \( c + d - r \geq 0 \), since \( 1 \leq r < 2F_1 \). On the other hand, \( (c - m)(d - m) \geq 0 \) implies \( cd \geq m(c + d) - m^2 \), so that

\[
(mF_1 + 1) [2F_1^2 + (r - m) F_1 + 1] > s = (cF_1 + 1)(dF_1 + 1) = cdF_1^2 + (c + d) F_1 + 1 \geq [m(c + d) - m^2] F_1 + (c + d) F_1 + 1 = (mF_1 + 1) [(c + d) - m] F_1 + 1.
\]

Hence, \( 2F_1^2 + (r - m) F_1 + 1 > [(c + d) - m] F_1 + 1 \), that is, \( c + d - r < 2F_1 \). It follows that \( c + d = r \) and \( cd = 2q \). Thus \( q \neq 0 \) and \( r^2 - 8q = (c - d)^2 \).

We now prove the sufficient condition. Let \( r^2 - 8q = t^2 \). We simply calculate

\[
s = F_1 R_1 + 1
\]

\[
= F_1 (2F_1 q + r) + 1
\]

\[
= [(r^2 - t^2) F_1^2]/4 + rF_1 + 1
\]

\[
= [F_1 (r - t)/2 + 1] [F_1 (r + t)/2 + 1].
\]
Since $q \neq 0$, these two factors are $> 1$. Hence $s$ is composite.

We now discuss the advantages theorem 17 has for primality testing.

a) The number of prime factors $p_i$ of $s - 1$ which we must take into account in the hypotheses of theorem 17 is reduced to a minimum. From (9), $s - 1$ needs to be factored at most until $F_1 \geq (s/2)^k$. A further reduction is possible if $m$ is chosen to be $> 1$ and large enough for (9) to be satisfied. Let us indeed consider the right-hand side of (9) as a function $f(m)$ of the variable $m$. In the interval defined by $1 \leq m \leq F_1 + r/2$, the function $f(m)$ is increasing. Thus in any case $F_1$ must be sufficiently large so that $s < f(F_1 + r/2) = (F_1^2 + rF_1/2 + 1)^2$. The cost of this reduction is the time needed to calculate the trial division of $s$ by $\lambda F_1 + 1$ for $m - 1$ values of $\lambda$.

b) Let us now discuss the hypotheses (8). If $s$ is prime, they are identical to those given in theorem 13. Hence, if $s$ is prime, for each $i$ the average number of $a_i$'s satisfying (8) is $(1 - 1/p_i)(s - 1)$. Thus the larger the prime factors of $F_1$, the more efficient the primality test based on this theorem. However additional computation is required relative to these hypotheses. But this can be reduced to only one greatest common divisor computation: first, for each $i$, find an $a_i$ such that $a_i^{(s-1)/p_i} - 1 \equiv b_i \neq 0$ (mod $s$); then calculate the product $\prod b_i = c$ (mod $s$); and finally, if $c \neq 0$, compute $d = \gcd(c, s)$. If $c = 0$, then some $b_i$ has a prime factor in common with $s$ and so $s$ is composite; if $d \neq 1$, then $s$ is composite too.

c) As the authors have checked on several intervals, the last condition of theorem 17, namely $q = 0$ or $r^2 - 8q$ not a perfect square, does not seem to be very severe. If we denote by $T(R_1, R_2)$ the set $\{s = 2pR_1 + 1 | p = \text{one of the ten largest primes less than 1000000}, R \text{ an odd number such that } \gcd(p, R) = 1 \text{ and } R_1 \leq R \leq R_2\}$ then, by exhaustive computations, the following results appear: for the sets $T_1 (999999900001, 999999999999)$ and $T_2 (999999900001, 999999999999)$, the condition just mentioned is always satisfied, ($|T_1| + |T_2| = 899991$) and for the set $T_3 (9999999999999, 99999999999999)$, this condition is violated 9 times ($|T_3| = 450000$).

Many other computations give similar results.

From the analysis of the primality criteria above, it appears that some tests are more efficient than other when applied to the problem of generating large prime numbers. Let us recall that the integer $s$ tested for primality is defined to be of the form $s = kF + 1$, where $F$ is a random large even number. If the complete factorization of $F$ is known, the primality test based on theorem 17 is the most efficient. $F_1$ is then taken to be the minimum even portion of $F$ with sufficiently large prime factors so as to satisfy the hypotheses of theorem 17.

The efficiency of this primality test can still be improved, by requiring $F$ to be of the form $F = 2^n p^a R$, where $p$ is a large prime, $p^a$ is about $(s/2)^k$ and $R$
An introduction to fast generation of large prime numbers

is a random odd integer. Then it is sufficient to take $F_1 = 2^n p^a$. If by chance a prime factor of $F$ exceeds $(s^k - 1)/2$, then theorem 15 should be taken into account to test the primality of $s$.

Note added in proof (November 1982): Additional references are 105-113.

Acknowledgements

Thanks are due to J. C. Lagarias, A. Odlyzko, H. Williams, Ph. Delsarte and J.-M. Goethals for helpful comments.

Philips Research Laboratory Brussels, August 1982

REFERENCES


19) J. P. Buhler, R. E. Crandall and M. A. Penk, Primes of the form $n! \pm 1$ and $2 \cdot 3 \cdot 5 \cdot \ldots \cdot p \pm 1$, Math. Comp. 38, pp. 639-643, 1982.


C. Couvreur and J. J. Quisquater


23) R. D. Carmichael, On composite numbers \(P\) which satisfy the Fermat congruence \(a^{P-1} \equiv 1 \pmod{P}\), Amer. Math. Monthly 19, pp. 22-27, 1912.


26) H. C. Williams and J. S. Judd, Determination of the primality of \(N\) by using factors of \(N^2 \pm 1\), Math. Comp. 30, pp. 157-172, 1976.


29) J. Bohman, Some computational results regarding the prime numbers below 200000000, BIT 13, pp. 242-244, 1973.


38) C. Bays and R. H. Hudson, Details of the first region of integers \(x\) with \(\pi_{3,2}(x) < \pi_{3,1}(x)\), Math. Comp. 32, pp. 571-576, 1978.


42) S. Weintraub, Distribution of primes between \(10^4\) and \(10^4 + 10^4\), Math. Comp. 26, p. 596 (UMT 27), 1972.


An introduction to fast generation of large prime numbers


64) P. Pritchard, A sublinear additive sieve for finding prime numbers, C. ACM 24, pp. 18-23, 1980.


74) L. Schoenfeld, Sharper bounds for the Chebyshev functions $\psi(x)$ and $\varphi(x)$, II. Math. Comp. 30, pp. 337-360, 1976.


85) Cipolla, Annali di Mat. 3, pp. 139-160, 1903.


87) S. Sipserov, Sobre los numeros pseudo-primos, Boletin Matematico 14, pp. 99-106, 1941.


91) J. D. Swift, Table of Carmichael numbers to $10^9$, Math. Comp. 29, pp. 338-339 (UMT 13), 1975.


C. Couvreur and J. J. Quisquater

111) G. Robin, Estimation de la fonction de Tchebychef $\theta$ sur le $k$ème nombre premier et grandes valeurs de le fonction $\omega(n)$, nombre de diviseurs premiers de $N$, Acta Arithmetica, to appear, 1983.