Nonlinear Analysis: Modelling and Control, 2004, Vol. 9, No. 2, 171–184

Recent Breakthrough in Primality Testing

R. Šleževičienė, J. Steuding, S. Turskienė

Department of Computer Science, Faculty of Physics and Mathematics
Šiauliai University, Višinskio st. 19, 77156 Šiauliai, Lithuania
office.ik@fm.su.lt

Received: 19.12.2003
Accepted: 27.01.2004

Abstract. This paper briefly surveys the history of primality tests. The recently discovered deterministic polynomial time primality test due to Agrawal, Kayal and Saxena is presented and some improvements are shortly discussed.

Keywords: primality tests, polynomial time, $\mathcal{P}$ and $\mathcal{NP}$.

AMS classifications: 11A51, 11A41.

1 Prime numbers and their global distribution

Prime numbers are rather old objects in mathematics, however, they did not loose their fascination and importance. Invented by the ancient Greek in analogy to the *indivisible* atoms in physics, primes are the multiplicative atoms of the integers. Their properties are studied in number theory but they occur in many other subfields of mathematics. In the last decades prime numbers entered the real world in many applications, e.g. as generator for keys in modern cryptographical algorithms.

An integer $n > 1$ is called prime if it has no other positive divisors than 1 and itself (within the set of integers); otherwise n is said to be composite. Every integer has a unique factorization into powers of distinct prime numbers. Euclid was the first who proved that there are infinitely many primes. His simple proof is now taught at school: if $p_1, \ldots, p_m$ are prime, then the number

$$q := p_1 \cdot \ldots \cdot p_m + 1$$

is not divisible by any of the p_j's. Thus q has a prime divisor different from $p_1, \ldots, p_m$ (which can be q itself). This construction of a *new* prime number out of an arbitrary finite collection of given primes implies the infinitude of prime numbers. For other, partially astonishing proofs of this basic fact we refer to [7].

The celebrated prime number theorem gives information how the primes are distributed. On the first view the prime numbers seem to appear in the sequence of positive integers without any visible rule. However, as conjectured about two hundred years ago by Gauss (at the early age of 17) and first proved about hundred years ago by Hadamard and de la Vallée-Poussin (independently) on the base of outstanding contributions due to Riemann, they satisfy a distribution law. Roughly speaking, the number $\pi(x)$ of primes less than or equal to x is

$$\pi(x) = \int_2^x \frac{du}{\log u} + \text{error term}; \tag{1}$$

the appearing logarithmic integral is asymptotically equal to $x/\log x$, where $\log x$ is here and in the sequel the natural logarithm. The error term in the prime number theorem is small in comparison with $x/\log x$ and is closely related to the zero distribution of the Riemann zeta-function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}, \tag{2}$$

where s has to be regarded as a complex variable and the product is taken over all primes; the series, and so the product, converges absolutely for $\operatorname{Re} s > 1$. The identity between the series and the product is nothing else than the analytic version of the unique factorization of integers, and provides another proof for the existence of infinitely many prime numbers which is due to Euler: assuming that there are only finitely many primes, the product converges throughout the complex plane, contradicting the fact that the series reduces for $s = 1$ to the divergent harmonic series.

The Riemann hypothesis claims that the complex zeros of $\zeta(s)$ all lie on the so-called critical line $\operatorname{Re} s = 1/2$ in the complex plane. This famous conjecture was stated by Riemann in 1859 and is still unproved. Its

value for mathematics is outstanding and so it is one of the seven millenium problems for which the Clay Institute awarded 1 million US-Dollars (see `http://www.claymath.org/Millennium_Prize_Problems/`). If the Riemann hypothesis is true, the error term in the prime number theorem is as small as possible, namely $\sim x^{1/2}\log x$, and so the prime numbers are distributed as uniformly as possible! For details on this fascinating link between elementary number theory and complex analysis we refer once more to [7].

2 The local decision problem: prime or not prime?

It is easy to check that 97 is prime and 99 is not, but it seems much harder to answer the same question for the numbers $10\,000\,000\,000\,097$ and $10\,000\,000\,000\,099$, at least in the same time. Indeed, a fundamental problem in number theory is the decision problem

Primes: *given a positive integer n, decide whether n is prime or not!*

This problem became very important by developments in cryptography in the late 1970s. It is easy to multiply two large prime numbers but it is much harder to factor a given large integer; at least there are no factoring algorithms of *satisfying* speed known so far. This simple observation led to so-called public key-cryptosystems where the key, a large integer N of about two hundred digits, is public knowledge (as the telephone number) but its prime factorization is the secret of its owner. This idea is attackable if N splits into small primes, but if N is the product of two (carefully chosen) primes with about hundred digits, the factorization of N is a nearly unsolvable task with present day computers; for more details we refer to [4]. For generating such keys one needs to find *large* prime numbers or, in other words, one needs to have a *fast* primality test, where *fast* means that the running time depending on the size of the number to be tested is *small*. Notice that a factoring algorithm and a primality test are different things: a number n can fail a primality test and the test does not tell us any of its divisors, whereas a factoring algorithm gives the complete factorization of n.

One of the first ideas for testing a given number n of being prime might be trial division, i.e., to try all positive integers $\leq \sqrt{n}$ whether they divide n

or not. Obviously, if there is no divisor of n among them, then n is prime. This strategy is not very useful if n is *large*. For example, it would take about 10^{50} arithmetic operations to test an integer with 100 digits; if now 10^{10} operations can be performed by a computer within one second, then this test would take about 10^{40} seconds which is still much more than 12 billion years, the estimated age of the Universe. However, hypothetical quantum computers, that are computers which compute with quantum states, if once realized, would solve this factorization problem within a fraction of a second (see `http://www.qubit.org/library/intros/cryptana.html` for more information). The simple idea of trial division leads to the sieve of Eratosthenes (due to the ancient greek Eratosthenes who was the first to measure approximately the circumference of the Earth 250 B.C.). If one deletes out of a list of integers $1 < n \leq x$ all multiples n of the primes $p \leq \sqrt{x}$, then only the prime numbers in between $\sqrt{x}$ and x remain. This gives a list of all primes under a given magnitude (and this is up to slight refinements still the best algorithm for this aim). Moreover, we obtain the factorizations of *all* integers in the list. For a primality test, this is a lot of superfluous information and we might ask for faster algorithms for detecting primes.

For numbers of special shape primality tests of satisfying speed are known for quite a long time. For instance, the Mersenne numbers, invented by the monk Mersenne in 1644, are defined by

$$M_p := 2^p - 1,$$

where $p \geq 3$ is prime; it is easily seen that composite exponents cannot produce primes of this form. In 1750 Euler corrected Mersenne's erroneous list of Mersenne prime numbers by use of the following criterion: if p is a prime number of the form $p = 4k + 3$, then $q = 2p + 1$ is a divisor of M_p if and only if q is prime; primes of the form $2p + 1$ for prime p are called Sophie Germain-primes (in honour for the French mathematician Sophie Germain and her work on Fermat's last theorem). For example, $M_{11} = 2047 = 23 \cdot 89$ is not prime as it was stated by Mersenne. In 1878 Lucas found a simple and *fast* primality test for Mersenne numbers (but only in 1935 Lehmer gave the first proof of the underlying mathematical theorem). His algorithm makes use of the congruence calculus. Given a positive integers n and arbitrary integers a

and b, we say that a is congruent to b modulo n and write

$$a \equiv b \bmod n$$

if n divides $a - b$. The set of integers b satisfying the above congruence forms the so-called residue class a modulo n, and we denote the smallest non-negative integer of this set by $a \bmod n$; this number is the remainder of any b from this residue class by division with n. With this notation the Lucas-Lehmer test can be described as follows:

Input: a prime $p \geq 3$. **Output:** M_p is PRIME or COMPOSITE.

1. Put $s = 4$.
2. For j from 3 to p do $s := s^2 - 2 \bmod M_p$.
3. If $s = 0$, return PRIME; otherwise return COMPOSITE.

A proof can be found in [4]. The first iterations (without reducing modulo M_p) are

$$s = 4 \quad \rightarrow \quad 14 = 2 \cdot \mathbf{7} \quad \rightarrow \quad 194 \quad \rightarrow \quad 37\,634 = 2 \cdot \mathbf{31} \cdot 607,$$

which yields the first two Mersenne primes $M_3 = 7$ and $M_5 = 31$. The *world record* among prime numbers, i.e., the largest known prime number, is a Mersenne prime, namely

$$M_{20\,996\,011} = 2^{20\,996\,011} - 1.$$

This number has more than six million digits and if these digits are typed in the size of this text, this world record would have a length of approximately 17 kilometers. This huge Mersenne prime was found by M. Shafer in November 2003 within the GIMPS-project (Great Internet Mersenne Prime Search); initiated by G. Woltman, GIMPS is a huge parallel computer connecting PCs and workstations worldwide via the internet (more details can be found under `http://www.mersenne.org`). It is an open question whether there are infinitely many Mersenne primes. With a bit heuristics we can be optimistic. We may interpret the prime number theorem (1) as follows: a positive integer n

is prime with probability $1/\log n$. Then the expectation value for the number of Mersenne primes M_p with $p \le x$ is

$$\sum_{p\le x} \frac{1}{\log(2^p-1)} \sim \frac{1}{\log 2} \sum_{p\le x} \frac{1}{p} \sim \frac{\log\log x}{\log 2},$$

which tends with x to infinity; the last asymptotic identity relies on taking the logarithm in (2). Note that this fits pretty well to the number of detected Mersenne primes.

3 Efficiency and Fermat's little theorem

First *general* primality tests superior to trial division (which actually is a factoring algorithm) were found rather late. One of the reasons might be that this question was not of striking importance in the early age of mathematics (which mainly was geometry and simple algebra). With the rise of number theory in the middle ages primality testing and factoring became fundamental problems in mathematics. Gauss wrote in his famous *disquisitiones arithmeticae* from 1801 (see [6], article 329):

> *"The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic (. . .). Nevertheless we must confess that all methods that have been proposed thus far are either restricted to very special cases or are so laborious and prolix that (. . .) these methods do not apply at all to larger numbers."*

About two hundred years before the computer age, this quotation points out the bottle neck of applying mathematics to the real world. Trial division yields the factorization of any integer after *some* time and thus it is the theoretical solution of the factoring problem. It works pretty well for *small* integers in particular, but it is hopeless if applied to integers with more than ten digits. The solution of a theoretical problem with respect to applications is only as good as its realization in practice!

For our later purpose we have to introduce a measure for *efficiency*. Roughly speaking, a primality test is *fast* if its running time is polynomial in the

input data. To be more precisely, we adopt now a bit from the language of complexity theory of computations. In computer science, the class $\mathcal{P}$ of problems solvable in polynomial time is of special interest. By definition, a decision problem P lies in the class $\mathcal{P}$ of polynomial time problems if there exists a polynomial p and an algorithm such that if any instance of P has input length $\leq m$, then the algorithm answers the question correctly in time $\leq p(m)$. Despite of its definition, it is a priori not clear that $\mathcal{P}$ is the class of problems which *in practice* can be solved rapidly. An algorithm with polynomial running time m^{100} is slowlier than another algorithm with exponential running time $\exp(m/10000)$ until m is greater than about ten million. However, experience shows that whenever an interesting problem was shown to be in $\mathcal{P}$, then there is also an algorithm for it whose running time is bounded by a *small* power of the input length. What is the input length in the decision problem Primes? In view of the binary expansion of integers,

$$n = a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + \ldots + a_m \cdot 2^m \qquad \text{with} \quad a_j \in \{0, 1\},$$

we need $m + 1 \leq C \log n$ bits to describe an integer n, where C is an absolute constant, independent of n. Thus, a primality test for n is of polynomial time if its running time is bounded by some absolute constant times a fixed power of $\log n$; we shall denote this by $O\left((\log n)^c\right)$.

If we are satisfied with a primality test which gives with a *high probability* the correct answer, then we can easily do better than trial division. Fermat's little theorem from 1640 states that if p is prime and a is not a multiple of p, then

$$a^{p-1} \equiv 1 \mod p. \tag{3}$$

For our later purpose, we shall have a closer look on Fermat's little theorem. The residue classes $a \bmod n$ obey a lot of algebraic structure, more precisely, they form a ring (that means roughly that they are closed under addition and multiplication) and we denote this ring traditionally by $\mathbb{Z}/n\mathbb{Z}$. If a is coprime with n, the residue class $a \bmod n$ possesses an inverse in $\mathbb{Z}/n\mathbb{Z}$ which can be found by solving (with the Euclidean algorithm) the linear diophantine equation

$$aX + nY = 1.$$

Such residue classes are called prime residue classes and they form the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$; its cardinality is denoted by $\varphi(n)$. The order of an element $a \in (\mathbb{Z}/n\mathbb{Z})^*$, denoted by $o_n(a)$, is the smallest positive integer k for which $a^k \equiv 1 \bmod n$. If there are no divisors of zero, the ring of residue classes has even more structure. The ring $\mathbb{Z}/n\mathbb{Z}$ is a field (which means that every non-zero element has a multiplicative inverse) if and only if n is prime. This can be regarded as a characterization of prime numbers but it does not give a practicable primality test. In this group-theoretical setting, Fermat's little theorem is nothing else than the statement that the order of each element of the multiplicative group of the finite field $\mathbb{Z}/p\mathbb{Z}$ is a divisor of $p-1$, the number of elements (resp. the order) of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$.

The converse implication of Fermat's little theorem is not true as the following example shows:

$$2^{340} \equiv 1 \bmod 341 \qquad \text{and} \qquad 341 = 11 \cdot 31.$$

But how can we quickly compute congruences with such big numbers? The trick is called fast exponentiation and works in the above example as follows: taking into account the binary expansion

$$340 = 1 \cdot 256 + 1 \cdot 64 + 1 \cdot 16 + 1 \cdot 4,$$

we may easily compute

$$\begin{aligned} 2^{340} = 2^{256} \cdot 2^{64} \cdot 2^{16} \cdot 2^4 &= 2^4 \cdot (2^4)^2 \cdot \left((2^4)^2\right)^2 \cdot \left(\left((2^4)^2\right)^2\right)^2 \\ &\equiv 16 \cdot 256 \cdot 64 \cdot 4 \mod 341 \end{aligned}$$

by iterating $(2^k)^2 \equiv (2^k \bmod 341)^2 \bmod 341$. Fast exponentiation uses only *small* integers, in our case non-negative integers < 341, and so the computation of congruences with powers is a simple task.

Composite numbers n for which

$$a^{n-1} \equiv 1 \mod n \tag{4}$$

holds true are called pseudoprimes to base a. Integers n that are pseudoprime for all bases $a \geq 2$, coprime with n, are called Carmichael numbers (after

their discoverer Carmichael in 1912); the first one is $561 = 3 \cdot 11 \cdot 17$, and there are infinitely many of them. Fortunately, Carmichael numbers do not appear too often if compared with primes (see [2]). Thus one can derive a *probabilistic* primality test from Fermat's little theorem as follows: an integer n is with a *high probability* prime if (4) holds for $1 \leq a \leq m$, where $m < n$ is a parameter; note that increasing m gives a higher probability for n being prime. In view of fast exponentiation this is a *fast* algorithm for generating prime candidates for public keys in cryptosystems. However, once found such a candidate for being prime, often we need a *deterministic* primality test, i.e., a test which gives the *correct* answer whether a given integer n is prime or not, and not only an answer which is *very likely correct*.

In the 1970s Miller found a primality test in polynomial time under assumption of the truth of the unproved Riemann hypothesis (more precisely, of the analogue of the Riemann hypothesis for Dirichlet L-functions). Miller's test is based on an extension of Fermat's little theorem. If one is not willing to accept any conditional result, there is the Jacobi sum test which has a running time

$$O\left((\log n)^{c \log\log n}\right),$$

where c is a positive absolute constant; the exponent is tending so slowly with n to infinity, that this running time is *nearly* polynomial for the range of numbers with which humans compute. For more details concerning these tests we refer to [4].

4 Recent breakthrough: the AKS-algorithm

It was an unexpected breakthrough when the Indian computer scientist Agrawal together with his students Kayal and Saxena published in August 2002 online a preprint [1] entitled 'Primes *is in* $\mathcal{P}$' in which they gave a first deterministic primality test in polynomial time without assuming any unproven hypothesis. Surprisingly, the test and its mathematical proof are quite simple.

The main idea of this new primality test, the so-called AKS-algorithm, is the following extension of Fermat's little theorem to polynomials: a positive

integer $n > 1$ is prime if and only if

$$(x+1)^n = x^n + 1 \tag{5}$$

in the ring of polynomials with coefficients from $\mathbb{Z}/n\mathbb{Z}$. For example, the Carmichael number $n = 561$ leads to the polynomial

$$(x+1)^{561} = x^{561} + \ldots + 51x^{11} + \ldots + 1 \mod 561.$$

The proof of (5) is rather simple and makes only use of Fermat's little theorem (3) and divisibility properties of binomial coefficients. However, this characterization would not give a polynomial time primality test since for testing n one has to compute about n coefficients for the polynomial on the left hand side of (5). It was the ingenious idea of Agrawal and his students to replace the polynomial identity (5) by a set of *weaker* congruences

$$(x-a)^n \equiv x^n - a \mod (n, x^r - 1), \tag{6}$$

where the a's have to be small residue classes modulo n and the r is a small positive integer. However, to assure that switching from the polynomial identity (5) to the set of congruences (6) still yields a characterization of prime numbers, one has to consider quite many a's and r's. On the contrary, these congruences can be checked much faster than (5) since it suffices to compute with polynomials of degree $\leq 2r$. The right balance leads to a deterministic primality test with polynomial running time.

Theorem 1 (Agrawal, Kayal, Saxena). *Let s, n be positive integers. Suppose that q and r are primes such that q divides $r-1$, $n^{(r-1)/q} \not\equiv 0, 1 \bmod r$, and*

$$\binom{q+s-1}{s} \geq n^{2[\sqrt{r}]}.$$

If for all $1 \leq a < s$, a coprime with n, the congruence (5) holds to be true, then n is a prime power.

We give a sketch of proof following Bernstein's shortened argument [3]. Let p be a prime divisor of n. Consider numbers of the form $t_k = n^{i_k} p^{j_k}$ with $0 \leq i_k, j_k \leq [\sqrt{r}]$, where, as usual, $[x]$ denotes the largest integer $\leq x$. The

pigeonhole principle shows that at least two distinct pairs of exponents (i_k, j_k) lead to numbers t_k lying in the same residue class modulo r. Without loss of generality,

$$t_1 \equiv t_2 \mod r. \tag{7}$$

Fermat's little theorem (3) implies that

$$(x-a)^{t_k} \equiv x^{t_k} - a \mod (p, x^r - 1)$$

holds for all $1 \leq a \leq p$ and $k = 1, 2$. In view of (7) $x^r - 1$ divides $x^{t_1} - x^{t_2}$, and thus

$$(x-a)^{t_1} \equiv x^{t_2} - a \mod (p, x^r - 1).$$

It follows that $g^{t_1} = g^{t_2}$ for all elements g of the multiplicative subgroup G generated by the linear factors $(\zeta_r - a)$ inside the cyclotomic field over $\mathbb{Z}/p\mathbb{Z}$, generated by adjunction of the rth roots of unity ζ_r (this step needs some fundamentals from algebra). Consequently, $t_1 - t_2$ is a multiple of the group order of G. Since a is coprime with n, and since

$$p^{(r-1)/q} \not\equiv 0, 1 \mod n,$$

G has at least $\binom{q+s-1}{s}$ elements (this step requires some elementary number theory). In view of the condition of the theorem

$$|t_1 - t_2| < (np)^{[\sqrt{r}]} \leq n^{2[\sqrt{r}]} \leq \binom{q+s-1}{s}.$$

Since this is a lower bound for the group order of G, it follows that $t_1 = t_2$ which implies $n = p^m$ for some non-negative integer m. This is the assertion of the theorem.

How does this theorem lead to a fast primality test? By some kind of Newton iteration one can check in polynomial time whether a given integer is a power of an integer. The congruence (5) can be tested by Fast Fourier transformation arithmetic in $\tilde{O}\left(sr(\log n)^2\right)$ steps; the notation $\tilde{O}$ incorporates further logarithmic factors in s, r and $\log n$. If now the quantities s and r in the Theorem of Agrawal et al. can be chosen as being bounded by some power

of $\log n$, we get a primality test with polynomial running time. By Stirling's formula it turns out that the hypothetical prime divisor q of $r-1$ is at least $c[\sqrt{r}]\log n$, where c is an absolute constant depending on s. The existence of such large prime divisors of integers of the shape $p-1$ follows from a deep theorem of Fouvry [5] (which became famous by its applications to Fermat's last theorem, before Wiles' final proof). Roughly speaking, Fouvry's result states that there are *many* primes r such that $r-1$ has a sufficiently large prime divisor; more precisely, there is a set of prime numbers r with positive density such that the largest prime divisor q of $r-1$ satisfies $q \geq r^{0.6687}$. The proof relies on advanced sieve methods. However, Hendrik Lenstra replaced the use of Fouvry's theorem by a tricky but elementary argument which we do not give here. According to the improvements by Lenstra and others, the AKS-algorithm has now the following form:

Input: an integer $n > 1$. **Output:** n is PRIME or COMPOSITE.

1. Test whether n is a prime power.
2. Find the smallest r such that the order $o_r(n)$ of $n \bmod r$ is greater than $4(\log n)^2$.
3. Test whether n has prime divisors $\leq r$.
4. If $n \leq r$, then return PRIME.
5. Test (6) for all $1 \leq a \leq 2\sqrt{\varphi(r)}\log n$.
6. If n survived all tests, then return PRIME; otherwise return COMPOSITE.

(Several implementations of this or related algorithms can be found under `http://fatphil.org/maths/AKS/`.) This primality test has a running time of $O\left((\log n)^{12}\right)$. Lenstra and Pomerance are working on refined faster versions of the new ideas of Agrawal and his collaborators (e.g. polynomials different from x^r-1); so far, they succeeded in the estimate $O\left((\log n)^{7.5}\right)$ for the running time. With some heuristics on the distribution of Sophie Germain-primes, which brings analytic number theory back into the game, the running time is expected to be $O\left((\log n)^3\right)$ (but a proof seems to be as hard as a proof

of the twin prime conjecture on the existence of infinitely many pairs of prime numbers $p, p+2$). For a discussion of the progress made since the appearance of the original AKS-algorithm we refer to the survey paper by Bernstein [3]).

5 $\mathcal{P} \neq \mathcal{NP}$?

In view of the primality test of Agrawal and his students it follows that the decision problem $\mathsf{Primes} \in \mathcal{P}$. On the other side, the integer factoring problem,

Factoring: *given an integer N, find the prime factzorization of N,*

is not expected to lie in $\mathcal{P}$ but in $\mathcal{NP}$. The class $\mathcal{NP}$ is, roughly speaking, the class of decision problems having solutions that, once given, can be verified in polynomial time. By definition the classes $\mathcal{P}$ and $\mathcal{NP}$ seem to be quite different: solving a problem seems to be harder than verifying a given solution. In the language of prime numbers, it is rather difficult to factor a given large integer, e.g.,

$$N = 10\,000\,000\,000\,097,$$

into its prime divisors, but it is easy to check whether or not

$$811 \cdot 12\,330\,456\,227$$

is the prime factorization of N. Once the factorization of an integer is produced by some factoring algorithm, we can use the AKS-algorithm to test its factors on primality in polynomial time. This shows that $\mathsf{Factoring} \in \mathcal{NP}$. It is widely expected that Factoring does not lie in $\mathcal{P}$; we already mentioned in Section 2 that public key-cryptography relies in the main part on this belief (however, this is not true for hypothetical quantum computers). Surprisingly, it seems to be rather difficult to find an example which is a member of $\mathcal{NP}$ but not of $\mathcal{P}$. Moreover, it is an open problem to prove (or disprove) $\mathcal{P} \neq \mathcal{NP}$. This fundamental conjecture in theoretical computer science is another millenium problem (see `http://www.claymath.org/Millennium_Prize_Problems/`).

We conclude our report on primes, primality testing and open problems with a nice quotation due to Paul Leyland who expressed his surprise about

the unexpected discovery of a simple deterministic polynomial time primality test by saying:

"Everyone is now wondering what else has been similarly overlooked."

References

1. Agrawal M., Kayal N., Saxena N. *Primes is in P,* available at `http://www.cse.iitk.ac.in/news/primality.html`
2. Alford W.R., Granville A., Pomerance C. "There are infinitely many Carmichael numbers", *Ann. of Math.*, **139**, p. 703–722, 1994
3. Bernstein D. *Proving primality after Agrawal-Kayal-Saxena,* available at `http://cr.yp.to/papers.html#aks`
4. Crandall R., Pomerance C. *Prime numbers – a computational perspective,* Springer 2001
5. Fouvry E. "Théorème de Brun-Titchmarsh; application à théorème de Fermat", *Inventiones*, **79**, p. 383–407, 1985
6. Gauss C.F. *Disquisitiones arithmeticae,* Yale University Press, New Haven, translated by A.A. Clarke, 1966
7. Ribbenboim P. *The new book of prime number records,* Springer, 3rd ed., 1996