PRIMALITY TESTS

By

Evangelos Kranakis[1]

Department of Computer Science

Yale University

New Haven CT, 06520

Technical Report 345, December 1984

---

[1]Research supported in part by the NSA under grant number MDA904 - 84 - H - 0004.

Contents

Frequently Used Notation

- $|A|$; the cardinal of the set A.
- $\bullet$; end of proof symbol.
- $\emptyset$; the empty set.
- $A \cup B, A \cap B, A - B$; the union, intersection and difference of the sets A, B.
- $f : A \longrightarrow B$; a mapping of a set A into a set B.
- $x \longrightarrow y$; the mapping carries the point x to the point y.
- $\exists, \forall, \Rightarrow, \Leftrightarrow$; there exists, for all, implies, if and only if.
- $x \equiv y \mod n$; x congruent to y modulo n.
- $(x|y)$; the Jacobi symbol of x with respect to y.
- $Z_n^* = \{x < n : \gcd(x, n) = 1\}$.
- $\varphi(n) = |Z_n^*|$; the Euler function.
- $\text{index}_{p,g}(n)$; the index of x with respect to $g \in Z_p^*$.
- $\lceil x \rceil, \lfloor x \rfloor, [x]$; ceiling of x, floor of x, integral part of x.
- $n! = 1 \cdot 2 \cdots n$; n factorial.
- $F_n = 2^{2^n} + 1$; n-th Fermat number.
- $M_p = 2^p - 1$; Mersenne number corresponding to the prime p.
- $\text{order}_m(x) =$ least $k \geq 0$ such that $x^k \equiv 1 \mod m$, where $x \in Z_m^*$.
- $\nu_m(t) =$ largest k such that $m^k | t$.
- ERH; the Extended Riemann Hypothesis.

PRIMALITY TESTS

By

Evangelos Kranakis

Department of Computer Science

Yale University

New Haven CT, 06520

1 Introduction

Prime numbers have fascinated the minds of mathematicians and amateurs alike for thousands of years. Unfortunately, research from its outset in ancient Greece to the 2nd World War was limited mostly to calculations done by hand. The advent of electronic computers has changed all this and has brought to the forefront the problem of how to efficiently test the primality of a given integer. In recent years, prime numbers as well as the ability to test the primality of a given integer efficiently has become very important for the construction of secure public key cryptosystems.

This paper is an attempt to give an account of recent work on Primality testing. The sieve of Eratosthenes (section 2) is still useful in listing all the primes less than or equal a given integer. Sections 3, 4 give two tests of theoretical significance; Wilson's and Lucas tests. In section 5 the number of steps needed to prove the primality of a given prime is studied. Sections 6, 7 and 8 study the primality of integers of specific forms, including Fermat and Mersenne numbers. The Extended Riemann Hypothesis (abbreviated ERH) is explained in 9. Sections 10, 11, 12 and 13 give three tests which prove that assuming ERH primality can be tested in polynomial time. Two probabilistic primality tests are given in sections 16 (Solovay - Strassen) and 17 (Rabin.) The test in section 14 is inspired from the tests based on ERH and is of practical value. The paper concludes with an account of the Rumeley - Adleman algorithm in section 18.

2 The Sieve of Eratosthenes

The sieve of Eratosthenes can be useful if one wants to determine all the primes less than or equal a given positive integer x, assuming that x is relatively small. To do this list all the numbers from 2 up to x in their natural order in the sequence

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, \ldots, x.$$

Starting from 2, the first prime in the above sequence, delete all the multiples $2m$ of 2 such that $2 < 2m \leq x$. The resulting sequence is

$$2, 3, 5, 7, 9, 11, 13, 15, \ldots, x.$$

Next, starting from 3, the next prime in the above sequence, delete all the multiples $3m$ of 3 such that $3 < 3m \leq x$. The resulting sequence is

$$2, 3, 5, 7, 11, 13, \ldots, x.$$

In general, if the resulting sequence at the $t-$th stage is

$$2, 3, 5, 7, 11, 13, \ldots, p, \ldots, x,$$

where p is the $t-$th prime, then delete all the multiples pm of p such that $p < pm \leq x$. Continue in this manner untill you exhaust all primes less than or equal to x. If at some stage in the course of this procedure a number k has dropped then k is composite, else it is prime. It is clear that the above procedure will give a list of all the primes less than or equal to x.

With minor alterations in the above procedure, it is easy to see that in order to get all the primes less than or equal to x one only needs to continue the process up to the t-th stage, where if p is the t-th prime then $p \leq \sqrt{x}$; moreover at the t-stage one need only delete all multiples pm such that $p^2 \leq pm \leq x$.

3 Wilson's Test

Theorem 3.1 *For any positive integer n the following are equivalent*

(1) n is prime

(2) $(n-1)! \equiv -1 \bmod n$.

Proof: Without loss of generality it can be assumed that $n > 2$.

$(1) \Rightarrow (2)$

For each $a \in Z_n^*$, the congruence $ax \equiv 1 \bmod n$ has a unique solution modulo n, say a^{-1} (here one uses the primality of n.) Since,

$$a^2 \equiv 1 \bmod n \Leftrightarrow a \equiv 1 \bmod n \text{ or } a \equiv (n-1) \bmod n,$$

it follows that the only fixed points of the mapping $a \rightarrow a^{-1}$ are the numbers $1, n-1$. Thus, one can write all the factors of the product $(n-1)! = 1 \cdot 2 \cdot 3 \cdots (n-1)$ (except for $1, n-1$) in pairs a, a^{-1}. It follows that $(n-1)! \equiv (n-1) \equiv -1 \bmod n$.

$(2) \Rightarrow (1)$

Assume on the contrary that n is composite. Let $n = ab$, where $a, b > 1$. Then it is clear that $a|(n-1)!$. Hence, by assumption $a|(n-1)$. But this is a contradiction since $a|n$•.

It appears that Wilson's test has only theoretical value. However it can be used to obtain a list of all the primes. Indeed, for each integer n let $r(n) =$ the remainder in the division of $(n-1)!$ by $n(n-1)/2$. It is clear that if n is composite then $r(n) = 0$. On the other hand if $n > 2$ is prime then by Wilson's theorem $n|(n-1)!+1$. It follows that $(n-1)/2|r(n)$, $n|r(n)+1$ and $r(n) < n(n-1)/2$. Hence there exist $s \geq 2$ and $t \geq 0$ such that $r(n) = s(n-1)/2$ and $r(n)+1 = tn$. It is now easy to see that $2tn = sn - s + 2$. This in turn implies $n|s-2$ and hence $r(n) = n-1$. Hence the following theorem has been proved (see [Di] page 428.)

Theorem 3.2 *(***Barinaga***)* $\{r(n)+1 : r(n) > 0\}$ *is exactly the set of odd prime numbers* •

4 Lucas Test

Theorem 4.1 *For any positive integer n the following are equivalent*

(1) n is prime

(2) There exists $g \in Z_n^*$ *such that* $g^{n-1} \equiv 1 \bmod n$, *but for all primes* $p|(n-1)$, $g^{(n-1)/p} \not\equiv 1 \bmod n$.

Proof: (1) $\Rightarrow$ (2)

If n is prime then it follows from the theorem of Gauss that the multiplicative group Z_n^* is cyclic. Let g be a generator of this group. It can be verified easily that the above g satisfies (2).

(2) $\Rightarrow$ (1)

Let g satisfy (2) and let m be the order of g in the group Z_n^* i.e. m = the least t such that $g^t \equiv 1 \bmod n$. Since, $g^{n-1} \equiv 1 \bmod n$, it follows that $m|(n-1)$. On the other hand, the second part of (2) implies that m cannot be a proper divisor of $n-1$. It follows that $m = n-1$. Further, the theorem of Euler-Fermat implies that $g^{\varphi(n)} \equiv 1 \bmod n$. Hence, $m = n-1|\varphi(n)$ and consequently $n-1 = \varphi(n)$. It follows that n is prime •

Lucas test like Wilson's test does not provide any efficient algorthm to test the primality of a given integer n. However the following Corollary shows that if the factorization of $n-1$ is known then it can be used to test if a given $g \in Z_n^*$ generates the multiplicative group Z_n^*.

Theorem 4.2 *For any positive integer n and any* $g \in Z_n^*$ *the following are equivalent*

(1) g generates Z_n^*

(2) $g^{n-1} \equiv 1 \bmod n$ *and for all primes* $p|(n-1)$, $g^{(n-1)/p} \not\equiv 1 \bmod n$ •

5 Pratt's Test

Pratt's test is concerned with the number of steps needed to show that a given integer n is prime. Call (a, n), where n is a positive integer and $a \in Z_n^*$, **Fermat pair** if and only if $(a, n) = (1, 2)$ or $a \geq 2$ and $a^{n-1} \equiv 1 \bmod n$.

Example 5.1 *(1) If p is prime then (a, p) is a Fermat pair, for all $a \in Z_p^*$.*
(2) None of $(5, 12), (7, 12), (11, 12)$ is a Fermat pair.
(3) $(2, 341)$ is a Fermat pair, while $(3, 341)$ is not (see [Scha], page 118.)

Define a partial ordering $\prec$ on Fermat pairs by

$$(b, m) \prec (a, n) \Leftrightarrow m|(n-1) \text{ and } a^{(n-1)/m} \not\equiv 1 \bmod n$$

It is clear from the above definition of $\prec$ that there are no infinite $\prec$ descending sequences i.e. infinite sequences $(a_1, n_1), (a_2, n_2), \ldots, (a_k, n_k), \ldots$ such that

$$\cdots \prec (a_k, n_k) \prec \cdots \prec (a_1, n_1)$$

For such a partial ordering it makes sense to define for each Fermat pair (a, n) the rank of (a, n) by

$$\text{rank}(a, n) = \sup\{\text{rank}(b, m) + 1 : (b, m) \prec (a, n)\}.$$

Call a sequence $(a_1, n_1), \ldots, (a_k, n_k)$ of Fermat pairs, where $k > 1$, a **Pratt sequence for** the Fermat pair (a, n) if and only if for each $i = 1, \ldots, k$, $(a_i, n_i) \prec (a, n)$ and $n - 1 = n_1 \cdots n_k$.

For any set (possibly empty) S of Fermat pairs, let $\Gamma(S)$ denote the set of Fermat pairs (a, n) such that either (a, n) has no $\prec$ predecessor or else there exists a Pratt sequence $(a_1, n_1), \ldots, (a_k, n_k)$ for (a, n) such that for all $i = 1, \ldots, k$, $(a_i, n_i) \in S$. Finally, for each $t \geq 0$ let the sets $\Gamma^{<t}$ and Γ^t of Fermat pairs be defined by induction on t as follows

$$\Gamma^{<t} = \bigcup_{r<t} \Gamma^r \text{ and } \Gamma^t = \Gamma(\Gamma^{<t})$$

In addition, let

$$\Gamma^\infty = \bigcup_t \Gamma^t.$$

It is an immediate consequence of the definition that the operator Γ is monotone i.e. $S \subseteq S' \Rightarrow \Gamma(S) \subseteq \Gamma(S')$. Using this, and $\prec$ induction it can be shown easily that the sequence Γ^t satisfies the following properties:

1. $t < t' \Rightarrow \Gamma^t \subseteq \Gamma^{t'}$.
2. For all t, $\Gamma^t \subseteq \Gamma(\Gamma^t)$.

3. $\Gamma(\Gamma^\infty) = \Gamma^\infty$.

Theorem 5.1 *(Pratt) For any Fermat pair (a,n) the following are equivalent*
(1) $(a,n) \in \Gamma^\infty$.
(2) n is prime and a generates Z_n^*.

Proof: (1) $\Rightarrow$ (2)
It will be shown by induction on t that for all Fermat pairs (a,n)

$$(a,n) \in \Gamma^t \Rightarrow n \text{ is prime and } a \text{ generates } Z_n^*.$$

If $t = 0$ then it will be shown that $\Gamma^0 = \{(1,2)\}$. Indeed, let $(a,n) \in \Gamma^0$. By definition of Γ, (a,n) does not have an $\prec$ predecessor. If $n > 2$, then write $n-1 = p_1 \cdots p_k$, where $p_1, \ldots, p_k$ are primes. For each $i = 1, \ldots, k$, let a_i be a generator of $Z_{p_i}^*$. Then it is clear that $(a_i, p_i) \prec (a,n)$, which is a contradiction. Hence, $(a,n) = (1,2)$. In the general case $t > 0$, let $(a,n) \in \Gamma^t$. By definition of Γ^t, $(a,n) \in \Gamma(\bigcup_{r<t} \Gamma^r)$. Hence, there exists an $r < t$ and a Pratt sequence $(a_1,n_1), \ldots, (a_k,n_k)$ for (a,n) such that for all $i = 1, \ldots, k$, $(a_i,n_i) \in \Gamma^r$ and $n-1 = n_1 \cdots n_k$. It follows from the induction hypothesis that for each $i = 1, \ldots, k$, n_i is prime and a_i generates $Z_{n_i}^*$. Moreover, each $(a_i,n_i) \prec (a,n)$, and hence $a^{(n-1)/n_i} \not\equiv 1 \bmod n$. It follows from Lucas test that n is prime. In addition, a generates Z_n^*.
(2) $\Rightarrow$ (1)
This direction will be proved by induction on the rank of the Fermat pair (a,n). If $\text{rank}(a,n) = 0$ then (a,n) has no $\prec$ predecessor. Hence, as in the proof of (1) $\Rightarrow$ (2) it can be shown that $(a,n) = (1,2)$. In general, if $n > 2$ write $n-1 = p_1 \cdots p_k$, where $p_1, \ldots, p_k$ are primes. For each $i = 1, \ldots, k$, let a_i be a generator of $Z_{p_i}^*$. It is then clear that $(a_i,p_i) \prec (a,n)$, and hence $\text{rank}(a_i,p_i) < \text{rank}(a,n)$, for all $i = 1, \ldots, k$. It follows from the induction hypothesis that for all $i = 1, \ldots, k$, $(a_i,p_i) \in \Gamma^\infty$. Hence, $(a,n) \in \Gamma(\Gamma^\infty) = \Gamma^\infty$, and the proof of the theorem is complete •

Example 5.2 *Consider the Fermat pair* $(6,971)$. *Notice that* $971-1 = 2 \cdot 5 \cdot 97$, $97-1 = 2^5 \cdot 3$, $5-1 = 2^2$, $3-1 = 2$. *$\prec$ predecessors of* $(6,971)$ *are* $(1,2),(2,5),(5,97)$; *$\prec$ predecessors of* $(5,97)$ *are* $(1,2),(2,3)$; *the only $\prec$ predecessor of* $(2,5)$ *and* $(2,3)$ *is* $(1,2)$. *It is clear that* $\text{rank}(1,2) = 0$, $\text{rank}(2,3) = \text{rank}(2,5) = 1$, $\text{rank}(5,97) = 2$, $\text{rank}(6,971) = 3$. *Moreover,* $(6,971) \in \Gamma^3$.

For each Fermat pair $(a,n) \in \Gamma^\infty$ let

$$|a,n|_\Gamma = \text{ smallest } t \geq 0 \text{ such that } (a,n) \in \Gamma^t.$$

In the next result an upper bound of the quantity $|a,n|_\Gamma$ will be determined which depends only on n. Let $(a,n) \in \Gamma^\infty$. Then there exists a Pratt sequence $(a_1,n_1), \ldots, (a_k,n_k)$ for (a,n) such that $n-1 = n_1 \cdots n_k$ and

$$|a,n|_\Gamma = \max\{|a_i,n_i|_\Gamma + 1 : i = 1, \ldots, k\}.$$

It follows by induction that

$$|a,n|_\Gamma \leq \max\{\log_2 n_i + 1 : i = 1,\ldots,k\} \leq$$

$$\log_2(n_1 \cdots n_k) = \log_2(n-1) < \log_2 n$$

Thus, the following theorem has been proved

Theorem 5.2 *For any prime n and any generator a of Z_n^*, $|a,n|_\Gamma \leq \log_2 n$•*

An immediate consequence of the above results is also the following

Theorem 5.3 *For any integer $n > 1$ the following statements are equivalent*
(1) n is prime.
(2) $\exists a\,((a,n)$ is a Fermat pair and $(a,n) \in \Gamma^{\lfloor \log_2 n \rfloor})$ •

For each prime n let $\Pi(n)$ be the number of multiplications and exponentiations needed to prove the primality of n. The above theorem implies that if n is prime then $(a,n) \in \Gamma^t$, where $t = \lfloor \log_2 n \rfloor$. To test the primality of n write $n-1 = p_1 \cdots p_k$ and verify the following two properties:

1. each p_i is prime
2. $a^{(n-1)/p_i} \not\equiv 1 \bmod n$, for $i = 1,\ldots,k$.

It is now easy to show by induction that

$$\Pi(n) \leq 1 + 2k + \sum_{i=1}^{k} \Pi(p_i) \leq 1 + 2k + \sum_{i=1}^{r}(-2 + 3\log_2 p_i) \leq -2 + 3\log_2 n.$$

Hence it has been shown that

Theorem 5.4 *For any prime n the number of multiplications and exponentiations needed to prove the primality of n is at most $-2 + 3\log_2 n$•*

6 Proth's Test

This and the next two tests can be used to verify the primality of positive integers of specific forms. Proth's test is concerned with numbers of the form $k2^n + 1$. Its proof requires the following lemma.

Lemma 6.1 *(**Pocklington**) Let $n = ab + 1 > 1$, where $0 < a \leq b + 1$. Assume that for any prime divisor p of b there exists an integer x such that $x^{n-1} \equiv 1 \bmod n$ and $x^{(n-1)/p} \not\equiv 1 \bmod n$. Then n is prime.*

Proof: Assume on the contrary that n is not prime and let q be a prime factor of n which is $\leq \sqrt{n}$. By assumption, for every prime factor p of b there exists an integer x_p such that

$$\text{order}_q(x_p) | (n-1) \text{ and } \text{order}_q(x_p) \nmid \frac{n-1}{p}.$$

Let p^k be the largest power of the prime p such that $p^k | b$. Then $\text{order}_q(x_p) = sp^k$, for some integer s. Considering the prime factorization of b and using the last assertion one can find an integer x such that $\text{order}_q(x) = b$. It follows that $q - 1 \geq b$ and hence,

$$q^2 \geq (b+1)^2 \geq a(b+1) = ab + a \geq n.$$

In particular, $q^2 = n$, $a = 1$ and $a = b + 1$, which is a contradiction •

It is now easy to prove Proth's theorem.

Theorem 6.1 *(Proth) Assume* $3 \nmid k$, $k \leq 2^n + 1$ *and* $3 < 2^n + 1$. *Then the following statements are equivalent*

(1) $k2^n + 1$ *is prime.*

(2) $3^{k2^{n-1}} \equiv -1 \bmod(k2^n + 1)$.

Proof: (2) $\Rightarrow$ (1)

This is immediate from the previous lemma, with $a = k$, $b = 2^n + 1$.

(1) $\Rightarrow$ (2)

Using Euler's criterion, it is enough to show that 3 is a quadratic nonresidue modulo $k2^n + 1$. Since $3 \nmid k$, $k2^n + 1 \equiv 2 \bmod 3$. Hence,

$$(k2^n + 1 | 3) = (2|3) = -1.$$

Using the law of quadratic reciprocity one easily obtains that

$$(3 | k2^n + 1) = (-1)^{k2^{n-1}} \cdot (k2^n + 1 | 3) = -1 \bullet$$

7 Pepin's Test

Suppose that $2^n + 1$ is prime. It will be shown that $n = 2^m$, for some integer $m \geq 0$. Indeed, assume on the contrary that $n = k \cdot 2^m$, where k is odd > 1. Put $a = 2^{2^m}$. Then

$$2^n + 1 = a^k + 1 = (a+1)(a^{k-1} - a^{k-2} + a^{k-3} - \cdots + 1),$$

which contradicts the primality of $2^n + 1$.

For each $n \geq 0$, let the $n-$th **Fermat number** be defined by

$$F_n = 2^{2^n} + 1.$$

Pepin's test is used to verify the primality of Fermat numbers, and is an immediate consequence of Proth's theorem.

Theorem 7.1 *(**Pepin**) For each $n \geq 1$, the following are equivalent*
(1) F_n is prime.
(2) $3^{(F_n-1)/2} \equiv -1 \bmod F_n$.

Remark: Since for all $k \geq 0$, $F_{k+1} = F_0 \cdots F_k + 2$, the Fermat numbers are relatively prime to each other.

According to [Scha], page 80, [Wi], page 134, and [BLSTW], F_1, F_2, F_3, F_4 are primes, but all of $F_5, \ldots, F_{19}$, F_{21} are composite. The status of F_{20} is not known. Other Fermat composites, for $n \geq 23$ are listed in [Wi] . Moreover no other Fermat prime seems to be known.

8 Lucas-Lehmer Test

It is easy to show that if $2^n - 1$ is prime so is n. Indeed, assume on the contrary that $2^n - 1$ is prime but n is composite. Let $n = ab$ be two nontrivial factors of n and put $x = 2^a$. Then one can show that

$$2^n - 1 = x^b - 1 = (x-1)(x^{b-1} + x^{b-2} + \cdots + x + 1),$$

which is a contradiction.

The Lucas-Lehmer test can be used to determine the primality of the so called Mersenne integers i.e. integers of the form $2^p - 1$, where p is prime. For each prime p, let the Mersenne number corresponding to p be defined by

$$M_p = 2^p - 1.$$

The main result to be used in the proof of the Lucas-Lehmer test is the following lemma.

Lemma 8.1 *(**H. W. Lenstra**) Let A be a commutative ring with unit which includes Z_n as a subring. Let $s > 0$. Further assume that there exists an $\alpha \in A$ such that $\alpha^s = 1$ but for all prime $q|s$, $\alpha^{s/q} - 1$ is invertible in A. If for some integer $t > 0$,*

$$\prod_{i=0}^{t-1} \left(x - \alpha^{n^i}\right)$$

is a polynomial with coefficients in Z_n then for any $r|s$, there exists an i such that $r \equiv n^i \bmod s$.

Proof: Assume that the hypothesis of the lemma is true. Let r be a divisor of n. Without loss of generality it can be assumed that r is prime. Since $r|n$, $n = rk = 0$ and hence r is a zero divisor in A. Clearly, $I = \{x \in A : xk = 0\}$ is an ideal of A such that $r \in I$. Let M be a maximal ideal containing r and consider the field $B = A/M$. The hypothesis of the lemma implies that the multiplicative

order of $\beta \equiv \alpha \bmod M$ in B is exactly s (this is because no invertible element can belong to a maximal ideal.) By assumption, the polynomial

$$p(x) = \prod_{i=0}^{t-1} \left(x - \beta^{n^i}\right)$$

has coefficients in Z_n. Since, $r \equiv 0 \bmod M$ and $r|n$, it can also be assumed without loss of generality that $p(x) \in Z_r[x]$. Moreover, $p(\beta) = 0$. The mapping $x \rightarrow x^r$ is a homomorphism of B which leaves Z_r fixed. It follows that $p(\beta^r) = 0$, and hence $\beta^r = \beta^{n^i}$ for some $0 \leq i < t$. The rest of the proof follows from the fact that the multiplicative order of β in B is exactly s •

Define the sequence e_k by induction on k as follows

$$e_1 = 4 \text{ and } e_{k+1} = e_k^2 - 2.$$

Theorem 8.1 *(**Lucas-Lehmer**) For all $m > 2$ the following statements are equivalent*

(1) $M_m = 2^m - 1$ is prime.

(2) $e_{m-1} \equiv 0 \bmod M_m$.

Proof: (H. W. Lenstra) If $m = 2k$ is even then $M_m = 2^{2k} - 1 = 3(4^{k-1} + 4^{k-2} + \cdots + 1)$ and hence M_m is not prime. In addition, it can be shown by induction on $t > 2$ that $e_{t-1} \equiv -1 \bmod 3$. In particular, $e_{m-1} \not\equiv 0 \bmod M_m$ (since $3|M_m$.) Thus, without loss of generality it can be assumed that m is odd.

Put $n = M_m$ and consider the element $a \equiv 2^{(m+1)/2} \bmod n$ of Z_n^*. It is then clear that

$$a^2 \equiv 2^{m+1} \equiv (2^m - 1) + (2^m + 1) \equiv 2 \bmod n.$$

Consider the quotient ring

$$A = \frac{Z_n^*[x]}{(x^2 - ax - 1)},$$

where $(x^2 - ax - 1)$ is the ideal generated from the polynomial $x^2 - ax - 1$ and let α be the image of x in A. Since $x^2 - ax - 1$ is of degree 2 it is clear that

$$A = \{s + t\alpha : s, t \in Z_n^*\},\ \alpha^2 = a\alpha + 1.$$

It follows that $\beta = a - \alpha = -\alpha^{-1}$ is the other root of $x^2 - ax - 1$ in A. Moreover, $\alpha + \beta = a$ and $\alpha\beta = -1$. Using this and induction on $k \geq 1$ it follows that

$$\alpha^{2^k} + \beta^{2^k} \equiv e_k \bmod n. \tag{1}$$

Now the proof of the main theorem can be completed.

(1) $\Rightarrow$ (2)

Assume n is prime. It follows easily from $n = 2^m - 1$ that $n \equiv 1 \bmod 3$ and $n \equiv -1 \bmod 8$. Using the last two congruences and quadratic reciprocity it can be shown that $(2|n) = -(3|n) = 1$ and hence $(6|n) = -1$. Since the discriminant of the polynomial $x^2 - ax - 1$ is equal to 6 it follows that A is a quadratic field extension of Z_n^*. Moreover, α, β are conjugate over Z_n^*, being roots of the same polynomial. Considering the automorphism $x \rightarrow x^n$ it follows easily that $\alpha^n = \beta$. Thus, $\alpha^{n+1} = \alpha\beta = -1$ and $\beta^{2^{m-1}} = \alpha^{-2^{m-1}}$. It follows from equation (1) that

$$e_{m-1} \equiv \alpha^{2^{m-1}} + \beta^{2^{m-1}} = \alpha^{2^{m-1}} + \alpha^{-2^{m-1}} = 0 \bmod n.$$

(2) $\Rightarrow$ (1)
Since $e_{m-1} \equiv 0 \bmod n$, it follows from equation (1) that

$$\alpha^{2^m} \equiv -1 \bmod n \text{ and } \alpha^{2^{m+1}} \equiv 1 \bmod n.$$

The idea is to apply lemma 8.1 to $s = 2^{m+1}$ and the ring $A = Z_n$. The lemma applies because $\alpha^n = \beta$ and hence $x^2 - ax - 1 = (x - \alpha)(x - \alpha^n)$. It follows that for any $r|s$, there exists an i such that $r \equiv n^i \bmod s$. But $n^2 \equiv (2^m - 1)^2 \equiv 1 \bmod 2^{m+1}$. Hence, for every $r|n$, either $r \equiv 1 \bmod 2^{m+1}$ or $r \equiv n \bmod 2^{m+1}$. It follows that n is prime •

Remark 1: It is known that for all n, m, $\gcd(2^n - 1, 2^m - 1) = 2^{\gcd(n,m)} - 1$ (see [Scha] theorem 10.) Hence, the Mersenne numbers $\{M_p : p \text{ is prime }\}$ are relatively prime to each other.

Remark 2: A different proof of the Lucas - Lehmer test can be given using the so called **Lucas - Lehmer functions**, which for any two relatively prime integers p, q are defined as follows:

$$u_n(p,q) = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad v_n(p,q) = \alpha^n + \beta^n,$$

where α, β are the two roots of the quadratic $x^2 - px + q$ and $n \geq 0$. Many of the properties of the Lucas - Lehmer functions can be found in [Wi]. In section 4.5.4. of [Kn] the Lucas - Lehmer functions $u_n(4,1), v_n(4,1)$ are used to derive theorem 8.1 .

Remark 3: It is not known if there exist infinitely many Mersenne primes or infinitely many Mersenne composites. $M_2, M_3, M_5, M_7, M_{13}, M_{17}, M_{19}$ are primes. All the remaining Mersenne primes for $p < 50,000$ are given in the table of Figure 1 . In addition [BLSTW] states that for $p = 86,243$, $2^p - 1$ is prime.

9 Extended Riemann Hypothesis

Let C^* denote the multiplicative group of the field of complex numbers. A character modulo n is a function $\chi : Z_n^* \rightarrow C^*$ which is a group homomorphism

p with $2^p - 1$ prime	Discoverer	Year	Machine
19	Cataldi	1588	–
31	Euler	1722	–
61	Pervushin	1883	–
89	Powers	1911	–
107	Powers	1914	–
127	Lucas	1876	–
521 607 1,279 2,203 2,281	Lehmer – Robinson	1952	SWAC
3,217	Riesel	1957	BESK
4,253 4,423	Hurwitz – Selfridge	1961	IBM 7090
9,689 9,941 11,213	Gillies	1963	ILIAC 2
19,937	Tuckerman	1971	IBM 360
21,701	Nickel – Noll	1978	CYBER 174
23,209	Noll	1978	CYBER 174
44,497	Slowinsky – Nelson	1979	CRAY–1

Figure 1: Table of Mersenne Primes

between Z_n^*, C^*. For each modulo n, the trivial character χ_n is defined by $\chi_n(a) = 1$, for all $a \in Z_n^*$. Any character χ can be extended to a function $\chi' : Z^* \to C^*$ as follows:

$$\chi'(a) = \begin{cases} \chi(a \bmod n) & \text{if } \gcd(a,n) = 1 \\ 0 & \text{if } \gcd(a,n) \neq 1, \end{cases}$$

where $Z^* = \{n \in Z : n > 0\}$. For simplicity the same symbol will be used for χ, χ'.

For any character χ modulo n the Dirichlet L function corresponding to χ is a function L_χ with a complex variable z defined by the following infinite series:

$$L_\chi(z) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^z}.$$

Notice that if $\chi \neq \chi_1$ then by analytic continuation the function L_χ can be extended to a unique analytic function defined on the half plane $\Re(z) > 0$ e.g. see [KP] ($\Re(z)$ is the real part of the complex number z.) **The Riemann Hypothesis** for the L function L_χ, abbreviated $RH[L_\chi]$ is the statement: all the zeroes of the function L_χ in the critical strip $0 < \Re(z) \leq 1$ must lie on the line $\Re(z) = 1/2$. **The Extended Riemann Hypothesis**, abbreviated ERH is the statement: for all n and all characters χ modulo n, $RH[L_\chi]$ holds.

The following theorem will be essential in understanding the primality tests that follow (see [Mont] theorems 13.1 and 13.2.)

Theorem 9.1 *(Ankeny-Montgomery) There exists a constant $C > 0$ such that if χ is a nontrivial character modulo n and $RH[L_\chi]$ holds then there exists a prime $p < C \cdot (\log n)^2$ for which $\chi(p) \neq 1$•*

It is a well known result from the theory of finite abelian groups that every finite abelian group G is the direct product of cyclic groups, say $G_1, \ldots, G_r$ (see [Ku], part II, chapter VI.) For each $i = 1, \ldots, r$, put $e_i = |G_i|$ and let

$$\xi_i = \exp\left(\frac{2\pi i}{e_i}\right)$$

be an e_i-th root of unity. Clearly, each cyclic group G_i is isomorphic to the cyclic group $\{\xi_i^j : j = 0, \ldots, e_i - 1\}$. It follows that the group G can be embedded into the group C^*.

Let $f : Z_n^* \to G$ be a nontrivial abelian group homomorphism. The image $Im(Z_n^*)$ of Z_n^* under f is also an abelian group and as such it can be embedded into C^*; let $g : Im(G) \to C^*$ be the embedding thus defined and let χ be the modulo n character $g \circ f$. It is then clear that for any $a \in Z_n^*$, $\chi(a) \neq 1$ if and only if $f(a) \neq 1$.

As an immediate consequence of the above remarks and theorem 9.1 it can be shown that

Theorem 9.2 *(Assume ERH) There exists a constant $C > 0$ such that if χ is a nontrivial homomorphism $\chi : Z_n^* \to G$ between abelian groups then there exists a prime $p < C \cdot (\log n)^2$ for which $\chi(p) \neq 1$•*

10 Solovay-Strassen Deterministic Test

This test is based on the following theorem.

Theorem 10.1 *For any odd integer $n > 1$ the following statements are equivalent*

(1) n is prime

(2) $(\forall a \in Z_n^*)(a^{(n-1)/2} \equiv (a|n) \bmod n)$

Proof: (1) $\Rightarrow$ (2) is an immediate consequence of Euler's criterion. For each $a \in Z_m^*$ let the order of a modulo m, abbreviated $\text{order}_m(a)$, be the least nonegative integer t such that $a^t \equiv 1 \bmod m$. Call n **square free** if $(\forall p)(p|n \Rightarrow p^2 \not| n)$. To prove (2) $\Rightarrow$ (1) the following lemma will be used.

Lemma 10.1 *If $(\forall a \in Z_n^*)(a^{n-1} \equiv 1 \bmod n)$ then n is square-free.*

Proof of the lemma: Let p be a prime dividing n and let p^t be the largest power of p dividing n. Let g be a generator of $Z_{p^t}^*$. Use the Chinese remainder theorem to find an $a \in Z_n^*$ such that

$$a \equiv g \bmod p^t \text{ and } a \equiv 1 \bmod (n/p^t).$$

It follows from the hypothesis that $a^{n-1} \equiv g^{n-1} \equiv 1 \bmod p^t$. Hence $\text{order}_{p^t}(g) = \varphi(p^t) = p^{t-1}(p-1) | (n-1)$. Thus, $t = 1$, as desired •

Proof of the main theorem:

The above lemma implies that if n is composite then it must be of the form $n = p_1 \cdots p_r$, where $p_1 \ldots, p_r$ are distinct primes and $r \geq 2$. Let a be a quadratic nonresidue modulo p_1. Use the Chinese remainder theorem to find an $x \in Z_n^*$ such that $x \equiv a \bmod p_1$ and $x \equiv 1 \bmod (n/p_1)$. Hypothesis (2) of the theorem implies that

$$(x|n) = (x|p_1) \cdots (x|p_r) = (a|p_1) = -1 \equiv x^{(n-1)/2} \bmod n.$$

However this contradicts $x \equiv 1 \bmod p_2$ •

Using the above theorem and theorem 9.2 it can be shown that

Theorem 10.2 *(Assume ERH) There exists a constant $C > 0$ such that for any odd integer $n > 1$ the following statements are equivalent*

(1) n is prime

(2) For all $a \in Z_n^*$ such that $a < C \cdot (\log n)^2$, $a^{(n-1)/2} \equiv (a|n) \bmod n$.

Proof: (1) $\Rightarrow$ (2) is trivial. To prove the converse assume (2) is true but n is composite. Let $C > 0$ be the constant of theorem 9.2. Consider the abelian group $G = \{a^{(n-1)/2} \cdot (a|n) \bmod n : a \in Z_n^*\}$ and the group homomorphism $\chi : Z_n^* \rightarrow G$ such that $\chi(a) = a^{(n-1)/2} \cdot (a|n) \bmod n$. Theorem 10.1 implies that χ is nontrivial. A contradiction follows easily from theorem 9.2 •

11 A Variant of Solovay-Strassen's Test

This test constitutes a simplification of the Solovay-Strassen deterministic test because it makes no mention of the Jacobi symbol. It is based on the following theorem.

Theorem 11.1 *For any odd integer $n > 1$ the following statements are equivalent*

(1) n is prime

(2) $(\forall a \in Z_n^*)(a^{(n-1)/2} \equiv^{\pm} 1 \bmod n)$ and $(\exists a \in Z_n^*)(a^{(n-1)/2} \equiv -1 \bmod n)$

Proof: (1) $\Rightarrow$ (2)

This is an immediate consequence of of Euler's criterion and the primality of n.

(2) $\Rightarrow$ (1)

It follows from lemma 10.1 that n is square free i.e. $(\forall p)(p|n \Rightarrow p^2 \not| n)$. Hence without loss of generality it can be assumed that n is the product of the distinct primes $p_1, \ldots, p_r$. The groups Z_n^* and $Z_{p_1}^* \times \cdots \times Z_{p_r}^*$ are isomporphic.

Since there exists an $a \in Z_n^*$ such that $a^{(n-1)/2} \equiv -1 \bmod n$, there exist $a_i \in Z_{p_i}^*$ such that $a_i^{(n-1)/2} \equiv -1 \bmod p_i$, for $i = 1, \ldots, r$. Consider the characters

$$\chi(a) = a^{(n-1)/2} \bmod n,\ \chi_i(a) = a^{(n-1)/2} \bmod p_i,$$

where $i = 1, \ldots, r$ and let $K, K_1, \ldots, K_r$ be their respective kernels. It is then clear that K is isomorphic to $K_1 \times \cdots \times K_r$ and hence

$$\frac{\varphi(n)}{2} = |K| = |K_1| \cdots |K_r| = \frac{\varphi(p_1)}{2} \cdots \frac{\varphi(p_r)}{2} = \frac{\varphi(n)}{2^r}$$

It follows that $r = 1$ and hence n is prime •

Using theorem 9.2 the following result can be proved.

Theorem 11.2 *(Assume ERH) There exists a constant $C > 0$ such that for any odd integer $n > 1$ the following statements are equivalent*

(1) n is prime

(2) $(\forall a < C \cdot (\log n)^2 \text{ in } Z_n^*)(a^{(n-1)/2} \equiv^{\pm} 1 \bmod n)$ *and*
$(\exists a < C \cdot (\log n)^2 \text{ in } Z_n^*)(a^{(n-1)/2} \equiv -1 \bmod n)$.

Proof: (1) $\Rightarrow$ (2)

Assume n is prime. The first part of (2) is an immediate consequence of theorem 11.1. To prove the second part use theorem 11.1 to conclude that the character $\chi(a) = a^{(n-1)/2} \bmod n$ is non trivial and use theorem 9.2 .

(2) $\Rightarrow$ (1)

It is enough to prove that both conditions of part (2) of theorem 11.1 are true. The second part is immediate. To prove the first part assume on the contrary $(\exists a \in Z_n^*) a^{(n-1)/2} \not\equiv^{\pm} 1 \bmod n$. Consider the quotient group G/H, where $G = Z_n^*$ and $H = \{1, -1\}$. Let $\chi : Z_n^* \to G/H$ be the character $\chi(a) =$ the equivalence class of $a^{(n-1)/2} \bmod n$ in the group G/H. Using theorem 9.2 one easily obtains an $a < C \cdot (\log n)^2$ such that $\chi(a) \neq H$ (H is the unit of the group G/H.) But this is a contradiction •

12 Miller's Deterministic Test

Miller's deterministic test is based on the following theorem.

Theorem 12.1 *For any odd integer $n > 1$ write $n - 1 = 2^e u$, with u odd. Then the following statements are equivalent*

(1) n is prime

(2) $(\forall a \in Z_n^*)(a^u \not\equiv 1 \bmod n \Rightarrow \exists k < e(a^{2^k u} \equiv -1 \bmod n))$

Proof: (1) $\Rightarrow$ (2) is an immediate consequence of the theorem of Euler-Fermat and the primality of n. The converse (2) $\Rightarrow$ (1) requires the following

Lemma 12.1 *Assume that $n = p_1^{k_1} \cdots p_r^{k_r}$ is the prime factorization of n, where $p_1, \ldots, p_r$ are distinct primes. Write $n - 1 = 2^e u$, with u odd and put $\nu = \min\{\nu_2(p_i - 1) : i = 1, \ldots, r\}$. Then the following statements hold*

(1) $e \geq \nu$

(2) $e = \nu \Leftrightarrow |\{1 \leq i \leq r : k_i$ is odd and $\nu_2(p_i - 1) = \nu\}|$ is odd.

Proof of the lemma: Clearly $e \geq \nu$ follows easily from

$$n - 1 = (p_r^{k_r} - 1) + \sum_{i=1}^{r-1} (p_i^{k_i} - 1) p_{i+1}^{k_{i+1}} \cdots p_r^{k_r}. \tag{2}$$

Without loss of generality it can be assumed that $1, \ldots, h$ are the indices i for which k_i is odd and $\nu_2(p_i - 1) = \nu$. It is easy to see that

$$(\forall i \geq h+1)(2^{\nu+1} | p_i^{k_i} - 1) \text{ and } (\forall i \leq h)(2^{\nu+1} \not| p_i^{k_i} - 1)$$

Hence $p_i^{k_i} \equiv 1 \bmod 2^{\nu+1}$, for $i \geq h+1$. For $i \leq h$, let s_i be odd such that $p_i^{k_i} = 1 + s_i 2^\nu$. Substituting in equation (2) and multiplying out it is easy to obtain

$$n - 1 \equiv (s_1 + \cdots + s_h) 2^\nu \bmod 2^{\nu+1} \tag{3}$$

It is now immediate from equation (3) that $e = \nu \Leftrightarrow s_1 + \cdots + s_h$ is odd. The result of the lemma follows easily •

Proof of the theorem: Assume that hypothesis (2) of the theorem is true. Theorem 10.1 implies that it is enough to show $(\forall a \in Z_n^*)(a^{(n-1)/2} \equiv (a|n) \bmod n)$. Indeed, let $a \in Z_n^*$. If $a^u \equiv 1 \bmod n$, then $a^{(n-1)/2} \equiv 1 \bmod n$. Moreover since u is odd

$$(a|n) = (a|n)^u = (a^n|p) = 1,$$

Hence without loss of generality it can be assumed that $a^u \not\equiv 1 \bmod n$. Hypothesis (2) of the theorem implies that there exists $k < e$ such that

$$a^{2^k u} \equiv -1 \bmod n \text{ and } a^{2^{k+1} u} \equiv 1 \bmod n. \tag{4}$$

Let $n = p_1^{k_1} \cdots p_r^{k_r}$ be the prime factorization of n, where $p_1, \ldots, p_r$ are distinct primes. For each $i = 1, \ldots, r$ let $\nu_i = \nu_2(p_i - 1)$; also let u_i be odd such that $p_i - 1 = 2^{\nu_i} u_i$. Then it is true that $(a|p_i) = (a|p_i)^u \equiv a^{u(p_i-1)/2} \equiv a^{2^{\nu_i - 1} u_i u} \bmod p_i$. Since both u, u_i are odd it follows that

$$k = \nu_i - 1 \Rightarrow (a|p_i) = -1, \text{ and } k < \nu_i - 1 \Rightarrow (a|p_i) = 1. \tag{5}$$

Assume on the contrary that $k > \nu_i - 1$, for some $i = 1, \ldots, r$. Then $(a|p_i) \equiv a^{2^{\nu_i - 1} u_i u} \bmod p_i$, and hence $a^{2^{\nu_i} u_i u} \equiv 1 \bmod p_i$, which contradicts congruences (4). It follows that $k \leq \nu - 1 \leq e - 1$. If $k < \nu - 1$ then equations (5) imply that for all $i = 1, \ldots, r$, $(a|p_i) = 1$ and hence also $(a|n) = 1$. Since $k < e - 1$ it follows

that $a^{(n-1)/2} \equiv 1 \bmod n$. Consequently to complete the proof of the theorem it is enough to consider the case $k = \nu - 1$. Without loss of generality let $1, \ldots, h$ be the indices such that k_i is odd and $\nu_i = \nu$. It follows from equations (5) that $(a|n) = (-1)^{k_1 + \cdots + k_h}$. If $\nu = e$ then the above lemma implies that h is odd. Hence $(a|n) = -1$ and $a^{(n-1)/2} \equiv a^{2^k u} \equiv -1 \bmod n$. On the other hand if $\nu < e$ then h is even. Moreover, $(a|n) = 1$ and $a^{(n-1)/2} \equiv a^{2^k u} \equiv 1 \bmod n$. This completes the proof of the theorem •

The above theorem and theorem 9.2 can be used to show.

Theorem 12.2 *(Assume ERH) There exists a constant $C > 0$ such that for any odd integer $n > 1$ if $n - 1 = 2^e u$, with u odd, then the following statements are equivalent*

(1) n is prime

(2) For all $a \in Z_n^*$ such that $a < C \cdot (\log n)^2$,

$$a^u \not\equiv 1 \bmod n \Rightarrow \exists k < e (a^{2^k u} \equiv -1 \bmod n).$$

Proof: (1) $\Rightarrow$ (2) is trivial. To prove the converse assume (2) is true but n is composite. Let $C > 0$ be the constant of theorem 9.2. Assume that for some prime p, $p^2 | n$. Consider the abelian group $G = \{a^{p-1} \bmod p^2 : a \in Z_{p^2}^*\}$ and the group homomorphism $\chi : Z_{p^2}^* \rightarrow G$ such that $\chi(a) = a^{p-1} \bmod p^2$. The following lemma implies that χ is nontrivial.

Lemma 12.2 *The congruence $x^{p-1} \equiv 1 \bmod p^2$ has at most $p - 1$ solutions.*

Proof of the lemma: Let g be a generator of $Z_{p^2}^*$. Then it is easy to show that the only solutions of the above congruence are

$$g^p \bmod p^2, g^{2p} \bmod p^2, \ldots, g^{(p-1)p} \bmod p^2 \bullet$$

It follows from theorem 9.2 that there exists an integer $a < C \cdot (\log p^2)^2$ such that $a^{p-1} \not\equiv 1 \bmod p^2$. It will be shown that in fact $a^{n-1} \not\equiv 1 \bmod p^2$. Indeed, if $a^{n-1} \equiv 1 \bmod p^2$ then $\text{order}_{p^2}(a) | (n-1)$ and $\text{order}_{p^2}(a) | \varphi(p^2) = p(p-1)$ imply that $\text{order}_{p^2}(a) | p - 1$, which is a contradiction. Hence $a^{n-1} \not\equiv 1 \bmod p^2$, which contradicts the hypothesis of the theorem.

Thus it can be assumed that n is the product of distinct primes. In this case let p, q be two distinct prime factors of n. Without loss of generality it can be assumed that $\nu_2(p-1) \geq \nu_2(q-1)$. Define an integer $d \equiv 1 \bmod 4$ by

$$d = \begin{cases} pq & \text{if } \nu_2(p-1) = \nu_2(q-1) \\ p & \text{if } \nu_2(p-1) > \nu_2(q-1) \end{cases}$$

It follows from theorem 9.2 that there exists an $a < C \cdot (\log d)^2 \leq C \cdot (\log n)^2$ such that $(a|d) = -1$. Put $b = a^u$. Since u is odd it follows that $(b|u) = -1$ and hence $b \not\equiv 1 \bmod d$. It will be shown that for all $j < e$, $b^{2^j} \not\equiv -1 \bmod n$. This

clearly contradicts hypothesis (2) of the theorem. Indeed, assume otherwise and let $j < e$ be maximal such that $b^{2^j} \equiv -1 \bmod n$. Then $\text{order}_p(b) = \text{order}_q(b) = 2^{j+1}$. One can now distinguish two cases.

Case 1: $\nu_2(p-1) > \nu_2(q-1)$

In this case $2^{j+1} | q-1$ and hence $2^{j+1} | (p-1)/2$. Thus, on the one hand $(b|d) = (b|p) = -1$ and on the other hand $b^{(p-1)/2} \equiv 1 \bmod p$, which contradicts the Euler-Fermat theorem.

Case 2: $\nu_2(p-1) = \nu_2(q-1)$

In this case $(b|d) = (b|p)(b|q) = -1$. Say, without loss of generality, $(b|p) = -(b|q) = -1$. Hence $b^{(q-1)/2} \equiv 1 \bmod q$ and $\text{order}_p(b) = \text{order}_q(b) | (q-1)/2$. Since $\nu_2(p-1) = \nu_2(q-1)$ this implies that $\text{order}_p(b) | (p-1)/2$ and hence $b^{(p-1)/2} \equiv 1 \bmod p$, which is a contradiction •

13 An Improvement of Miller's Test

The proof of theorem 12.2 requires the Riemann hypothesis for the characters

$$\chi(a) = a^{p-1} \bmod p^2, p \text{ is prime and}$$

$$\chi(a) = (a|d),$$

where $d \equiv 1 \bmod 4$ and d is either a prime or the product of two primes. H.W. Lenstra in [Len3] has observed that the Riemann hypothesis is not necessary for the characters $\chi(a) = a^{p-1} \bmod p^2$. In fact it can be shown that

Theorem 13.1 *Assume that the Extended Riemann Hypothesis holds for all $L-$ functions of the form $L_d(z) = \sum_{k \geq 1} (k|d) k^{-z}$, where $d \equiv 1 \bmod 4$ and d is either a prime or the product of two primes. Then there exists a constant $C > 0$ such that for any odd integer $n > 1$ if $n - 1 = 2^e u$, with u odd, then the following statements are equivalent*

(1) n is prime

(2) For all $a \in Z_n^*$ such that $a < C \cdot (\log n)^2$,

$$(a^u \not\equiv 1 \bmod n \Rightarrow \exists k < e (a^{2^k u} \equiv -1 \bmod n)).$$

Proof: The proof of (2) $\Rightarrow$ (1) is exactly as the proof of theorem 12.2. However if for some prime p, $p^2 | n$ then one does not use the ERH but instead the following lemma (due to H. W. Lenstra)

Lemma 13.1 *There exists an odd prime $a < 4(\log p)^2$ such that*

$$a^{p-1} \not\equiv 1 \bmod p^2.$$

This completes the proof of the theorem •

Details of the proof of lemma 13.1 can be found in [Len3].

14 Selfridge-Weinberger Test

For each prime p let $F(p)$ = the least positive square free integer n such that for all prime numbers $q \leq p$, $(q|n) = 1$.

Theorem 14.1 *Let $n > 1$ be an odd integer and suppose that p is a prime such that $p < n < F(p)$. Then the following statements are equivalent*

(1) n is prime

(2)(a) $(\forall q \text{ prime } \leq p)\ \gcd(q, n) = 1$

(b) *n is not a nontrivial power of a prime*

(c) $(\forall q \text{ prime } \leq p)(q^{(n-1)/2} \equiv^{\pm} 1 \bmod n$

(d) $(\exists q \text{ prime } \leq p)(q^{(n-1)/2} \equiv -1 \bmod n)$

Proof: (1) $\Rightarrow$ (2)

This is an immediate consequence of Euler's criterion, the primality of n and the minimality of $F(p)$.

(2) $\Rightarrow$ (1)

Assume on the contrary that n is composite. Let $n = p_1^{k_1} \cdots p_r^{k_r}$ be the prime factorization of n, where $p_1, \ldots, p_r$ are distinct primes. By assumption $r \geq 2$. For $i = 1, \ldots, r$, write $n - 1 = 2^e u, p_i - 1 = 2^{\nu_i} u_i$, where $u, u_1, \ldots, u_r$ are odd. The basic step in the proof is the following

Claim: $\nu_i = e$, for all $i = 1, \ldots, r$.

Proof of the Claim: Consider an integer $i = 1, \ldots, r$. Since $p_i < n < F(p)$ there exists a prime $q \leq p$ such that $(q|p_i) = -1$. Let $d = \text{order}_{p_i}(q)$. By Euler's criterion $q^{(p_i-1)/2} \equiv -1 \bmod p_i$. By assumption, $q^{(n-1)/2} \equiv^{\pm} 1 \bmod p_i$. It follows that $2^{\nu_i} | d$ and $d | n-1$ and hence $\nu_i \leq e$. It remains to show that $\nu_i \geq e$. By assumption there exists a prime $q \leq p$ such that $q^{(n-1)/2} \equiv -1 \bmod p_i$. On the other hand $q^{p_i-1} \equiv 1 \bmod p_i$. It follows that $\nu_i \geq e$ and the proof of the claim is complete.

It follows from the claim and lemma 12.1 that there exist two distinct primes p_i, p_j such that $p_i \cdot p_j < n$ (assume for simplicity that $i = 1$ and $j = 2$.) By assumption there exists a prime $q \leq p$ such that $(q|p_1 \cdot p_2) = -1$. Without loss of generality it can be assumed that $(q|p_1) = -(q|p_2) = 1$. Moreover it is true that

$$q^{(n-1)/2} \equiv^{\pm} 1 \bmod n. \tag{6}$$

For $i = 1, 2$ put $d_i = \text{order}_{p_i}(q)$. Since $q^{(p_2-1)/2} \equiv -1 \bmod p_2$, $2^e | d_2$ and hence

$$q^{(n-1)/2} \equiv -1 \bmod p_2. \tag{7}$$

Since $q^{(p_1-1)/2} \equiv 1 \bmod p_1$, $d_1 | 2^{e-1} u_1$. It follows from congruence (6) that $d_1 | (n-1)/2$. Hence,

$$q^{(n-1)/2} \equiv 1 \bmod p_1. \tag{8}$$

However congruences (6), (7), (8) give a contradiction •

Besides its theoretical value the Selfridge-Weinberger test has practical significance as well. In applications one uses tables of values of the function $F(p)$ and tests the primality of an integer $p < n < F(p)$ via theorem 14.1. Such a table of values of $F(p)$ can be found in [LLS], from which the table in Figure 2 is extracted.

p	$F(p)$	p	$F(p)$
3	73	53	22,000,801
7	1,009	67	175,244,281
13	8,089	79	898,716,289
19	53,881	101	10,310,263,441
29	117,049	103	23,616,331,489
37	1,083,289	127	196,265,095,009

Figure 2: Table of Values of $F(p)$

In addition, Weinberger has shown (unpublished) that assuming ERH there exist constants $c_1, c_2, c_3 > 0$ such that for all n and all primes p,

$$p > (c_1 \log n + c_2 \log\log n + c_3)^2 \Rightarrow n < F(p).$$

15 Probabilistic Primality Tests

The main feature of a probabilistic primality test is the construction of a family $P = \{P_n : n \geq 1\}$ of sets of integers such that the following properties hold:

1. For each $n \geq 1$, $P_n \subseteq Z_n^*$
2. Given $b \in Z_n^*$ it is easy to check (i.e. in time polynomial in the length of the integer n) if $b \in P_n$
3. If n is prime then $P_n = \emptyset$
4. There is a constant $0 < \epsilon < 1$ which is indepedent of n such that for all sufficiently large composite odd $n \geq 1$, $Pr[x \in Z_n^* : x \notin P_n] \leq \epsilon$.

Remark: In practice property 4 above will be true for all $n > n_0$, where n_0 is small (e.g. $n_0 = 1$ in the Solovay-Strassen test and $n_0 = 9$ in the Rabin test.)

Such a family $P = \{P_n : n \geq 1\}$ will be called a **primality sequence** and the constant ϵ satisfying condition (4) above is called the **primality constant** corresponding to the family P. To any primality sequence P one can associate a primality test, denoted by A_P and defined as follows:

Input: $n > 1$

Step 1: Choose an integer $b \in Z_n^*$ at random.
Step 2: Check if $b \in P_n$.
Output:

$$A_P(n) = \begin{cases} \text{PRIME} & \text{if } b \notin P_n \\ \text{COMPOSITE} & \text{if } b \in P_n \end{cases}$$

The following result is now an immediate consequence of the above definitions.

Theorem 15.1 *Let ϵ be a primality constant corresponding to the primality sequence P. Then for any sufficiently large odd integer $n \geq 1$,*
(1) n is prime $\Rightarrow A_P(n) = PRIME$.
(2) n is odd and composite $\Rightarrow Pr[A_P(n) = PRIME] \leq \epsilon$ •

In other words, if n is prime the test A_P will output the correct answer (i.e. PRIME). However, if n is composite and odd the test A_P may not necessarily output COMPOSITE; in fact it may very well output PRIME. However, the probability of making such an error is less than or equal to ϵ.

If the random choices of b are indepedent in successive runs of the algorithm A_P then one can significantly improve the probability of error. In fact it is very easy to show that

Theorem 15.2 *Let ϵ be a primality constant corresponding to the primality sequence P. Then for any integer $m \geq 1$, and any sufficiently large odd integer n,*

$$n \text{ is composite } \Rightarrow Pr[A_P(n) = PRIME, \ m \text{ times}] \leq \epsilon^m \bullet$$

The next two tests are probabilistic primality tests. In each case the primality sequence will be defined and the primality constant corresponding to this sequence will be determined. The probabilistic primality test corresponding to each such sequence P is A_P.

16 Solovay-Strassen Test

The following lemma will be essential for the present as well as the next subsection.

Lemma 16.1 *Let $n = p_1^{k_1} \cdots p_r^{k_r}$ be the prime factorization of an odd integer n, where $p_1, \ldots, p_r$ are distinct primes. Put $\nu = \min\{\nu_2(p_i - 1) : i = 1, \ldots, r\}$ and $s = \prod_{i=1}^{r} \gcd(m, \varphi(p_i^{k_i}))$. Then it can be shown that*
(1) $x^m \equiv 1 \bmod n$ has exactly s solutions.
(2) $(\exists x)(x^m \equiv -1 \bmod n) \Leftrightarrow \nu_2(m) < \min\{\nu_2(p_i - 1) : i = 1, \ldots, r\}$.
(3) If $x^m \equiv -1 \bmod n$ has a solution then it must have exactly s solutions.

Proof: For each $i = 1, \ldots, r$ let g_i be a generator of $Z^*_{p_i^{k_i}}$. Taking the indices of both sides of the congruence $x^m \equiv a \bmod n$ one obtains the congruences

$$m \cdot \text{index}_{g_i}(x) \equiv \text{index}_{g_i}(a) \bmod \varphi(p_i^{k_i}), \text{ for } i = 1, \ldots, r. \tag{9}$$

If $a = 1$ then $\text{index}_{g_i}(1) = 0$ and hence congruences (9) become

$$m \cdot \text{index}_{g_i}(x) \equiv 0 \bmod \varphi(p_i^{k_i}), \text{ for } i = 1, \ldots, r. \tag{10}$$

If $a = -1$ then $\text{index}_{g_i}(1) = \varphi(p_i^{k_i})/2$ and hence congruences (9) become

$$m \cdot \text{index}_{g_i}(x) \equiv \frac{\varphi(p_i^{k_i})}{2} \bmod \varphi(p_i^{k_i}), \text{ for } i = 1, \ldots, r. \tag{11}$$

Part (1) of the lemma follows from congruences (10) and the theorem on solving linear congruences. On the other hand the same theorem implies that congruences (11) have a solution if and only if $\gcd(m, \varphi(p_i^{k_i}))|\varphi(p_i^{k_i})/2$, for each $i = 1, \ldots, r$. However it is easy to see that this last equivalence holds exactly when $\nu_2(m) < \min\{\nu_2(p_i - 1) : i = 1, \ldots, r\}$ •

The primality sequence of the Solovay-Strassen test is defined by

$$P_n = \{b \in Z_n^* : b^{(n-1)/2} \not\equiv (b|n) \bmod n\}.$$

It follows from Euler's criterion that $P = \{P_n : n \geq 1\}$ satisfies conditions $(1) - (3)$ of primality sequences. For each n consider the multiplicative group automorphisms $f_n, g_n, h_n : Z_n^* \to Z_n^*$ defined by

$$f_n(a) = a^{(n-1)/2} \bmod n, \; g_n(a) = (a|n) \bmod n, \; h_n(a) = (a|n) \cdot a^{(n-1)/2} \bmod n.$$

Let K_n, L_n, M_n denote the kernels of the homomorphisms f_n, g_n, h_n respectively. Put $K'_n = \{b \in Z_n^* : f_n(b) \equiv -1 \bmod n\}$, $L'_n = \{b \in Z_n^* : g_n(b) \equiv -1 \bmod n\}$ and $M'_n = \{b \in Z_n^* : h_n(b) \equiv -1 \bmod n\}$. It is clear that $M_n = Z_n^* - P_n$.

Theorem 16.1 *(Monier) For all odd n, if $p_1, \ldots, p_r$ are the distinct prime factors of n then*

$$|Z_n^* - P_n| = \delta_n \cdot \prod_{i=1}^{r} \gcd\left(\frac{n-1}{2}, p_i - 1\right),$$

where δ_n has one of the values $1/2, 1, 2$.

Proof: It is clear from the definition of K_n that

$$|K_n| = \prod_{i=1}^{r} \gcd\left(\frac{n-1}{2}, p_i - 1\right).$$

On the other hand it is true that $M_n = (K_n \cap L_n) \cup (K'_n \cap L'_n)$. Hence,

$$|M_n| = \begin{cases} |K_n \cap L_n| & \text{if } K'_n \cap L'_n = \emptyset \\ 2|K_n \cap L_n| & \text{if } K'_n \cap L'_n \neq \emptyset \end{cases}$$

(if $K'_n \cap L'_n \neq \emptyset$ choose $b_0 \in K'_n \cap L'_n$ and consider the function $b \longrightarrow bb_0$ to show that $K_n \cap L_n = K'_n \cap L'_n$.) A similar argument using $K_n = (K_n \cap L_n) \cup (K_n \cap L'_n)$ is the kernel of the homomorphism g_n shows that

$$|K_n \cap L_n| = \begin{cases} |K_n| & \text{if } K_n \cap L'_n = \emptyset \\ (1/2) \cdot |K_n| & \text{if } K_n \cap L'_n \neq \emptyset. \end{cases}$$

Hence $|M_n| = \delta_n |K_n|$ as desired •

Now it is not very difficult to determine the primality constant.

Theorem 16.2 *(***Solovay-Strassen***) For all composite odd integers n,*

$$\frac{|Z_n^* - P_n|}{\varphi(n)} \leq \frac{1}{2}.$$

Proof: Let $p_1, \ldots, p_r$ be the distinct prime factors of n and suppose that $p_i^{t_i}$ is the largest power of p_i dividing n. It follows from Monier's theorem and the properties of the function φ that

$$\frac{|Z_n^* - P_n|}{\varphi(n)} = \delta_n \cdot \prod_{i=1}^{r} \frac{\gcd\left(\frac{n-1}{2}, p_i - 1\right)}{p_i^{t_i - 1}(p_i - 1)} \tag{12}$$

If for some i, $t_i \geq 2$ then the righthand side of inequality (12) is $\leq \delta_n/3 \leq 2/3$. Hence, $Z_n^* - P_n$ is a proper subgroup of Z_n^* and as such it must be true that $|Z_n^* - P_n| \leq (1/2)\varphi(n)$.

Thus, without loss of generality it can be assumed that for all i, $t_i = 1$. In this case $n = p_1 \cdots p_r$. Assume on the contrary that $Z_n^* = M_n$. Since n is composite, $r \geq 2$. Let g be a generator of $Z_{p_1}^*$. Use the Chinese Remainder theorem to find an $a \in Z_n^*$ such that $a \equiv g \bmod p_1$ and $a \equiv 1 \bmod (n/p_1)$. Since $Z_n^* = M_n$ it is true that $a^{(n-1)/2} \equiv (a|n) \bmod n$. However, $(a|n) = (a|p_1) \cdots (a|p_r) = (a|p_1) = (g|p_1) = -1$. Hence, $a^{(n-1)/2} \equiv -1 \bmod (n/p_1)$, which contradicts $a \equiv 1 \bmod (n/p_1)$•

As an immediate corollary of equality (12) one can also obtain that

Theorem 16.3 *For all composite odd integers n, if $(n-1)/2$ is odd and r is the number of distinct prime factors of n then*

$$\frac{|Z_n^* - P_n|}{\varphi(n)} \leq \frac{1}{2^{r-1}}\bullet$$

17 Rabin Test

The Rabin primality sequence is defined by

$$P_n = \{b \in Z_n^* : b^{(n-1)/2^e} \not\equiv 1 \bmod n \text{ and } (\forall t > 0)(b^{(n-1)/2^t} \not\equiv -1 \bmod n\},$$

where $e = \nu_2(n-1)$. It is easy to show that $P = \{P_n : n \geq 1\}$ satisfies conditions (1 - 3) of primality sequences. It is clear that $Z_n^* - P_n =$

$$\{b \in Z_n^* : b^{(n-1)/2^e} \equiv 1 \bmod n \text{ or } (\exists t > 0)(b^{(n-1)/2^t} \equiv -1 \bmod n)\}, \qquad (13)$$

The following theorem determines the exact size of the above set.

Theorem 17.1 *(Monier) Let n be a composite odd integer, with prime factorization $n = p_1^{t_1} \cdots p_r^{t_r}$, where $p_1, \ldots, p_r$ are distinct primes. Write $n - 1 = 2^e u, p_i - 1 = 2^{\nu_i} u_i$, with u, u_i odd and let $\nu = \min\{\nu_i : i = 1, \ldots, r\}$. Then the following equality holds*

$$|Z_n^* - P_n| = \left(1 + \frac{2^{r\nu} - 1}{2^r - 1}\right) \prod_{i=1}^{r} \gcd(u, u_i)$$

Proof: Put $s = \prod_{i=1}^{r} \gcd(u, u_i)$. The leftmost congruence of the set in (13) has exactly s solutions (see lemma 16.1.) For any given $t > 0$ the other congruence has a solution if and only if $\nu_2((n-1)/2^t) = e - t < \nu$. Hence, for each $t > e - \nu$ the number of solutions of $b^{(n-1)/2^t} \equiv -1 \bmod n$ is

$$\prod_{i=1}^{r} \gcd\left(\frac{n-1}{2^t}, p_i - 1\right).$$

It follows that

$$|Z_n^* - P_n| = s + \sum_{e-\nu<t\leq e} \prod_{i=1}^{r} \gcd\left(\frac{n-1}{2^t}, p_i - 1\right).$$

The theorem now follows easily from

$$\gcd\left(\frac{n-1}{2^t}, p_i - 1\right) = 2^{e-t} \cdot \gcd(u, u_i) \bullet$$

It remains to determine the primality constant of the Rabin sequence. Let R_n be the set

$$\left\{b \in Z_n^* : b^{n-1} \not\equiv 1 \bmod n \text{ or } (\exists e \geq t \geq 0)\left[1 < \gcd\left(b^{(n-1)/2^t} - 1, n\right) < n\right]\right\},$$

where $n - 1 = 2^e u$ and u is odd. It is now easy to show that

Theorem 17.2 *(Miller-Rabin-Monier) For all odd integers $n > 2$, $P_n = R_n$.*

Proof: For each t such that $2^t | n-1$ let

$$d(t) = \frac{n-1}{2^t},\ x(t) = b^{d(t)},\ \ g(t) = \gcd(x(t)-1, n).$$

It is very easy to show that for all t such that $2^t | n-1$, the following hold

1. $g(t) = n \Leftrightarrow x(t) \equiv 1 \bmod n$
2. $g(t) = n \Rightarrow g(t-1) = n$
3. $x(t-1) = x(t)^2$.

Proof of $P_n \subseteq R_n$

Assume on the contrary that $b \in P_n$ but $b \notin R_n$. It follows that there exists an integer $k \leq e$ such that $g(k) = n$. Since $b \in P_n$, $b^{d(e)} \not\equiv \bmod n$ and hence $g(e) \neq n$. It follows that there exists $k < e$ such that

$$g(0) = g(1) = \cdots = g(k) = n > g(k+1) = \cdots = g(e) = 1.$$

But $g(k) = n$. Hence, $x(k+1)^2 \equiv 1 \bmod n$. Therefore $n | (x(k+1)-1)(x(k+1)+1)$. This and $g(k+1) = \gcd(x(k+1)-1, n) = 1$ imply that $x(k+1) \equiv -1 \bmod n$, which in turn contradicts $b \in P_n$.

Proof of $R_n \subseteq P_n$

Assume that $b \notin P_n$. Then either $x(e) \equiv 1 \bmod n$ or $\exists t > 0 (x(t) \equiv -1 \bmod n)$. In the first case $b \notin R_n$. Thus without loss of generality it can be assumed that $x(e) \not\equiv 1 \bmod n$. Choose $k \leq e$ such that

$$x(0) \equiv x(1) \equiv \cdots \equiv x(k-1) \equiv 1,\ x(k) \equiv -1 \bmod n.$$

Using the fact that $x(k) \equiv x(k+j)^{2^j} \equiv -1 \bmod n$ it follows that

$$x(k) - 1 \equiv x(k+1)^2 - 1 \equiv x(k+2)^{2^2} - 1 \equiv \cdots \equiv x(e)^{2^{e-k}} - 1 \equiv -2 \bmod n.$$

However, for all $j \leq e-k$ there exists an integer b_j such that

$$x(k+j)^{2^{2^j}} - 1 \equiv (x(k+j)-1)b_j \equiv -2 \bmod n.$$

Since n is odd > 2 it follows that $(\forall j \leq e-k)(g(k+j) = 1)$. Since $(\forall j < k)(g(j) = n)$ it follows that $(\forall t)(g(t) = 1 \text{ or } n)$. Hence, $b \notin R_n$ •

It remains to determine the primality constant of the Rabin sequence. Let n be an odd integer with $p_1, \ldots, p_r$ its distinct prime factors. Let $n = p_1^{k_1} \cdots p_r^{k_r}$ be the prime factorization of n and put $q_i = p_i^{k_i}$, where $i = 1, \ldots, r$. Let $t_i = \gcd(\varphi(q_i), n-1)$ and $m_i = \varphi(q_i)/t_i$. In addition put $e_i = \nu(t_i)$, $\alpha_i = \max\{e_i -$

$e_j : j = 1, \ldots, r\}$. It is clear that if e_i is minimum among the $\{e_1, \ldots, e_r\}$ then $\alpha_i = 0$. Consider the sets

$$I = \{1 \leq i \leq r : \alpha_i > 0\},\ J = \{1 \leq i \leq r : \alpha_i = 0\}$$

and put $\alpha = \alpha_1 + \cdots + \alpha_r$, $\beta = |J|$. It is clear that $\beta > 0$ and $\alpha + \beta \geq r$. The following result uses the above notation and is the main theorem of this subsection.

Theorem 17.3 *For any composite odd integer $n > 2$, if the number r of distinct prime factors of n is ≥ 2 then*

$$\frac{|Z_n^* - R_n|}{\varphi(n)} \leq \frac{1}{2^{\alpha+\beta-1} m_1 \cdots m_r}$$

Proof: Let $b \in Z_n^* - R_n$. Then $b^{n-1} \equiv 1 \bmod n$. For each $i = 1, \ldots, r$ let a_i be a generator of $Z_{q_i}^*$. It follows that there exists an $s_i < \varphi(q_i)$ such that $b \equiv a_i^{s_i} \bmod q_i$. Thus, $b^{n-1} \equiv a_i^{s_i(n-1)} \equiv 1 \bmod q_i$ and $\varphi(q_i) | s_i(n-1)$. Since $\gcd(m_i, n-1) = 1$ and $m_i = \varphi(q_i)/t_i | s_i(n-1)$ it follows that $m_i | s_i$ and $s_i = m_i h_i$, for some $h_i < \varphi(q_i)/m_i$. So for all $i = 1, \ldots, r$,

$$b \equiv a_i^{m_i h_i} \bmod q_i \tag{14}$$

and $s_i(n-1) = m_i h_i (n-1) = \varphi(q_i) h_i \frac{n-1}{t_i}$. An essential step of the proof is the following

Claim: For all $i = 1, \ldots, r$, $2^{\alpha_i} | h_i$.

Proof of the Claim: Without loss of generality it can be assumed that $\alpha_i > 0$. Let j be an index such that $\alpha_i = e_i - e_j > 0$. Let $f_i \geq 0$ be such that $\nu_2(n-1) = e_i + f_i$. Put $\gamma_i = e_i - e_j + f_i$. Then $\nu_2(d(\gamma_i)) = e_j$. In addition, $t_j | d(\gamma_i)$. Hence, $\varphi(q_j) = t_j m_j | m_j d(\gamma_i)$. It follows from congruence (14) that $b^{d(\gamma_i)} \equiv a_j^{m_j h_j d(\gamma_i)} \equiv 1 \bmod q_j$. Hence, $1 < q_j \leq \gcd(b^{d(\gamma_i)} - 1, n)$. Since $b \notin R_n$, $\gcd(b^{d(\gamma_i)} - 1, n) = n$ and hence $b^{d(\gamma_i)} \equiv 1 \bmod n$. Using the last congruence, the fact that a_i generates $Z_{q_i}^*$ as well as congruence (14) it follows that $t_i | d(\gamma_i) h_i$. But this easily implies that $2^{e_i - e_j} = 2^{\alpha_i} | h_i$, which completes the proof of the claim.

Using the above claim and congruence (14) it follows easily that

$$|Z_n^* - R_n| \leq \frac{\varphi(q_1)}{2^{\alpha_1} m_1} \cdots \frac{\varphi(q_r)}{2^{\alpha_r} m_r} \leq \frac{\varphi(n)}{2^{\alpha} m_1 \cdots m_r}$$

The above inequality shows that the proof of the theorem is complete if $\beta = 1$. Hence without loss of generality it can be assumed that $\beta \geq 2$. It follows from the definition of J that for all $i, j \in J$, $e_i = e_j$; let e^* be the common value of the e_j's, for $j \in J$. Put $\gamma_j' = f_j + 1$ (where f_j was defined above) and notice

that for $j \in J$ the value of f_j, and hence of γ'_j, does not depend on j; let γ be the common value of the γ'_j's, for $j \in J$. It is now clear that

$$\frac{t_j}{2} | d(\gamma) \text{ and } t_j \not| d(\gamma)$$

On the other hand using congruence (14) it is true that for all $j \in J$,

$$b^{d(\gamma)} \equiv 1 \bmod q_j \Leftrightarrow \varphi(q_j) | h_j m_j d(\gamma) \Leftrightarrow t_j | h_j d(\gamma).$$

However $b \in Z_n^* - R_n$ and hence $\gcd(b^{d(\gamma)} - 1, n) = 1$ or n. It follows that either $(\forall j \in J)(2 | h_j)$ or $(\forall j \in J)(2 \not| h_j)$. Since $(\forall i \in I)(2^{\alpha_i} | h_i)$, the proof of the theorem is complete •

As a first corollary it can be shown that

Theorem 17.4 *(**Rabin**) For all odd composite integers $n > 9$,*

$$\frac{|Z_n^* - R_n|}{\varphi(n)} \leq \frac{1}{4}$$

Proof: If $r \geq 3$ the theorem follows from theorem 17.3. If $r = 2$ then $\alpha + \beta - 1 \geq 1$. Hence the theorem follows from theorem 17.3 if either $m_1 = 2$ or $m_2 = 2$. Assume on the contrary that $m_1 = m_2 = 1$. This last statement implies that $n = p_1 p_2$. Say $p_1 < p_2$. Then $p_2 - 1 = \varphi(p_2) | n - 1 = p_1(p_2 - 1) + (p_1 - 1)$, which is a contradiction. It remains to prove the theorem in the case $r = 1$. Let $n = p^t$, some $t \geq 2$. But

$$|Z_n^* - R_n| \leq |\{b \in Z_n^* : b^{n-1} \equiv 1 \bmod n\}| \leq \gcd(n - 1, p - 1) = p - 1.$$

It follows that

$$\frac{|Z_n^* - R_n|}{\varphi(n)} \leq \frac{p - 1}{p^{t-1}(p - 1)} = \frac{1}{p^{t-1}}.$$

Since $n > 9$ the proof of theorem is complete •

Another corollary is

Theorem 17.5 *For all odd integers $n > 2$, if r is the number of distinct prime factors of n then*

$$\frac{|Z_n^* - R_n|}{\varphi(n)} \leq \frac{1}{2^{r-1}} \bullet$$

18 Rumeley-Adleman Test

The Rumeley-Adleman algorithm (abbreviated by RA) is different from the previously considered probabilistic primality tests. Given as input an odd integer $n > 1$, $RA(n)$ may not converge; however if $RA(n)$ converges then the test gives the correct answer.

Throughout the proof below n will be an odd integer > 1. For each prime p let $\varsigma_p = \exp(2\pi i/p)$ be a primitive p–th root of unity and consider the cyclic group $G_p = \{\varsigma_p^i : 0 \leq i \leq p-1\}$. Let p, q be primes such that $p|q-1$ and consider a character $\chi_{p,q} = \chi : Z_q^* \to G_p$ of Z_q^* onto G_p. Such characters exist (e.g. let g be a generator of Z_q^* and put $\chi(g^x \bmod q) = \varsigma_p^x$), which is well defined since $p|q-1$, and are called **characters of order p and conductor q**. Further, consider the ring $Z[\varsigma_p, \varsigma_q]$.

For each character χ of order p and conductor q the **generalized Gaussian sum** is defined by

$$G(a,\chi) = -\sum_{i=1}^{q-1} \chi(i)\varsigma_q^{ia}, \text{ where } a \in Z_q^*.$$

The **Gaussian sum** is defined by $G(\chi) = G(1,\chi)$.

Now one can prove the following

Lemma 18.1 *Let $\chi : Z_q^* \to G_p$ be a character of order p and conductor q, where $p|q-1$. Then for any odd integer r the following statements hold:*

(1) $G(a,\chi) = \overline{\chi(a)} \cdot G(\chi)$, *for* $a \in Z_q^*$.

(2) $G(\chi) \cdot \overline{G(\chi)} = q$.

(3) $G(\chi)^r \equiv \chi(r)^{-r} \cdot G(\chi^r) \bmod(rZ[\varsigma_p, \varsigma_q])$

Proof: The proof of (1) is immediate from the equations below

$$G(a,\chi) = -\sum_{i=1}^{q-1} \chi(ia)\overline{\chi(a)}\varsigma_q^{ia} = \overline{\chi(a)}G(\chi).$$

To prove (2) notice that for $a \in Z_q^*$, $\sum_{i=1}^{q-1} \varsigma_q^{ia} = (\varsigma_q^{aq} - 1)/(\varsigma_q^a - 1) = 0$. Hence,

$$G(\chi)\overline{G(\chi)} = -G(\chi)\sum_{i=1}^{q-1} \overline{\chi(i)}\varsigma_q^{-i} = -\sum_{i=1}^{q-1} \varsigma_q^{-i} G(i,\chi) = \sum_{i,j=1}^{q-1} \chi(j)\varsigma_q^{i(j-1)} = q.$$

It is easy to show that if congruence (3) holds for each of the integers r, s then it must also hold for their product $r \cdot s$. Hence without loss of generality it is enough to prove (3) when r is prime. Using the binomial theorem it can be shown that

$$G(\chi)^r = -\left(\sum_{i=1}^{q-1} \chi(i)\varsigma_q^i\right)^r \equiv -\sum_{i=1}^{q-1} \chi(i)^r \varsigma_q^{ir} \equiv$$

$$-\chi(r)^{-r}\sum_{i=1}^{q-1} \chi(ir)^r \varsigma_q^{ir} \equiv \chi(r)^{-r} G(\chi^r) \bmod(rZ[\varsigma_p, \varsigma_q]) \bullet$$

The next lemma is basic for the proof of the Rumeley-Adleman test.

Lemma 18.2 *Let $\chi : Z_q^* \to G_p$ be a character of order p and conductor q, where $p|q-1$ and $\gcd(pq,n)=1$. Then for any odd integer r one can show that*

(1) If there exists an $\eta(\chi) \in G_p$ such that

$$G(\chi)^r \equiv \eta(\chi)^{-r} G(\chi^r) \bmod(rZ[\varsigma_p, \varsigma_q]) \tag{15}$$

$$\text{then } \eta(\chi) \equiv G(\chi)^{r^{p-1}-1} \bmod(rZ[\varsigma_p, \varsigma_q]).$$

(2) In particular,

$$\chi(r) \equiv G(\chi)^{r^{p-1}-1} \bmod(rZ[\varsigma_p, \varsigma_q]).$$

Proof: Clearly (2) is an immediate consequence of (1) and part (3) of lemma 18.1. To prove part (1) apply the homomorphism of $Z[\varsigma_p, \varsigma_q]$, which carries ς_p to $\varsigma_p^{r^i}$ and ς_q to ς_q, to congruence (15) above to obtain

$$G(\chi^{r^i})^r \equiv \eta(\chi)^{-r^{i+1}} G(\chi^{r^{i+1}}) \bmod(rZ[\varsigma_p, \varsigma_q]). \tag{16}$$

Using this and induction on i it follows easily that

$$G(\chi)^{r^i} \equiv \eta(\chi)^{-ir^i} G(\chi^{r^i}) \bmod(rZ[\varsigma_p, \varsigma_q]). \tag{17}$$

Now apply congruence (17) to $i = p-1$ and use $G(\chi) \cdot \overline{G(\chi)} = q$ to obtain the desired result •

Let $r|n$ be such that $\nu_p(r^{p-1}-1) \geq \nu_p(n^{p-1}-1)$. Then $(r^{p-1}-1)/(n^{p-1}-1)$ is a fraction of the form $(p^k a)/b$, where a, b are relatively prime to p and $k \geq 0$. Hence b is invertible in Z_p^* and it makes sense to define

$$\ell_p(r) \equiv \frac{r^{p-1}-1}{n^{p-1}-1} \bmod p$$

It is clear that $\ell_p(n) = 1$. If one uses

$$(rs)^{p-1} - 1 = (r^{p-1}-1)(s^{p-1}-1) + (r^{p-1}-1) + (s^{p-1}-1)$$

then it can be shown easily that

Lemma 18.3 *Assume that $\gcd(p,n)=1$ and that for all primes $r|n$,*

$$\nu_p(r^{p-1}-1) \geq \nu_p(n^{p-1}-1). \tag{18}$$

Then for all integers $r, s|n$, $\ell_p(rs) \equiv \ell_p(r) + \ell_p(s) \bmod p$ •

Lemma 18.4 *Let p be a prime such that $\gcd(p,n)=1$. Assume there exists a character $\chi : Z_q^* \to G_p$ of order p and conductor q such that $\gcd(pq,n)=1$ and $p|q-1$. If there exists an $\eta(\chi) \in G_p$ such that $\eta(\chi) \neq 1$ and*

$$G(\chi)^n \equiv \eta(\chi)^{-n} G(\chi^n) \bmod(nZ[\varsigma_p, \varsigma_q]) \tag{19}$$

then one can prove that for all $r|n$,

(1) $\nu_p(r^{p-1}-1) \geq \nu_p(n^{p-1}-1)$

(2) $\chi(r) \equiv \eta(\chi)^{\ell_p(r)} \bmod(rZ[\zeta_p,\zeta_q])$

(3) $\chi(n) = \eta(\chi)$ *and* $\chi(r) \equiv \chi(n)^{\ell_p(r)} \bmod(rZ[\zeta_p,\zeta_q])$

Proof: It follows from lemma 18.2 (for $r = n$) that

$$\eta(\chi) \equiv G(\chi)^{n^{p-1}-1} \bmod(nZ[\zeta_p,\zeta_q]).$$

Assume that $r|n$.

Let a be the order of $G(\chi)$ in $Z[\zeta_p,\zeta_q]/nZ[\zeta_p,\zeta_q]$. Since $\eta(\chi) \neq 1$, $a \not| n^{p-1}-1$. Since $\eta(\chi)^p = 1$, $a|p(n^{p-1}-1)$. In addition lemma 18.2 implies that $1 \equiv \chi(r)^p \equiv G(\chi)^{p(r^{p-1}-1)} \bmod(rZ[\zeta_p,\zeta_q])$. Hence it follows that $a = \nu_p(p(n^{p-1}-1)) \leq \nu_p(p(r^{p-1}-1))$ and the proof of (1) is complete.

To prove part (2) write $(r^{p-1}-1)/(n^{p-1}-1) = a/b$, where $a, b > 0$ and $b \equiv 1 \bmod p$. It is then clear that $\ell_p(r) \equiv a \bmod p$ and hence

$$\chi(r) \equiv \chi(r)^b \equiv G(\chi)^{b(r^{p-1}-1)} \equiv G(\chi)^{a(n^{p-1}-1)} \equiv$$

$$\eta(\chi)^a \equiv \eta(\chi)^{\ell_p(r)} \bmod(nZ[\zeta_p,\zeta_q])\bullet$$

For each integer t let

$$s(t) = \prod\{q : q-1|t \text{ and } q \text{ is prime}\} > \sqrt{n}.$$

To study the running time of the Rumeley-Adleman algorithm one needs the following result from analytic number theory (see [APR].)

Theorem 18.1 ***(Odlyzko-Pomerance)*** *There is a constant $c > 0$ which is effectively computable such that for all integers $n > e^e$, there is an integer*

$$0 < t < (\log n)^{c \log\log\log n}$$

(which is not actually constructed in the proof) such that $s(t) > \sqrt{n}$ •

Now it is possible to state the Rumeley-Adleman algorithm.

Input: n odd > 1.

Step 1: Try the integers $t = 0, 1, \ldots,$ until you compute an integer t such that $s(t) > \sqrt{n}$.

Step 2: Put $s = s(t)$ and confirm $\gcd(st, n) = 1$.

Step 3: For any prime $p|t$ **do**

1. If $n^{p-1} \not\equiv 1 \bmod p^2$ then **go to** Step 4.

2. If $n^{p-1} \equiv 1 \bmod p^2$ then **do**

   (a) select $q|s$ such that $p|q-1$

(b) select a character $\chi : Z_q^* \rightarrow G_p$ of order p and conductor q and verify that $G(\chi)^n \equiv \eta(\chi)^{-n} G(\chi^n) \bmod(nZ[\zeta_p, \zeta_q])$ holds for some $\eta(\chi) \in G_p - \{1\}$.

If for each $p|t$ either 1. holds or a q can be found such that 2. holds, then **go to** Step 4.

Step 4: For each $i = 0, 1, \ldots, s-1$ compute $\gcd(n^i \bmod s, n)$.

Output:

$$RA(n) = \begin{cases} \text{PRIME} & \text{if } (\forall i < s)(\gcd(n^i \bmod s, n) = 1 \text{ or } n) \\ \text{COMPOSITE} & \text{if } (\exists i < s)(1 < \gcd(n^i \bmod s, n) < n) \end{cases}$$

It is clear that the algorithm may not terminate but instead run forever in Step 3. However it can be shown that

Theorem 18.2 *(***Rumeley-Adleman***) For all odd integers $n > 1$, if $RA(n)$ terminates then the following statements are equivalent:*

(1) *n is prime.*

(2) *$RA(n) = PRIME$.*

Moreover, if $RA(n)$ terminates then the number of steps needed to output the answer is $O\left((\log n)^{c \log\log\log n}\right)$.

Proof: Assume on the contrary that $RA(n) = \text{PRIME}$ but that n is composite. Let r be a prime divisor of n such that $r \leq \sqrt{n}$. Let t be an integer such that $s = s(t) > \sqrt{n}$ and suppose that $\gcd(st, n) = 1$. Since $RA(n)$ converges the integer n passes the test in step 3. It follows from lemma 18.4 that $\nu_p(k^{p-1} - 1) \geq \nu_p(n^{p-1} - 1)$, for all $k|n$. Hence $\ell_p(k)$ is defined for all $k|n$. Use the Cinese Remainder theorem to find an integer $\ell(r) \in \{0, 1, \ldots, s-1\}$ such that for all prime divisors p of t, $\ell(r) \equiv \ell_p(r) \bmod p$. It follows from parts (2), (3) of lemma 18.4 that for any character $\chi : Z_q^* \rightarrow G_p$ of order p and conductor q (such that $p|q-1$),

$$\chi(r) = \chi(n^{\ell(r)}).$$

However, such characters generate the group $Char(Z_s^*)$ of characters modulo s (which is isomorphic to Z_s^*.) It follows from the duality theorem of the theory of characters (see [KP], page 129 or [Cohn], page 24) that $r \equiv n^{\ell(r)} \bmod s$. But this is a contradiction since $1 < r = \gcd(n^{\ell(r)} \bmod s, n) < n$. The other direction is easy. If the test declares n composite (i.e. $RA(n) = \text{COMPOSITE}$) then n must be composite •

Lenstra in [Len2] has observed that the integer $s(t)$ used in the proof of the Rumeley - Adleman algorithm can in fact be replaced with

$$e(t) = 2 \cdot \prod \{q^{\nu_q(t)+1} : q - 1 | t \text{ and } q \text{ is prime}\}.$$

Details of the proof (which is similar to the above proof) have been carried out by H. Cohen in [Cohe]. In addition Lenstra has pointed out that condition

$e(t) > \sqrt{n}$ can in fact be replaced by $e(t) > n^{1/3}$. Although both of these observations are useful for applications they do not alter the theoretical bound $O\left((\log n)^{c \log\log\log n}\right)$. In practice one need only form a table of values of $e(t)^2$ (see [Cohe], page 31.)

t	$e(t)^2$
$60 = 2^2 35$	$4.64\ E\ 19$
$1,260 = 2^2 3^2 57$	$1.31\ E\ 62$
$10,080 = 2^5 3^2 57$	$1.83\ E\ 128$
$55,440 = 2^4 3^2 5711$	$2.42\ E\ 213$
$166,320 = 2^4 3^3 5711$	$4.88\ E\ 313$

Figure 3: Table of Values of $e(t)^2$

The table in Figure 3 shows that to test the primality of a 200 digit integer one need only factor integers $t < 55,440$ (by all means an easy task) and then use the Rumeley - Adleman algorithm. According to [SciCit] this algorithm can be used to test the primality of an arbitrary 97 digit number in 78 seconds of computer time.

19 Bibliographical Remarks

Eratosthenes developed the sieve method in the 3rd century BC. The observation that one need only run the algorithm for $p \leq \sqrt{n}$ is due to Pisano (1202); this was also oserved by Ibn Albanna (end of 13th century.) For more details see [Di]. A discussion of the limits of the sieve method can be found in [Se]. In [Rad] a double sieve method is applied to show that $\sum\{1/p+1/(p+2)\}$ converges, where the sum ranges over primes p such that $p+2$ is also a prime. The reader should also consult [Haw] for the notion of random sieve. In addition exercise 8 in section 4.5.4 of [Kn] is relevant. Barinaga's theorem is an immediate application of Wilson's theorem and is stated in page 428 of [Di]. Pratt's test was first proved in [Pra]. For more information see [Len1].

Gauss was the first to state that Fermat's assertion that every F_n is prime is false. It is not known if there exist infinitely many Fermat primes or infinitely many Fermat composites. Fermat numbers play an important role in Gauss' theorem: a regular polygon of m sides can be inscribed in a circle if and only if m is the product of distinct Fermat primes and a power of 2 (see [Va].) The present proof of the Lucas-Lehmer test is due to Lenstra (see [Len1].) The traditional proof uses Lucas functions and can be found in [Kn], page 391 or better yet in [Wi]. In addition [Wi] gives an excellent survey of Lehmer functions and generalized Lehmer sequences.

For more information on the Riemann Zeta function and the Extended Riemann Hypothesis the reader should consult [KP], [Prac], [T], [Da]. The proof of Ankeny-Montgomery's theorem can be found in [Mont]. The idea of the proof of the Solovay-Strassen deterministic test is from [SoSt]. The deterministic test in subsection 11 is inspired from the Selfridge-Weinberger test and unlike the Solovay-Strassen test it makes no mention of the Jacobi symbol. Miller was the first to show that under the Extended Riemann Hypothesis there is a polynomial time algorithm to test primality The original proof of Miller's test uses the Carmichael function (see [Mil], [An].) The present proof is from [Mig] and [Len3]; the last reference also includes the proof of lemma 13.1.

The probabilistic Solovay-Strassen test comes from [SoSt] and Rabin's test from [Rab]. Theorem 17.3 is from [Kran]. In addition Monier in [Moni] compares the performance of the last two probabilistic tests. The first proof of the Rumeley-Adleman test was published in [Ad]. The proof given here is essentially due to Lenstra (see [Len1], [Len2], [Cohe].)

An interesting history of the machines used since 1925 for factoring and testing primality can be found in [BLSTW] .

Bibliography

[Ad] Adleman, L., On Distinguishing Prime Numbers from Composite Numbers, 21-st IEEE FOCS, 1980, pp. 387-406.

[APR] Adleman, L., Pomerance, C., Rumeley, R., On Distinguishing Prime Numbers from Composite Numbers, Annals of Mathematics, 117 (1983), pp. 173 - 206.

[An] Angluin, Dana, Lecture Notes on the Complexity of Some Problems in Number Theory, Yale University, Department of Computer Science, August, 1982, 243.

[BLSTW] Brillhart, J., Lehmer, D.H., Selfridge, J.L., Tuckerman, B., and Wagstaff Jr, S.S., Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers, pp. xxvii - lxi, Contemporary Mathematics, Vol. 22, American Mathematical Society, 1983, Providence, RI.

[Cohe] Cohen, H., Tests de Primalite d' après Adleman, Rumeley, Pomerance et Lenstra, Séminaire de Theories des Nombres, Grenoble, June 1981.

[Cohn] Cohn, H., Advanced Number Theory, Dover Publication, New York, 1962.

[Da] Davenport, H., Multiplicative Number Theory, 2nd edition, Springer Verlag Graduate Texts in Mathematics, Heidelberg 1980.

[Di] Dickson, L. E., History of the Theory of Numbers, Vol. 1, Chelsea, New York, 1952.

[Gar] Gardner, M., The Remarkable Lore of the Prime Numbers, In: Mathematics an Introduction to its Spirit and Use, M. Kline editor, W. H. Freeman and Company, 1979, pp. 49 - 54, San Fransisco.

[Gr] Grosswald, E., Topics from the Theory of Numbers, Birkäuser Verlag, 1984.

[Haw] Hawkins, D., Mathematical Sieves, In: Mathematics an Introduction to its Spirit and Use, M. Kline editor, W. H. Freeman and Company, 1979, pp. 55 - 62, San Fransisco.

[Kn] Knuth, D. E., The Art of Computer Programming: Seminumerical Algorithms, Addison-Wesley, Vol. II, 1981, Reading Mass.

[KP] Koch H. and Pieper H., Zahlentheorie, VEB Deutscher Verlag der Wiss., 1976, Berlin.