PRIMALITY PROVING WITH GAUSS AND JACOBI SUMS

Andrzej Chmielowiec
Enigma Information Security Systems Sp. z o.o.
8 Cietrzewia Str., 02-492 Warsaw, Poland
E-mail: achmielowiec@enigma.com.pl

ABSTRACT

This article presents a primality test known as APR (Adleman, Pomerance and Rumely) which was invented in 1980. It was later simplified and improved by Cohen and Lenstra. it can be used to prove primality of numbers with thousands of bits in a reasonable amount of time. The running time of this algorithm for number N is $O((\ln N)^{C \ln\ln\ln N})$ for some constant C. This is almost polynomial time since for all practical purposes the function $\ln\ln\ln N$ acts like a constant.

1 INTRODUCTION

Probabilistic primality tests are in fact compositness tests. That kind of test gives us correct answer only if the number has nontrivial factor. In other words this test gives two possible answers:

1. number is composite,
2. number may be prime.

In the former case we are absolutely sure that the number is composite, but in the latter one we receive only statistical information. That kind of unsertainty can be accepted in RSA users keys. Situation is completely different with certificate authority keys and elliptic curve parameters. In those cases wrong verification of primality may compromise all keys in cryptosystem.

We can avoid this problem using algorithm which proves primality and always gives correct answer. There are two very effective methods of primality proving. One of them gives primality certificate and is based on elliptic curves [AM93]. The second one – Gauss and Jacobi sums primality test [APR83] – is the topic of this paper. The test based on Gauss sums [BS96], [CP01] is interesting only from theoretical point of view and it doesn't have practical implications. Its improvement – Jacobi sums test [BvdH90], [Coh93] – is much more efficient and can be used to prove primality of numbers with thousands of bits in a reasonable amount of time.

In the following sections we will show how the theoretical results can be interpreted in terms of computer programming. It will allow to understand the basic idea of Jacobi sums method and will be helpful for those who will try to implement this test in practice. The article does not contain any proof, as it can be easily found in references. Probably the best theoretical description of this algorithm can be found in Henri Cohen's book [Coh93].

2 THEORETICAL BACKGROUND

In the whole article we will use the following notation:

N	number which is tested for primality,
p, q	small prime numbers.

2.1 Cyclotomic fields

We start from definition of algebraic structure in which the test operations are performed.

Definition 1 If $\zeta_n \in \mathbb{C}$ is such that $\zeta_n^n = 1$ and for all $k < n$ we have $\zeta_n^k \neq 1$, then ζ_n is a primitive n-th root of unity, and field extension $\mathbb{Q}(\zeta_n)$ is the n-th cyclotomic field. □

Proposition 1 Let $K = \mathbb{Q}(\zeta_n)$ be n-th cyclotomic field.

1. The extension $K/\mathbb{Q}$ is a Galois extension, with Abelian Galois group given by

$$G = \text{Gal}(K/\mathbb{Q}) =$$

$$\{\sigma_a : \ (a,n) = 1, \ \text{where } \sigma_a(\zeta_n) = \zeta_n^a\}.$$

   In particular, the degree of $K/\mathbb{Q}$ is $\phi(n)$, where ϕ is the Euler function.

2. The ring of integers of K is $\mathbb{Z}_K = \mathbb{Z}[\zeta_n]$.

■

Such a definition is good from a theoretical point of view, but is also completely impractical. We need to find a way that would allow us to represent elements of $\mathbb{Q}(\zeta_n)$ and $\mathbb{Z}[\zeta_n]$ in a computer. This is possible by the definition of a cyclotomic polynomial

$$\Phi_n(X) = \prod_{(a,n)=1,\ 0<a<n} (X - \zeta_n^a).$$

It is possible to show that $\Phi_n(X) \in \mathbb{Z}[X]$ and the following lemma is true.

Lemma 1 If ζ_n is a primitive n-th root of unity, and $\Phi_n(X)$ is the n-th cyclotomic polynomial, then

$$\begin{aligned} \mathbb{Q}(\zeta_n) &\simeq \mathbb{Q}[X]/\Phi_n(X), \\ \mathbb{Z}[\zeta_n] &\simeq \mathbb{Z}[X]/\Phi_n(X). \end{aligned}$$

This isomorphism fixes elements of $\mathbb{Q}$, and sends ζ_n on to X. ■

In this approach we only need to compute the n-th cyclotomic polynomial. The following formula gives us a very effective way to do this for small values of n

$$\Phi_n(X) = \prod_{d|n} \left(1 - X^{\frac{n}{d}}\right)^{\mu(d)}, \qquad (\star)$$

where $\mu(d)$ is the Möbius function

$$\mu(d) = \begin{cases} 1 & \text{if } d = 1, \\ (-1)^k & \text{if } d \text{ is product of } k \text{ distinct primes,} \\ 0 & \text{in other cases.} \end{cases}$$

Example 1 Using formula $(\star)$ for a prime or a power of prime, we can easily compute cyclotomic polynomials

$$\begin{aligned} \Phi_p(X) &= \frac{1 - X^p}{1 - X} = \sum_{i=0}^{p-1} X^i \\ &= X^{p-1} + \cdots + X + 1, \\ \Phi_{p^k}(X) &= \frac{1 - X^{p^k}}{1 - X^{p^{k-1}}} = \sum_{i=0}^{p-1} X^{ip^{k-1}} \\ &= X^{(p-1)p^{k-1}} + \cdots + X^{p^{k-1}} + 1. \end{aligned}$$

□

The main part of Jacobi sums test will be based on computations in the ring $\mathbb{Z}[\zeta_{p^k}]$. It is known from Lemma 1 that $\mathbb{Z}[\zeta_{p^k}] \simeq \mathbb{Z}[X]/\Phi_{p^k}(X)$, and $\Phi_{p^k}(X)$ can be computed from $(\star)$. The next example shows how to do arithmetic operations in such a ring.

Example 2 Let $p = 2$, and $k = 2$. The previous considerations lead us to

$$\mathbb{Z}[\zeta_4] \simeq \mathbb{Z}[X]/\Phi_4(X),$$

where $\Phi_4(X) = X^2 + 1$. Of course every element of $\mathbb{Z}[X]/\Phi_4(X)$ may be represented as polynomial of degree $< \deg(\Phi_4)$. Suppose that

$$\begin{aligned} a(X) &= a_1X + a_0, \\ b(X) &= b_1X + b_0 \end{aligned}$$

are such representations. Addition and subtraction can be done by coordinates

$$a(X) \pm b(X) = (a_1 \pm b_1)X + (a_0 \pm b_0).$$

Multiplication is a little bit more complicated. To do this we first have to compute $a(X)b(X)$ in $\mathbb{Z}[X]$, and then reduce the product modulo $\Phi_4(X)$. Since $(a_1X+a_0)(b_1X+b_0) \mod (X^2+1) = a_1b_1X^2 + (a_1b_0 + a_0b_1)X + a_0b_0 \mod (X^2+1) = (a_1b_0 + a_0b_1)X + (a_0b_0 - a_1b_1)$, then we have

$$a(X)b(X) = (a_1b_0 + a_0b_1)X + (a_0b_0 - a_1b_1).$$

□

2.2 Group rings

In the previous section Galois group of extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ was defined as

$$G = \{\sigma_a :\ (a, n) = 1, \text{ where } \sigma_a(\zeta_n) = \zeta_n^a\}.$$

If we interpret $\mathbb{Q}(\zeta_n)$ as $\mathbb{Q}[X]/\Phi_n(X)$ then every element $\sigma_a \in G$ can be written as $\sigma_a(X) = X^a \mod \Phi_n(X)$. Group G is in fact the group of automorphisms of the field $\mathbb{Q}(\zeta_n)$ which fixes the base field $\mathbb{Q}$ [Rot90]. There is a natural action of G on $\mathbb{Q}(\zeta_n)$ and $\mathbb{Z}[\zeta_n]$.

Example 3 Consider $\mathbb{Q}(\zeta_4) \simeq \mathbb{Q}[X]/(X^2 + 1)$ a Galois group of extension $\mathbb{Q}(\zeta_4)/\mathbb{Q}$ is defined as

$$G = \{\sigma_1, \sigma_3\} \simeq (\mathbb{Z}/4\mathbb{Z})^*.$$

Let $b(X) = b_1X + b_0$ be the representation of element from $\mathbb{Q}[X]/(X^2 + 1)$. Since every $\sigma_a \in G$ fixes $\mathbb{Q}$ elements, we have

$$\begin{aligned} \sigma_1(b(X)) &= b_1\sigma_1(X) + b_0 \\ &= b_1X + b_0, \\ \sigma_3(b(X)) &= b_1\sigma_3(X) + b_0 \\ &= b_1X^3 + b_0 \mod (X^2 + 1) \\ &= -b_1X + b_0. \end{aligned}$$

The same is true if $b(X) \in \mathbb{Z}[X]/(X^2 + 1)$. □

Now we will introduce the ring of $\mathbb{Z}$-linear combinations of elements of G. This structure plays a crucial role in the extension of Gauss sums test to Jacobi sums test, and it allows to apply the latter in practice.

Definition 2 Define group ring $\mathbb{Z}[G]$ as the set of elements $f = \sum_{\sigma \in G} f_\sigma \sigma$, where all $f_\sigma \in \mathbb{Z}$. Operations in $\mathbb{Z}[G]$ are defined in the following way

$$\begin{aligned} f \pm g &= \sum_{\sigma \in G} (f_\sigma \pm g_\sigma)\sigma, \\ f \cdot g &= \sum_{\sigma,\tau \in G} (f_\sigma g_\tau)(\sigma\tau). \end{aligned}$$

□

Addition and subtraction is in $\mathbb{Z}[G]$ defined by coordinates. Multiplication is a little bit more complicated. The following example explains how to do this operation.

Example 4 Consider group ring $\mathbb{Z}[G]$ with G defined as in previous example $G = \{\sigma_1, \sigma_3\} \simeq (\mathbb{Z}/4\mathbb{Z})^*$. The following table presents group law for G

$\cdot$	σ_1	σ_3
σ_1	σ_1	σ_3
σ_3	σ_3	σ_1

If $f = f_1\sigma_1 + f_3\sigma_3$ and $g = g_1\sigma_1 + g_3\sigma_3$ are elements of $\mathbb{Z}[G]$, then we have

$$\begin{aligned} f \pm g &= (f_1 \pm g_1)\sigma_1 + (f_3 \pm g_3)\sigma_3, \\ f \cdot g &= (f_1g_1)(\sigma_1\sigma_1) + (f_1g_3)(\sigma_1\sigma_3) + \\ &\quad (f_3g_1)(\sigma_3\sigma_1) + (f_3g_3)(\sigma_3\sigma_3) \\ &= (f_1g_1)\sigma_1 + (f_1g_3)\sigma_3 + \\ &\quad (f_3g_1)\sigma_3 + (f_3g_3)\sigma_1 \\ &= (f_1g_1 + f_3g_3)\sigma_1 + (f_1g_3 + f_3g_1)\sigma_3. \end{aligned}$$

□

Now we are ready to extend group action given by G to action given by $\mathbb{Z}[G]$.

Definition 3 Let G be a Galois group of extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, and $\mathbb{Z}[G]$ denote its group ring. If $f \in \mathbb{Z}[G]$ and $x \in \mathbb{Q}(\zeta_n)$, then we define action of f on x by

$$x^f = \prod_{\sigma \in G} \sigma(x)^{f_\sigma}$$

for $x \neq 0$, and $0^f = 0$. □

This definition is quite natural and it has very nice properties. One can immediately check, that for all $x, x_1, x_2 \in \mathbb{Q}(\zeta_n)$ and $f, f_1, f_2 \in \mathbb{Z}[G]$ we have

1. $x^{f_1+f_2} = x^{f_1}x^{f_2}$,
2. $x^{f_1f_2} = \left(x^{f_1}\right)^{f_2} = \left(x^{f_2}\right)^{f_1}$,
3. $(x_1 + x_2)^f = x_1^f + x_2^f$,
4. $(x_1x_2)^f = x_1^f x_2^f$.

Example 5 Let $a(X) = a_1X + a_0$ represent an element of $\mathbb{Q}(\zeta_4) \simeq \mathbb{Q}[X]/(X^2 + 1)$, then for $f = \sigma_1 + \sigma_2$ we can obtain

$$\begin{aligned} a(X)^f &= \sigma_1(a_1X + a_0)\sigma_3(a_1X + a_0) \\ &= -a_1^2X^2 + a_0^2 \mod (X^2 + 1) \\ &= a_1^2 + a_0^2, \end{aligned}$$

and for $g = 2\sigma_1 + \sigma_3$ we have

$$\begin{aligned} a(X)^g &= a(X)^{\sigma_1+f} \\ &= \sigma_1(a_1X + a_0)(a_1^2 + a_0^2) \\ &= (a_1^3 + a_0^2a_1)X + (a_0a_1^2 + a_0^3). \end{aligned}$$

□

The most interesting is the case of $n = p^k$, where p is prime. The following proposition shows the relation which will be usful in the next section.

Proposition 2 If $n = p^k$ and $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, then the set

$$\mathfrak{p} = \{f \in \mathbb{Z}[G] : \zeta_p^f = 1\}$$

is a prime ideal of group ring $\mathbb{Z}[G]$. ■

2.3 Dirichlet characters

Dirichlet character χ modulo q is a group homomorphism from $(\mathbb{Z}/q\mathbb{Z})^*$ to $\mathbb{C}^*$. If q is prime then character χ can be defined by choosing value $\chi(g)$ for some generator g of $(\mathbb{Z}/q\mathbb{Z})^*$.

Example 6 If $q = 5$, then $g = 2$ is a generator of $(\mathbb{Z}/5\mathbb{Z})^*$, and all Dirichlet characters may be defined by choosing value for $\chi(g)$. But χ must be a homomorphism, so its image has to be a multiplicative subgroup of order four in $\mathbb{C}^*$. There are only four such possibilities

1. $\chi_1(g) = 1$ (trivial character),
2. $\chi_2(g) = -1$,
3. $\chi_3(g) = i$,
4. $\chi_4(g) = -i$.

□

It can be shown, that the set of all characters modulo q forms a group.

Proposition 3 All characters from $(\mathbb{Z}/q\mathbb{Z})^*$ to $\mathbb{C}^*$ form a group with neutral element χ_0 such that $\chi_0(x) = 1$ for all $x \in (\mathbb{Z}/q\mathbb{Z})^*$. ■

Since χ is a homomorphism and $|(\mathbb{Z}/q\mathbb{Z})^*| < \infty$ one can show that the set of character values forms a multiplicative group which is a subgroup of $\langle\zeta_q\rangle = \langle e^{\frac{2\pi i}{q}}\rangle$. Definition of character may be extended to a multiplicative map from $\mathbb{Z}/q\mathbb{Z}$ to $\mathbb{C}$ by taking $\chi(x) = 0$ for all $x \notin (\mathbb{Z}/q\mathbb{Z})^*$. It can then be lifted to map from $\mathbb{Z}$ to $\mathbb{C}$. More information about characters can be found in [IR90].

2.4 Gauss and Jacobi sums

We are now ready to give the definition and some basic properties of Gauss and Jacobi sums.

Definition 4 1. Let χ be a character modulo q. The Gauss sum $\tau(\chi)$ is defined by

$$\tau(\chi) = \sum_{x\in(\mathbb{Z}/q\mathbb{Z})^*} \chi(x)\zeta_q^x,$$

where $\zeta_q = e^{\frac{2\pi i}{q}}$.

2. Let χ_1, χ_2 be two characters modulo q. The Jacobi sum $j(\chi_1, \chi_2)$ is defined by

$$j(\chi_1, \chi_2) = \sum_{x\in(\mathbb{Z}/q\mathbb{Z})^*} \chi_1(x)\chi_2(1-x).$$

□

There is a nontrivial connection between those two objects. It allows us to implement our primality proof in a very effective way.

Proposition 4 Let χ_1, χ_2 be characters modulo q such that $\chi_1\chi_2 \neq \chi_0$. Then

$$j(\chi_1, \chi_2) = \frac{\tau(\chi_1)\tau(\chi_2)}{\tau(\chi_1\chi_2)}.$$

■

It is clear that if χ is a character modulo prime number q, then its values belong to some group $\langle\zeta_n\rangle$, where $n \mid q-1$. But it means that $\tau(\chi) \in \mathbb{Z}[\zeta_n, \zeta_q]$ and $j(\chi_1, \chi_2) \in \mathbb{Z}[\zeta_n]$. The second ring is simpler and has smaller cost of arithmetic operations. The next section will show how to use it to effectively implement the primality test.

3 PRIMALITY TEST

The previous section presented the theoretical basis of Jacobi sums test concept. Now we will try to sum up the theory and show how it can be used in the construction of a primality proving algorithm. It will be done in two steps. The first step describes an impractical algorithm based on Gauss sums (that are located in a large ring). The second one uses particular properties of Jacobi sums to move computations into a smaller ring, where Gauss sums are replaced by Jacobi sums.

We assume that N has already passed the Rabin-Miller test and it is highly improbable that N is composite. Our aim is the proof of primality of N. In this section we fix prime numbers p, q such that $p^k \mid q-1$ and $p^{k+1} \nmid q-1$. Let χ be character modulo q of order $n = p^k$ in the group of characters.

3.1 Basic test

The fundamental concept is to prove a generalization of Fermat's little theorem. It allows us to verify many congruences that are satisfied by prime numbers and together imply primality of the tested number.

Proposition 5 Let $\beta \in \mathbb{Z}[G]$. Then if N is prime, there exists $\eta(\chi) \in \langle\zeta_n\rangle$ such that

$$\tau(\chi)^{\beta(N-\sigma_N)} \equiv \eta(\chi)^{-\beta N} \mod N, \qquad (\star_\beta)$$

where $\eta(\chi) = \chi(N)$. ■

Note that $\mathbb{Z}[G]$ acts not only on $\mathbb{Z}[\zeta_n]$ but also on $\mathbb{Z}[\zeta_n, \zeta_q]$. But it doesn't matter because action on ζ_q is trivial (identity action). In the final version of the test, the congruence $(\star_\beta)$ in $\mathbb{Z}[\zeta_n, \zeta_q]$ will be transformed to equivalent condition in $\mathbb{Z}[\zeta_n]$. So results of this section are important only from the theoretical point of view and it is unnecessary to give examples of operations in $\mathbb{Z}[\zeta_n, \zeta_q]$.

In order to present the main result of this section, first we have to define the so called $\mathcal{L}_p$ condition.

Definition 5 Condition $\mathcal{L}_p$ is satisfied iff for all prime divisors r of N and all positive integers a we can find $l_p(r, a)$ such that

$$r^{p-1} \equiv N^{(p-1)l_p(r,a)} \mod p^a.$$

□

Now we are ready to formulate the fundamental theorem which allows us to give primality proof of number N.

Theorem 1 Let t be an even integer. Define

$$e(t) = 2 \prod_{q \text{ prime},\ (q-1)|t} q^{v_q(t)+1}.$$

Assume that $(N, te(t)) = 1$ and $e(t) > \sqrt{N}$. For each pair of primes (p, q) such that $(q-1) \mid t$ and $p^k \parallel (q-1)$, let $\chi_{p,q}$ be a character modulo q of order p^k (if g_q is a generator modulo q, then we can take $\chi_{p,q}(g_q) = \zeta_{p^k}$). If the following conditions are satified

1. all $\chi_{p,q}$ satisfy $(\star_\beta)$ for some $\beta_{p,q} \notin \mathfrak{p}$,
2. condition $\mathcal{L}_p$ is true for all primes $p \mid t$,
3. for every $0 \leq i < t$ and $r = N^i \mod e(t)$ if $r \neq 1$, then $r \nmid N$,

then N is prime. ■

This theorem is interpreted as follows. If congruence $(\star_\beta)$ is false for some $\chi_{p,q}$, then we have that N is not prime (just like in Fermat test). But if $(\star_\beta)$ is true for all defined characters then we get some extra information about possible divisors of N. This allows to prove primality of N or gives its nontrivial factor. So the only problem is to verify the $\mathcal{L}_p$ condition. The following proposition gives a practical method for checking it.

Proposition 6 Suppose that χ is a character modulo q of order p^k which satisfies $(\star_\beta)$ for some $\beta \notin \mathfrak{p}$. If one of the following conditions is true, then $\mathcal{L}_p$ is satisfied:

1. $p \geq 3$,
2. $p = 2, k = 1$ and $N \equiv 1 \mod 4$,
3. $p = 2, k \geq 2$ and $q^{\frac{N-1}{2}} \equiv -1 \mod N$.

■

3.2 Jacobi sums

The test based on Gauss sums is asymptotically fast, however it is far from being practical. Main reason for this situation is the computation of $\tau(\chi)^{\beta(N-\sigma_N)}$. One needs to work in $\mathbb{Z}[\zeta_n, \zeta_q]$ and this is very slow in practice.

Example 7 If we want to test number $N < 10^{100}$ then we can take $t = 5040$. In this case $n = p^k$ will be very small, more precisely $p^k \leq 16$. Unfortunately q will be much larger, the largest value being $q = 2521$. This forces us to consider polynomials of degree $> 1,5 \cdot 10^4$ and coefficients reduced modulo N. Multiplying such polynomials takes about $2 \cdot 10^8 \approx 2^{27}$ multiplications modulo N and makes this completely unpractical. □

The above example shows that using Gauss sums is computationally infeasible. One of possible ways to make the test practical, is to replace the $(\star_\beta)$ congruence by some condition depending only on Jacobi sum which lies in a smaller ring $\mathbb{Z}[\zeta_n]$. Fortunately, it is possible and the next three propositions give complete description of this construction.

First we present a very nice result which gives equivalent condition for all practically considered odd primes p.

Proposition 7 Let $3 \leq p < 6 \cdot 10^9$ and $p \neq 1093, 3511$. If we denote by E the set of all integers $1 \leq x < p^k$ coprime to p, then condition $(\star_\beta)$ is equivalent to congruence

$$j(\chi, \chi)^\alpha \equiv \eta(\chi)^{-cN} \mod N,$$

where

$$\alpha = \sum_{x \in E} \left\lfloor \frac{Nx}{p^k} \right\rfloor \sigma_x^{-1}$$

and $c = 2(2^{(p-1)p^{k-1}} - 1)/p^k$. ■

Note that the restriction on p in above proposition is completely irrelevant in practice. Even if we want to test the primality of numbers having 10^9 decimal digits, we would never need primes larger than 1093. This means that the practical problem of testing $(\star_\beta)$ for $p \geq 3$ is solved. The next two propositions decribe the case $p = 2$.

Proposition 8 Let χ be a character modulo q of order 2^k with $k \geq 3$. Denote by E the set of all integers $1 \leq x < 2^k$ that are congruent to 1 or 3 modulo 8. Set $\delta_N = 0$ for N congruent to 1 or 3 modulo 8, $\delta_N = 1$ if N is congruent to 5 or 7 modulo 8. The $(\star_\beta)$ condition can be replaced by

$$\left(j(\chi, \chi) j(\chi, \chi^2)\right)^\alpha j\left(\chi^{2^{k-3}}, \chi^{3 \cdot 2^{k-3}}\right)^{2\delta_N} \equiv$$

$$(-1)^{\delta_N} \eta(\chi)^{-cN} \mod N,$$

where

$$\alpha = \sum_{x \in E} \left\lfloor \frac{Nx}{2^k} \right\rfloor \sigma_x^{-1}$$

and $c = 3(3^{2^{k-2}} - 1)/2^k$. ■

Proposition 9 For $p = 2$, $k = 1$ and $\beta = 1$ condition $(\star_\beta)$ is equivalent to the congruence

$$(-q)^{\frac{N-1}{2}} \equiv \eta(\chi) \mod N.$$

For $p = 2$, $k = 2$ and $\beta = 1$ condition $(\star_\beta)$ is equivalent to the congruence

$$j(\chi, \chi)^{\frac{N-1}{2}} q^{\frac{N-1}{4}} \equiv \eta(\chi)^{-1} \mod N$$

if $N \equiv 1 \mod 4$, and to the congruence

$$j(\chi,\chi)^{\frac{N+1}{2}} q^{\frac{N-3}{4}} \equiv -\eta(\chi) \mod N$$

if $N \equiv 3 \mod 4$. ■

4 IMPLEMENTATION AND RESULTS

4.1 Description of the algorithm

This subsection is based on algorithm given by Henri Cohen in his book [Coh93] and gives pseudocode of Jacobi sums primality test.

Algorithm 1 (Precomputations) Let B be an upper bound on the numbers we want to test. This algorithm makes precomputations of values that don't depend on N.

1. Find such t that $e(t)^2 > B$ (see theorem 1 for definition).

2. For every prime q dividing $e(t)$ with $q \geq 3$ do as follows.

(a) Find a primitive root g_q modulo q, and a table of the function $f(x)$ defined for $1 \leq x \leq q-2$ by $1 - g_q^x = g_q^{f(x)}$ and $1 \leq f(x) \leq q-2$.

(b) For every prime p dividing $q-1$ let k be such number that $p^k \mid q-1$ and $p^{k+1} \nmid q-1$. Let $\chi_{p,q}$ denote the character defined by $\chi_{p,q}(g_q^x) = \zeta_{p^k}^x$.

(c) If $p \geq 3$ or $p = 2$ and $k = 2$, compute

$$J(p,q) = j(\chi_{p,q}, \chi_{p,q}) = \sum_{1 \leq x \leq q-2} \zeta_{p^k}^{x+f(x)}.$$

If $p = 2$ and $k \geq 3$, compute $J(2,q)$ as above and then

$$J_3(q) = j(\chi_{2,q}, \chi_{2,q}) j(\chi_{2,q}, \chi_{2,q}^2) =$$

$$J(2,q) \left(\sum_{1 \leq x \leq q-2} \zeta_{2^k}^{2x+f(x)} \right),$$

and

$$J_2(q) = j\left(\chi_{2,q}^{2^{k-3}}, \chi_{2,q}^{3 \cdot 2^{k-3}}\right)^2 =$$

$$\left(\sum_{1 \leq x \leq q-2} \zeta_8^{3x+f(x)} \right)^2.$$

The above algorithm shows how to compute the set of Jacobi sums for tested numbers that are smaller than some upper bound B. The key step of this part is to compute a very large table $f(x)$ of $q-1$ elements, which allows us to determine Jacobi sums. Of course this part doesn't have to be precomputed as it was suggested before. Experiments show that it takes about $3-5\%$ of total time of the testing procedure, so the described step can be done during every test. The next algorithm combines all previous theoretical results and it proves primality or compositeness of the tested number.

Algorithm 2 (Jacobi sums primality test) Suppose that $N \leq B$ and precomputation step has been done.

1. If $(te(t), N) > 1$, then N is composite.

2. For every prime $p \mid t$ set $l_p \leftarrow 1$ if $p \geq 3$ and $N^{p-1} \not\equiv 1 \mod p^2$, $l_p \leftarrow 0$ otherwise.

3. For each pair (p,q) of primes such that $p^k \parallel (q-1) \mid t$ execute 4a if $p \geq 3$, 4b if $p = 2$ and $k \geq 3$, 4c if $p = 2$ and $k = 2$, 4d if $p = 2$ and $k = 1$. Then go to step 5.

4a. (Based on Proposition 7) Let E be the set of all positive integers smaller than p^k and coprime to p. Set $\Theta \leftarrow \sum_{x \in E} x\sigma_x^{-1}$, $r \leftarrow N \mod p^k$, $\alpha \leftarrow \sum_{x \in E} \left\lfloor \frac{rx}{p^k} \right\rfloor \sigma_x^{-1}$, and compute $s_1 \leftarrow J(p,q)^{\Theta} \mod N$, $s_2 \leftarrow s_1^{\lfloor N/p^k \rfloor} \mod N$, and $S(p,q) \leftarrow s_2 J(p,q)^{\alpha} \mod N$.

If p^k-th root of unity η such that $S(p,q) \equiv \eta \mod N$ doesn't exist, then N is composite. If η exists and is a primitve root, then set $l_p \leftarrow 1$.

4b. (Based on Proposition 8) Let E be the set of all positive integers smaller than 2^k that are congruent to 1 or 3 modulo 8. Set $\Theta \leftarrow \sum_{x \in E} x\sigma_x^{-1}$, $r \leftarrow N \mod 2^k$, $\alpha \leftarrow \sum_{x \in E} \left\lfloor \frac{rx}{2^k} \right\rfloor \sigma_x^{-1}$, and compute $s_1 \leftarrow J_3(q)^{\Theta} \mod N$, $s_2 \leftarrow s_1^{\lfloor N/2^k \rfloor} \mod N$, and $S(2,q) \leftarrow s_2 J_3(q)^{\alpha} J_2(q)^{\delta_N} \mod N$, where $\delta_N = 0$ if $r \in E$, $\delta_N = 0$ otherwise.

If 2^k-th root of unity η such that $S(2,q) \equiv \eta \mod N$ doesn't exist, then N is composite. If η is a primitve root and in addition $q^{(N-1)/2} \equiv -1 \mod N$, then set $l_2 \leftarrow 1$.

4c. (Based on Proposition 9) Compute $s_1 \leftarrow J(2,q)^2 \cdot q \mod N$, $s_2 \leftarrow s_1^{\lfloor N/4 \rfloor} \mod N$, and $S(2,q) \leftarrow s_2$ if $N \equiv 1 \mod 4$, $S_2, q) \leftarrow s_2 J(2,q)^2$ if $N \equiv 3 \mod 4$.

If the fourth root of unity η such that $S(2,q) \equiv \eta \mod N$ doesn't exist, then N is composite. If η is a primitve root and in addition $q^{(N-1)/2} \equiv -1 \mod N$, then set $l_2 \leftarrow 1$.

4d. (Based on Proposition 9) Compute $S(2,q) \leftarrow (-q)^{(N-1)/2} \mod N$.

If $S(2,q) \not\equiv \pm 1 \mod N$ then N is composite. If $S(2,q) \equiv -1 \mod N$, and $N \equiv 1 \mod 4$, then set $l_2 \leftarrow 1$.

5. (Based on Proposition 6) For every $p \mid t$ such that $l_p = 0$ do as follows. Take random number q such that $q \nmid e(t), p \mid (q-1)$ and $(q,N) = 1$. Execute step 4a-4d according to the value of pair (p,q).

If after a reasonable number of tries, some l_p is still equal to 0, then send message saying that the test failed (this is highly improbable).

6. (Based on Theorem 1) For $i = 1, \ldots, t-1$ compute $r_i \leftarrow N^i \mod e(t)$. If for some i, r_i is a nontrivial factor of N then N is composite. Otherwise N is prime.

Presented algorithm works well both in theory and in practice. Pomerance and Odlyzko have shown that the complexity of the Jacobi sums test is

$$O(\ln N^{C \ln\ln\ln N})$$

for some constant C. This is almost polynomial time.

4.2 Choosing good t

We see that in step 6 Algorithm 2 needs to do $O(t)$ divisions. That means that the chosen t shouldn't be too large. On the other hand, if t will be small, then $e(t)^2$ may be smaller than N and this will not allow to use the algorithm. Steps 4a-4d have small complexity only if factors of t are small. All the above considerations tell us that t shouldn't be too small and too large, and it should have small factors.

Unfortunately there is no good description of this problem. So we present values of t that are based on intuition and experiments. Table 1 presents the sample values.

4.3 Running times of the algorithm

We have implemented Algorithm 2 and Rabin-Miller test using the same standard modular arithmetic. Table 2 presents comparison of running time between Jacobi sums test and 320 iterations of Rabin-Miller test. Presented times suggest that the Jacobi sum test can not be used for fast generation of prime numbers. But it can be used for single operations such as generation of

1. cryptosystem parameters,
2. certificate authority key.

The benefit is the certainty that the base of our cryptosystem satisfies theoretical requirements.

$\log_2 N$	t
≤ 101	$180 = 2^2 \cdot 3^2 \cdot 5$
≤ 152	$720 = 2^4 \cdot 3^2 \cdot 5$
≤ 204	$1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$
≤ 268	$2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$
≤ 344	$5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$
≤ 525	$27720 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$
≤ 774	$98280 = 2^3 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13$
≤ 1035	$166320 = 2^4 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11$
≤ 1566	$720720 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$
≤ 2082	$1663200 = 2^5 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11$
≤ 3491	$8648640 = 2^6 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$

Table 1: Sample values of t for testing numbers.

$\log_2 N$	Jacobi sums	Rabin-Miller
64	0.06 s.	0.06 s.
128	0.16 s.	0.15 s.
256	2.09 s.	0.75 s.
512	37.6 s.	5.02 s.
1024	907 s.	37.1 s.

Table 2: Sample runnig times for Jacobi sums test and 320 iterations of Rabin-Miller test on 430 MHz PC.

Comparsion of times from Table 2 is also presented on Figure 1. The logarithmic scale of time was taken to show how close is the runnig time of Jacobi sums test to polynomial time. We can see that the complexity is bounded by $C_1 \ln^3 N$ for Rabin-Miller test and by $C_2 \ln^{4.5} N$ for Jacobi sums primality prooving method. Last remark shows that for practical applications Jacobi sums method is faster than deterministic, polynomial algorithm proposed by Agrawal, Kayal and Saxena [AKS02].

5 CONCLUSIONS

This article presented a primality proving algorithm based on Jacobi sums. Described algorithm is about 2400 times slower than a single iteration of

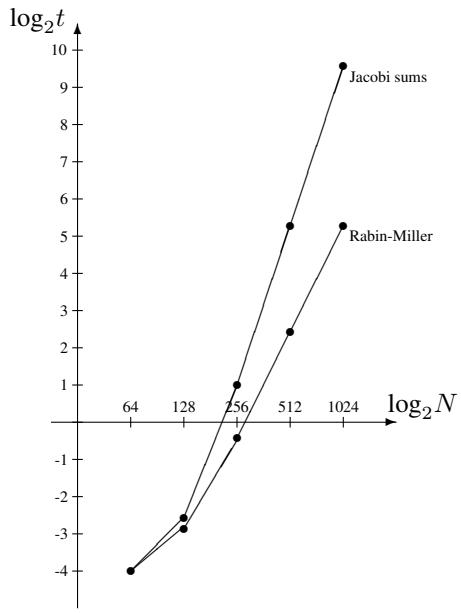

Figure 1: Comparsion of runnig times for Jacobi sums test and 320 iterations of Rabin-Miller test (based on data from Table 2).

Rabin-Miller test for 512-bit numbers. This means that it can't be used in applications where time is one of the most critical resourses and where high speed is necessary. On the other hand there exist situations where security is much more important than speed. Then Jacobi sums test can be successfully used to verify primality of strong pseudoprime numbers.

References

[AKS02] M. Agrawal, N. Kayal, and N. Saxena. Primes is in p. Technical report, Departament of Computer Science and Engineering Indian Institute of Technology Kanpur, 2002.

[AM93] O. Atkin and F. Morain. Elliptic curves and primality proving. *A.M.S.*, 61:29–68, 1993.

[APR83] L. Adleman, C. Pomerance, and R. Rumely. On distinguishing prime numbers from composite numbers. *Ann. of Math*, 117:173–206, 1983.

[BS96] E. Bach and J. Schallit. *Algorithmic number theory*. MIT Press, Cambridge, 1996.

[BvdH90] W. Bosma and M. van der Hulst. *Primality proving with cyclotomy*. PhD thesis, Univ. of Amsterdam, 1990.

[Coh93] H. Cohen. *A course in computational algebraic number theory*. Springer-Verlag, Berlin, 1993.

[CP01] R. Crandall and C. Pomerance. *Prime numbers: a computational perspective*. Springer-Verlag, New York, 2001.

[IR90] K. Ireland and M. Rosen. *A classical introduction to modern number theory*. Springer-Verlag, New York, 1990.

[Rot90] J. Rotman. *Galois theory*. Springer-Verlag, New York, 1990.