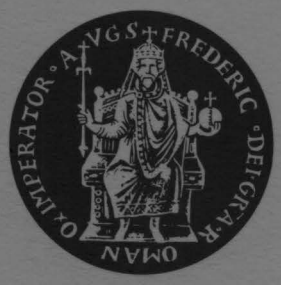
UNIVERSITÄT KAISERSLAUTERN

A GENERALIZATION OF PROTH'S THEOREM

Andreas Guthmann

Preprint Nr. 216



FACHBEREICH MATHEMATIK

A GENERALIZATION OF

PROTH'S THEOREM

Andreas Guthmann

Preprint Nr. 216

UNIVERSITÄT KAISERSLAUTERN
Fachbereich Mathematik
Erwin–Schrödinger–Straße
6750 Kaiserslautern

März 1992

A Generalization of Proth's Theorem

Andreas Guthmann, Fachbereich Mathematik, Universität Kaiserslautern, Pfaffenbergstr. 95, D-6750 Kaiserslautern.

1980 Mathematics Subject Classification (1985 Revision): Primary 11Y11

Abstract: We present a generalization of Proth's theorem for testing certain large integers for primality. The use of Gauß sums leads to a much simpler approach to these primality criteria as compared to the earlier tests. The running time of the algorithms is bounded by a polynomial in the length of the input string. The applicability of our algorithms is linked to certain diophantine approximations of l-adic roots of unity.

§0. Introduction

A fundamental problem in computational number theory is to determine whether a given integer N is prime or composite. In general this can be quite a delicate problem [1, 2, 5], requiring sophisticated tools from algebraic number theory and algebraic geometry. However, if the integer N is of a special form then very rapid tests for primality can be found. For example, by using properties of second order recurring series it is possible to give effective tests, provided $N+1$ is easily factored [3, 12]. In particular, this applies to the Mersenne numbers $N = M_p = 2^p - 1$, where p is any odd prime. The appropriate algorithm is the well known Lucas-Lehmer test [10, 12]. It is effective in the sense that its running time is bounded by a polynomial in the length of the input string, i.e. by a polynomial in $\log N$.

Similarly, the converse of Fermat's theorem provides an effective primality test if $N - 1$ is factored. Here the analogue of the Lucas-Lehmer test is Pepin's theorem [12] which applies to Fermat numbers $F_n = 2^{2^n} + 1$. An extension of this test has been given by Proth [12, 14]: Assume that $N = k \cdot 2^n + 1$, where

$0 < k < 2^n$ and k is odd. The algorithm runs as follows. Let $a \in \mathbf{Z}$ such that $(\frac{a}{N}) = -1$. Then N is prime if, and only if, $a^{(N-1)/2} \equiv -1 \bmod N$. To apply this test, use the law of quadratic reciprocity to find an appropriate a. Then compute $b := a^k \bmod N$ and perform $n-1$ squarings modulo N.

Recently [7] we generalized Proth's theorem to integers of the form $N = k \cdot 3^n + 1$ and $N = k \cdot 2^m 3^n + 1$. Using the law of cubic reciprocity, this leads to tests which are completely analogous to that of Proth.

In the present investigation we consider the general case where l is a prime and $N = k \cdot l^n + 1$. Instead of the higher reciprocity laws we use Gauß sums, which simplifies the analysis considerably. This kind of exponential sums is well known in the theory of cyclotomic fields [9, 15] and was introduced in primality testing by Lenstra and Cohen[4, 5].

Tests for integers of the form $N = k \cdot 3^n + 1$ and $N = k \cdot l^n + 1$ have also been given by Williams and Zarnke([17], without proof) and Williams [16]. Their derivation was based on properties of certain recurring series and works for integers $N = k \cdot l^n - 1$ as well. On the other hand, a generalization of Proth's theorem seems to be a very natural approach here and the Gauß sums provide very simple proofs of our algorithms.

Some basic properties of Gauß sums are reviewed in section 1. The next paragraph contains the general form of Proth's theorem. As it turns out, its application to primality testing is related to Diophantine approximations of certain roots of unity in the ring $\mathbf{Z}_l$ of l-adic integers.

§1. Gauß sums

We here collect some basic properties of Gauß sums, proofs of which can be found, for example, in Lang's book [9].

Let p be a prime number, q a power of p and consider the finite field $GF(q)$ of q elements. If n is a positive integer we denote by $\zeta_n = e^{2\pi i/n}$ a primitive nth root of unity. Furthermore, we let $< \zeta_n >$ denote the group of nth roots of unity.

We consider an additive character λ and a multiplicative character χ of $GF(q)$. If we let $\mathrm{Tr} : GF(q) \to GF(p)$ denote the trace, then $\lambda : GF(q) \to < \zeta_p >$ is given by $\lambda(x) = \zeta_p^{\mathrm{Tr}(x)}$. The multiplicative character $\chi : GF(q)^* \to < \zeta_{q-1} >$ is defined on the nonzero elements of $GF(q)$ and satisfies $\chi(xy) = \chi(x)\chi(y)$.

The *Gauß sum* $\tau(\chi, \lambda)$ is given by

$$\tau(\chi, \lambda) = \sum_{x \in GF(q)^*} \chi(x)\lambda(x). \tag{1}$$

Usually, we write $\tau(\chi)$ instead of $\tau(\chi, \lambda)$ since λ is fixed. From the definition it is immediate that $\tau(\chi)$ is an integer in the cyclotomic field $\mathbf{Q}(\zeta_{q-1}, \zeta_p) = \mathbf{Q}(\zeta_{(q-1)p})$, i.e. $\tau(\chi) \in \mathbf{Z}[\zeta_{(q-1)p}]$. An important special case occurs if $q = p$ is prime. Then

$$\tau(\chi) = \sum_{x=1}^{q-1} \chi(x)\zeta_q^x, \ q \text{ prime.} \tag{2}$$

Now let m be a divisor of $q-1$ and assume that χ is of order m, i.e. $\chi^m = 1$ and m is minimal with respect to this property. Then $\chi(x) \in < \zeta_m >$ and $\tau(\chi) \in \mathbf{Z}[\zeta_{mp}]$.

The cyclotomic field $\mathbf{Q}(\zeta_{mp})$ has the following automorphisms σ_b and ε_c, where b, c are integers:

$$\sigma_b : \zeta_m \to \zeta_m^b, \ \zeta_p \to \zeta_p, \ (b, m) = 1,$$

and

$$\varepsilon_c : \zeta_m \to \zeta_m, \ \zeta_p \to \zeta_p^c, \ (c, p) = 1.$$

The action of these automorphisms induces a natural action of the group ring $\mathbf{Z}[\sigma_b, \varepsilon_c]$ on $\mathbf{Q}(\zeta_{mp})$.

The behaviour of $\tau(\chi)$ under these automorphsims is well known [9]. Clearly,

$$\tau(\chi)^{\sigma_b} = \tau(\chi^b). \tag{3}$$

We also find easily

$$\tau(\chi)^{\varepsilon_c} = \overline{\chi(c)}\tau(\chi), \tag{4}$$

since

$$\begin{aligned} \tau(\chi)^{\varepsilon_c} &= \sum \chi(x)\zeta_p^{c\mathrm{Tr}(x)} = \sum \chi(x)\zeta_p^{\mathrm{Tr}(cx)} \\ &= \chi(c)^{-1} \sum \chi(x)\zeta_p^{\mathrm{Tr}(x)}. \end{aligned}$$

If we let $\alpha = \tau(\chi)^m$ we see that

$$\alpha^{\varepsilon_c} = \tau(\chi)^{m\varepsilon_c} = \left[\overline{\chi(c)}\tau(\chi)\right]^m = \alpha.$$

Thus α is fixed under all automorphisms ε_c, which implies

$$\alpha := \tau(\chi)^m \in \mathbf{Z}[\zeta_m]. \tag{5}$$

Similarly, (4) shows that $\tau(\chi)^{b-\sigma_b}$ is invariant under the action of ε_c, hence

$$\tau(\chi)^{b-\sigma_b} \in \mathbf{Q}(\zeta_m), \ (b, m) = 1. \tag{6}$$

We next consider the Frobenius operation on $\tau(\chi)$. Let K denote the mth cyclotomic field and n be a prime not dividing the discriminant of K, i.e. $(m,n) = 1$. Then n is unramified in K and by definition the Frobenius automorphism $\varphi_n \in \mathrm{Gal}(K/\mathbf{Q})$ corresponding to n is given by $\varphi_n(\gamma) \equiv \gamma^n \bmod n\mathbf{Z}[\zeta_m]$ for each $\gamma \in \mathbf{Z}[\zeta_m]$. From this property it follows easily that φ_n is given explicitly by $\varphi_n(\zeta_m) = \zeta_m^n$.

Lemma 1: *Let q be a power of the odd prime p and χ be a multiplicative character of $GF(q)^*$ of order m. Let n be a prime number such that $(n, 2mp) = 1$. Then*

$$\tau(\chi)^{n-\sigma_n} \equiv \chi(n)^{-n} \bmod n\mathbf{Z}[\zeta_m].$$

Proof: Let $K = \mathbf{Q}(\zeta_{mp})$ and φ_n be the Frobenius automorphism corresponding to n. Then $\varphi_n(\zeta_{mp}) = \zeta_{mp}^n$. Hence $\varphi_n(\zeta_m) = \varphi_n(\zeta_{mp}^p) = \zeta_{mp}^{pn} = \zeta_m^{\sigma_n}$. In the same manner $\varphi_n(\zeta_p) = \zeta_p^{\epsilon_n}$. Thus we obtain by (3) and (4)

$$\begin{aligned}\tau(\chi)^n \equiv \varphi_n(\tau(\chi)) = \tau(\chi)^{\sigma_n \epsilon_n} &= \left[\overline{\chi(n)}\tau(\chi)\right]^{\sigma_n} \\ &\equiv \chi(n)^{-n}\tau(\chi)^{\sigma_n} \bmod n\mathbf{Z}[\zeta_{mp}].\end{aligned}$$

Now observe that the ideal $(\tau(\chi)) = \tau(\chi)\mathbf{Z}[\zeta_{mp}]$ is prime to (n) since the only prime ideals dividing $(\tau(\chi))$ are those lying over (p). Thus, $\tau(\chi)$ is invertible modulo (n) and we get

$$\tau(\chi)^{n-\sigma_n} \equiv \chi(n)^{-n} \bmod n\mathbf{Z}[\zeta_{mp}].$$

The conclusion follows from property (6).

In the next section we need the following special case of lemma 1.

Lemma 2: *Same assumptions as in the previous lemma. Moreover, assume $n \equiv 1 \bmod m$ and define α by $\alpha = \tau(\chi)^m$. Then $\alpha \in \mathbf{Z}[\zeta_m]$ and*

$$\alpha^{\frac{n-1}{m}} \equiv \overline{\chi(n)} \bmod n\mathbf{Z}[\zeta_m].$$

Proof: We have $\sigma_n = 1$ since $n \equiv 1(m)$. Consequently, by lemma 1

$$\alpha^{\frac{n-1}{m}} = \tau(\chi)^{n-1} = \tau(\chi)^{n-\sigma_n} \equiv \chi(n)^{-n} \equiv \overline{\chi(n)} \bmod n.$$

We now specialize the previous discussuion to the case where $q = p$ is prime and also $m = l$ is prime. Then χ is a character of order l on $(\mathbf{Z}/q\mathbf{Z})^*$ and $\tau(\chi)$ is given by (2). Let $\alpha = \tau(\chi)^l$. If n is a prime number satisfying $(n, 2pq) = 1$ and $n \equiv 1(l)$ then

$$\alpha^{\frac{n-1}{l}} \equiv \zeta_l^a \bmod n\mathbf{Z}[\zeta_l], \tag{7}$$

for some integer a. We have, of course, $\zeta_l^a = \chi(n)^{-1}$ and we may assume $0 \leq a \leq l-1$. The next result shows what, conversely, can be said if this congruence holds for n.

Theorem 1: *Let q, l be primes and $l|q-1$. Define $\tau(\chi)$ by (2) where χ is of order l and let $\alpha = \tau(\chi)^l \in \mathbf{Z}[\zeta_m]$.*

Assume that n is a positive integer such that $(n, 2pq) = 1$ and that (7) holds for some $a \not\equiv 0(l)$. Finally, let $l^e \| n-1$. Then

$$r^{\mathrm{ord}_l(r)} \equiv 1 \bmod l^e$$

for each divisor r of n.

Proof: We may assume that r is prime. If $f = \mathrm{ord}_l(r)$ then $f|l-1$ and

$$(r) = r\mathbf{Z}[\zeta_l] = P_1 \cdots P_t, \; t = \tfrac{l-1}{f}.$$

The P_i are prime ideals in $\mathbf{Z}[\zeta_l]$ which are pairwise distinct and have residue class degree f. This means that $\mathbf{Z}[\zeta_l]/P_i \simeq GF(r^f)$ and $\mathcal{N}(P_i) = r^f$ (here $\mathcal{N}$ denotes the norm).

Let $\mathrm{ord}_P(\alpha)$ denote the order of α in $\mathbf{Z}[\zeta_l]/P$, where P is one of the P_i. From (7) we get $\alpha^{n-1} \equiv 1 \bmod P$. Hence $\mathrm{ord}_P(\alpha)|n-1$. On the other hand, $\mathrm{ord}_P(\alpha)$ is not a divisor of $\frac{n-1}{l}$, since in this case $\zeta_l^p \equiv \alpha^{(n-1)/l} \equiv 1 \bmod P$. Since $a \not\equiv 0(l)$ this would imply that $l = \mathcal{N}(\zeta_l - 1) \in P$. Thus we obtain a contradiction to the fact that $(l, r) = 1$.

We therefore conclude that $l^e | \mathrm{ord}_P(\alpha)$ and the theorem follows from $\mathrm{ord}_P(\alpha) | \mathcal{N}(P_i) - 1$.

If $l = 2$ then Theorem 1 implies $r \equiv 1 \bmod 2^e$ if $2^e \| n-1$ and $r|n$. In this case we immediately get Proth's theorem.

Concerning $l = 3$, we find $r^2 \equiv 1 \bmod 3^e$, hence $r \equiv \pm 1 \bmod 3^e$. This leads to the primality tests of our earlier paper [7]. However, the present derivation is

much simplified by the consequent use of the Gauß sums, thereby avoiding the law of cubic reciprocity. For some explicit examples we refer to the last section.

Since $l = 2$ leads to Proth's theorem we may henceforth assume that $l > 2$. The next theorem links the efficiency the tests for primality to certain l-adic approximations of roots of unity in $\mathbf{Z}_l$.

Here we denote by $\mathbf{Z}_l$ the l-adic integers. We further let U denote the group of $(l-1)$st roots of unity in $\mathbf{Z}_l$, provided $l > 2$. Then $U =< \zeta >$ is generated by a primitive $(l-1)$st root ζ.

Theorem 2: *Let $l > 2$ be a prime. Under the assumptions of Theorem 1 there exists $\eta = \eta(r) \in U$ for each prime r dividing n such that*

$$r \equiv \eta \bmod l^e.$$

Proof: Since l is odd, the congruence $x^{l-1} \equiv 1 \bmod l^e$ has exactly $l-1$ solutions. Each solution is congruent to an element of U modulo l^e. Since r solves the congruence by Theorem 1, the conclusion follows.

§2. Tests for primality.

We are now going to apply the results of §1 to test integers $N = k \cdot l^n + 1$ for primality. Let l be an odd prime and let U as before be the group of $(l-1)$st roots of unity in $\mathbf{Z}_l$. The l-adic absolute value is denoted by $|x|_l$ for $x \in \mathbf{Z}_l$.

We set

$$U = \{\eta_1, \ldots, \eta_{l-1}\},\ \eta_i \equiv i \bmod l,\ \eta_i = \sum_{j=0}^{\infty} a_{ij} l^j,\ 0 \le a_{ij} < l.$$

Clearly, $\eta_1 = 1$ and $\eta_{l-1} = -1 = \sum_{j=0}^{\infty}(l-1)l^j$. We also define

$$\eta_i^{(n)} = \sum_{j=0}^{n-1} a_{ij} l^j,\ n \ge 1.$$

Then $\eta_i^{(n)}$ is a positive integer. Moreover, $0 < \eta_i^{(n)} < l^n$ and $|\eta_i^{(n)} - \eta_i|_l \le l^{-n}$. Finally, we let for $n \ge 1$

$$H_n = \min\{\eta_i^{(n)} | 2 \le i \le l-2\}. \tag{8}$$

Theorem 3: *Let l, p be primes, where l is odd and $l|p-1$. Define $\tau(\chi)$ and α as in Theorem 1. Let $N = k \cdot l^n + 1$ be such that $(N, 2lp) = 1$ and l does not divide k. Moreover, let $0 < k < H_n^2 l^{-n}$.*

Then N is prime if, and only if,

$$\alpha^{\frac{N-1}{l}} \equiv \zeta_l^a \bmod N, \ a \not\equiv 0(l).$$

Proof: If N is prime the congruence holds with $\zeta_l^a = \chi(N)^{-1}$ by (7).

Conversely, assume $\alpha^{(N-1)/l} \equiv \zeta_l^a \bmod N$. Let r be any prime dividing N. By Theorem 2, there exists $\eta_i \in U$ such that $|r - \eta_i|_l \leq l^{-n}$. If $i = 1$, then $r \equiv 1(l^n)$, i.e. $r > l^n > H_n$. Otherwise $|r - \eta_i^{(n)}|_l \leq l^{-n}$ and $r \geq \eta_i^{(n)}$ since $0 < \eta_i^{(n)} < l^n$. Consequently, $r \geq H_n$ and since

$$r^2 \geq H_n^2 \geq l^n(k+1) > N,$$

we conclude that $r = N$, q.e.d.

To apply this result we need the constants H_n as defined by (8). In the simplest case $l = 3$ we have $U = \{1, -1\}$ and $H_n = \eta_2^{(n)} = 3^n - 1$. Hence, in Theorem 3 we may allow k to be as large as $(3^n - 1)^2 3^{-n} > 3^n - 2$.

If $l > 3$ however, there is no simple argument leading to a lower bound for H_n. In practice, on the other hand, there are no difficulties to compute H_n. This can be accomplished as follows.

We start with $\eta_i^{(1)} = i$ for $2 \leq i \leq l-2$. Given $\eta_i^{(n)}$ we have $\eta_i^{(n)} \equiv \eta_i \bmod l^n$. Thus $(\eta_i^{(n)})^l \equiv \eta_i^l \equiv \eta_i \bmod l^{n+1}$. Consequently,

$$\eta_i^{(n+1)} \equiv (\eta_i^{(n)})^l \bmod l^{n+1}.$$

For practical purposes it is useful to consider the normalized constants

$$\delta_j = H_j l^{-j}, \ j \geq 1,$$

as well as

$$\Delta_n = \min\{\delta_j | 1 \leq j \leq n\}.$$

Clearly, $0 < \Delta_n < 1$. Having computed Δ_n, the condition on k in Theorem 3 can be replaced by

$$0 < k < \Delta_n^2 l^n. \tag{9}$$

Hence, the larger Δ_n the larger is the admissible range for k in Theorem 3. As remarked, it is easy to compute H_n and Δ_n but is definitely not easy to prove good lower bounds for Δ_n.

Of course, we expect $\Delta_n \to 0$, but it is not easy to find the exact rate of decrase. If the "digits" a_{ij} in the l-adic expansion of η_i were random numbers, we could view them as representing an infinite sequence of Bernoulli trials, where success ($a_{ij} = 0$) occurs with probability l^{-1}. The law of the iterated logarithm [6] suggests $\Delta_n \to 0$, but not faster than $c_1 n^{-1}$ for some positive constant c_1. The data from the table in §3 fit well with this heuristic argument.

On the other hand, lower bounds for Δ_n can be deduced from the theory of diophantine approximations to l-adic numbers. For example, Ridout's l-adic version [13] of the Thue-Siegel-Roth theorem immediately gives

$$\Delta_n \geq c_2 l^{-(\frac{1}{2}+\epsilon)n}, \ c_2 > 0,$$

for each $\epsilon > 0$. For our purposes, however, this bound is too weak.

§3. Running time

In order to apply the tests of §2 the prime l is considered to be fixed. We thus are looking for primes N of the form

$$N = k \cdot l^n + 1, \ k \not\equiv 0 \bmod l.$$

Before searching for primes it is advisable to compute some constants in advance. First, we need the Δ_n as defined in the previous section. This problem reduces to the computation of the $(l-1)$st roots of unity in $\mathbf{Z}_l$. A short tables for the primes l below 20 and some small values of n is given at the end of this paragraph.

Next, consider the Gauß sums $\tau(\chi)$, where χ is a character modulo p. In our case p is prime such that $l|p-1$. Let g be any primitive root modulo p and let $\chi(x) = \zeta_l^{\mathrm{ind}(x)}$, where $\mathrm{ind}(x)$ denotes the index of $x \bmod p$ with respect to g. In particular, we have $\chi(g) = \zeta_l \neq 1$. Then

$$\tau(\chi) = \tau(p,g,l) = \sum_{x=1}^{p-1} \zeta_l^{\mathrm{ind}(x)} \zeta_p^x.$$

Finally,

$$\alpha = \alpha(p,g,l) = \tau(p,g,l)^l \in \mathbf{Z}[\zeta_l]. \tag{10}$$

We may therefore write

$$\alpha = \sum_{j=0}^{l-2} \alpha_j \zeta_l^j, \ \alpha_j \in \mathbf{Z}.$$

Since $\alpha^{(N-1)/l} = \alpha^{kl^{n-1}}$ we also compute in advance $\beta_0 := \alpha^k$, provided k is fixed. To test N for primality, raise β_0 to the l^{n-1}th power in $\mathbf{Z}[\zeta_l]/N\mathbf{Z}[\zeta_l] \simeq (\mathbf{Z}/N\mathbf{Z})[\zeta_l]$. Denote this ring by R_N. Then the computation of $\beta_0^{l^{n-1}}$ involves $O(\log l^{n-1}) = O(n \log l)$ multiplications in R_N. Each of these needs at most $(l-1)^2$ multiplications in $\mathbf{Z}/N\mathbf{Z}$ together with some additions. Hence we have

Theorem 4: *Given $N = k \cdot l^n + 1$ and $\beta_0 = \alpha^k$, the primality of N can be decided with at most $O(n(\log N)^2 l^2 \log l)$ bit operations. The implied constant does not depend on n, N and l.*

By using fast algorithms for integer and matrix multiplication [8] we can even achieve a running time of $O(n(\log N)^{1+\varepsilon} l^{1+\varepsilon})$ for every $\varepsilon > 0$.

For small primes l however, there are other ways to reduce the number of multiplications in $\mathbf{Z}/N\mathbf{Z}[\zeta_l]$. Formulas of this kind are often special cases of certain convolution algorithms and are widely used in practice [5, 11]. See the remarks in the final section.

Finally, we note that is it also necessary to find suitable primes p and characters χ to satisfy the condition $\chi(N) \neq 1$ if N is prime. In the case of Proth's theorem ($l = 2$) this is accomplished by using the law of quadratic reciprocity. If k is fixed appropriate values for p and χ are easily found in practice. Again we refer to the next section for some examples.

l	n=50	n=100	n=300
5	4.6549E-2	5.0327E-3	4.5042E-3
7	4.3159E-3	4.3159E-3	6.0847E-4
11	1.7181E-3	1.2334E-3	9.5421E-4
13	2.3642E-3	1.8515E-3	3.6136E-4
17	3.1664E-3	1.8648E-3	1.1647E-3
19	3.5415E-3	3.0809E-4	1.5404E-4

Table of Δ_n for primes $l < 20$.

§4. Some examples

In this final section we consider some explicit examples. First, let $l = 3$. Tests for integers of the form $N = k \cdot 3^n + 1$ have been given by Williams and Zarnke[17] and Guthmann[7]. The justification of the latter algorithms depends on the use of the law of cubic reciprocity, while that of the former depends on the properties of recurring series.

Given k even, we would like to test $N = k \cdot 3^n + 1$ for primality. Since $\Delta_n = 3^n - 1$ in this case Theorem 3 immediately leads to

Theorem 5: *Let $N = k \cdot 3^n + 1$, where k is even, $k \not\equiv 0(3)$ and $0 < k < 3^n - 1$. Let p be a prime such that $p \equiv 1(3)$ and p does not divide N. Let χ be a character modulo p of order 3 such that $\chi(N) \neq 1$.*

Then N is prime if, and only if,

$$\alpha^{\frac{N-1}{3}} \equiv \zeta_3^a \bmod N, \ a \in \{1, 2\},$$

where α is defined by (9).

Computations in $\mathbf{Z}[\zeta_3]$ can be performed as usual. If $a = a_0 + a_1\zeta_3$ and $b = b_0 + b_1\zeta_3$ are elements of $\mathbf{Z}[\zeta_3]$ then

$$ab = a_0b_0 - a_1b_1 + (a_0b_1 + a_1b_0 - a_1b_1)\zeta_3.$$

This formula needs four multiplications. Using instead the identity

$$ab = a_0b_0 - a_1b_1 + [(a_0 + a_1)(b_0 + b_1) - 2a_1b_1 - a_0b_0]\,\zeta_3,$$

three multiplications are sufficient (where the computation of $2a_1b_1$ is counted as one addition). The computation of the Gauß sum $\tau(p, g, 3)$ is straightforward, as well as the evaluation of $\alpha(p, g, 3) = \tau(p, g, 3)^3$.

The condition $\chi(N) \neq 1$ is equivalent to $\mathrm{ind}(N) \not\equiv 0 \bmod 3$, if the character χ corresponds to a primitive root modulo p. Generally, this condition is easily met. As an example, we consider the case $k = 2$. We are looking for primes $N = 2 \cdot 3^n + 1$. Choosing $p = 7$, we have $\chi(N) = 1$ if, and only if, $N \equiv \pm 1(7)$. Now $N \not\equiv 1(7)$ and $N \equiv -1(7)$ is equivalent to $3|n$. Thus, we can use $p = 7$ if n is not divisible by 3. If it is, say $N = 2 \cdot 3^{3n} + 1$, then take $p = 13, g = 2$, since in this case $\chi(N) = \chi(3) = \chi(g)^4 = \zeta_3$.

To summarize, take $p = 7$ if $N = 2 \cdot 3^n + 1$ and $n \not\equiv 0(3)$ and take $p = 13$ if $N = 2 \cdot 3^{3n} + 1$. The corresponding values of α are

$$\alpha(7,3,3) = -7(1+\zeta_3),\ \alpha(13,2,3) = -13(4+3\zeta_3).$$

Finally, we treat the case $l = 5$. If we represent elements of $\mathbf{Z}[\zeta_5]$ by $a_0 + a_1\zeta_5 + a_2\zeta_5^2 + a_3\zeta_5^3, a_i \in \mathbf{Z}$, then ordinary multiplication in $\mathbf{Z}[\zeta_5]$ needs 16 integer multiplications and 15 additions. Using the formulas given by Nussbaumer [11, App. B2] this can also be achieved with 7 integer multplications and 46 additions which is much better for large N.

Let $N = 2 \cdot 5^{105} + 1$. We want to show that N is prime. For the prime $p = 11$ we take the primitive root $g = 2$ and $\chi(g) = \zeta_5$. Since $N \equiv 3(11)$, we have $\chi(N) = \zeta_5^3$. Then

$$\alpha(11,2,5) = 11 \cdot (-26 - 20\zeta_5 + 15\zeta_5^2 - 10\zeta_5^3).$$

We compute

$$\alpha^{(N-1)/5} \equiv c \cdot \zeta_5^3 \bmod N,$$

where c is a certain integer. Hence by Theorem 3 and the table given above, N is a prime number.

Bibliography

[1] Adleman, L.M., Pomerance, C., Rumely, R.S., On Distinguishing Prime Numbers from Composite Numbers, Ann. of Math. **117**, 173-206(1983).

[2] Atkin, A.O.L., Morain, F., Elliptic Curves and Primality Proving, to appear.

[3] Brillhart, J., Lehmer, D.H., Selfridge, J.L., New Primality Criteria and Factorizations of $2^m \pm 1$, Math. Comp. **29**, 620-647(1975).

[4] Cohen, H., Lenstra, A.K., Implementation of a New Primality Test, Math. Comp. **48**, 103-121(1987).

[5] Cohen, H., Lenstra, H.W., jr., Primality Testing and Jacobi Sums, Math. Comp. **42**, 297-330(1984).

[6] Feller, W., An Introduction to Probability Theory and its Applications, Vol. I, Third Ed., Wiley 1968.

[7] Guthmann, A., Effective Primality Tests for Integers of the Form $k3^n + 1$ and $k2^m3^n + 1$, BIT, to appear.

[8] Knuth, D.E., The Art of Computer Programming, Vol. II, Second Ed., Addison Wesley 1981.

[9] Lang, S., Cyclotomic Fields, Springer 1978.

[10] Lehmer, D.H., An Extended Theory of Lucas' Functions, Ann. of Math. **31**, 419-448(1930).

[11] Nussbaumer, H., Fast Fourier Transform and Convolution Algorithms, Second Ed., Springer 1982.

[12] Riesel, H., Prime Numbers and Computer Methods for Factorization, Birkhäuser 1985.

[13] Ridout, D., Rational Approximations to Algebraic Numbers, Mathematika **4**, 125-131(1957).

[14] Robinson, R.M., The Converse of Fermat's Theorem, Am. Math. Monthly **64**, 703-710(1957).

[15] Washington, L.C., Introduction to Cyclotomic Fields, Springer 1982.

[16] Williams, H.C., An Algorithm for Determining Certain Large Primes, Congressus Numerantium III, Baton Rouge 1971.

[17] Williams, H.C., Zarnke, C.R., Some Prime Numbers of the Forms $2A3^n + 1$ and $2A3^n - 1$, Math. Comp. **26**, 995-998(1972).