EFFECTIVE PRIMALITY TESTS FOR INTEGERS OF THE FORMS $N = k3^n+1$ AND $N = k2^m3^n+1$

Andreas Guthmann

Preprint No 199

UNIVERSITÄT KAISERSLAUTERN
Fachbereich Mathematik
Erwin–Schrödinger–Straße
D–6750 Kaiserslautern

Juni 1991

Effective Primality Tests for Integers of the Forms $N = k3^n + 1$ and $N = k2^m3^n + 1$

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

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

1. INTRODUCTION. A well known theorem of Proth's [2, 3] states that if N is an integer of the form $N = k \cdot 2^n + 1$, where k is odd and $0 < k < 2^n$, and if a is an integer such that $(\frac{a}{N}) = -1$, then N is prime if, and only if

$$a^{\frac{N-1}{2}} \equiv -1 \bmod N.$$

This test is very effective. Indeed, having found the appropriate a, compute $b := a^k \bmod N$ and then perform $n-1$ squarings mod N. The integer a may be found by quadratic reciprocity. Hence this is an example of a polynomial test, which means that its running time is bounded by a polynomial in $\log N$.

What we shall do here is to generalize this test to integers of the form $N = k \cdot 3^n + 1$. An effective algorithm for these integers has already been given by Williams [4 , without proof], by using properties of certain Lucas sequences. While these methods seem to be somewhat *ad hoc* our proof consists of a direct generalization of Proth's theorem. This is accomplished by using elementary facts about the arithmetic in $\mathbf{Z}[\varpi]$, where ϖ is a primitive third root of unity. The advantage of our method is also shown by the fact that our test combines well with Proth's test to give an algorithm for integers of the form $N = k \cdot 2^m 3^n + 1$. This case has not been considered earlier in the literature (but see Williams' test [5]).

2. ARITHMETIC IN $\mathbf{Z}[\varpi]$. Set $\varpi = \frac{1}{2}(-1 + \sqrt{-3})$. Then ϖ is a primitive third root of unity and $\varpi^2 = -\varpi - 1$. The following facts concerning the arithmetic

of $\mathbf{Q}[\varpi] = \mathbf{Q}[\sqrt{-3}]$ can be found, for example, in the book by Ireland and Rosen [1]. Let R be the ring of integers of $\mathbf{Q}[\sqrt{-3}]$. Then $R = \{a + b\varpi | a, b \in \mathbf{Z}\}$. The group of units $G(R)$ of R consists of the six elements $G(R) = \{1, -1, \varpi, -\varpi, \varpi^2, -\varpi^2\}$. The field $\mathbf{Q}[\varpi]$ has an automorphism $\overline{}$ of order two, sending ϖ to $\overline{\varpi} = \varpi^{-1}$. This gives $\overline{a + b\varpi} = a - b - b\varpi$. The norm $\mathcal{N}$ of an element $\alpha = a + b\varpi$ (with $a, b \in \mathbf{Q}$) is defined by $\mathcal{N}(\alpha) = \alpha\overline{\alpha} = a^2 - ab + b^2$. The group of units $G(R)$ consists exactly of the elements of norm 1.

Now assume that $\pi \in R$ is a prime element, i.e. if $\pi \notin G(R)$ and $\pi | \alpha\beta$ (where $\alpha, \beta \in R$) then $\pi | \alpha$ or $\pi | \beta$. Moreover $\mathcal{N}(\pi) = p$ or p^2 where p is a rational prime number. Conversely, assume that p is a prime number and $p \equiv 2 \bmod 3$. Then p is also prime in R and $\mathcal{N}(p) = p^2$. If $p \equiv 1 \bmod 3$ then p splits as $p = \pi\overline{\pi}$ and $\mathcal{N}(\pi) = p$. Finally, for $p = 3$ we have $3 = -\varpi^2(1 - \varpi)^2$ and $1 - \varpi$ is prime in R.

3. PRIMALITY TESTS FOR INTEGERS OF THE FORM $N = k3^n + 1$.

Now let π be a prime element of R such that $\mathcal{N}(\pi) = \pi\overline{\pi} = N \equiv 1(3)$ is a rational prime. If $\alpha \in R$, then there exists a unique integer j with the property

$$\alpha^{\frac{N-1}{3}} \equiv \varpi^j \bmod \pi, \ j \in \{0, 1, 2\},$$

provided π does not divide α. Assume that $\overline{\alpha}^{(N-1)/3} \equiv \varpi^k(\pi)$. Define $\beta \in R$ by $\beta \equiv \alpha\overline{\alpha}^{-1} \bmod N$. Since R is euclidean this can be computed by the generalized euclidean algorithm. We then have

$$\beta^{\frac{N-1}{3}} \equiv \varpi^{j-k} \bmod \pi.$$

Applying the automorphism $\overline{}$ and noting that $\overline{\beta} \equiv \beta^{-1} \bmod N$ we obtain

$$\beta^{-\frac{N-1}{3}} \equiv \overline{\varpi}^{k-j} \bmod \overline{\pi},$$

or, equivalently,

$$\beta^{\frac{N-1}{3}} \equiv \varpi^{j-k} \bmod \overline{\pi}.$$

Since this congruence holds mod π and mod $\overline{\pi}$, it holds mod their product N by the Chinese remainder theorem. We summarize these facts as follows:

Theorem 1: Let $N \equiv 1(3)$ be a prime number and let $\alpha \in R$ be such that α is prime to N. Define $\beta \in R$ by $\beta \equiv \alpha\overline{\alpha}^{-1} \bmod N$. Then there exists an integer j such that

$$\beta^{\frac{N-1}{3}} \equiv \varpi^j \bmod N, \ j \in \{0, 1, 2\}.$$

We would like to have $j \neq 0$ in Theorem 1. To investigate this problem further, we need some properties of the cubic residue symbol, which is defined as follows [1]. If $\pi \in R$ is a prime with $\mathcal{N}(\pi) \neq 3$, and $\alpha \in R$ is prime to π then we define $\left(\frac{\alpha}{\pi}\right)_3$ by

$$\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{\frac{\mathcal{N}(\pi)-1}{3}} \equiv \varpi^j \bmod \pi, \ j \in \{0,1,2\}.$$

Then, clearly $\left(\frac{\alpha_1\alpha_2}{\pi}\right)_3 = \left(\frac{\alpha_1}{\pi}\right)_3 \left(\frac{\alpha_2}{\pi}\right)_3$. This symbol also satisfies a reciprocity law. To state it we need a further concept. If $\alpha \in R$ and $\alpha = a + b\varpi$ with integers a and b, then α is called primary if, and only if, $\alpha \equiv 2(3)$, i.e. $a \equiv 2(3)$, $b \equiv 0(3)$. Assume that $q \equiv 1(3)$ is a prime number and $q = \alpha\overline{\alpha}$. It is an easy exercise to show that among the associates of α there is exactly one that is primary. Moreover, if α is primary so is $\overline{\alpha}$. We now can state the cubic law of reciprocity: if $\alpha, \pi \in R$ are prime and primary, and $\mathcal{N}(\alpha) \neq 3 \neq \mathcal{N}(\pi)$, and if π does not divide α then

$$\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\pi}{\alpha}\right)_3.$$

Theorem 2: Same assumptions as in Theorem 1. Moreover, assume that α is a primary prime with $q = \alpha\overline{\alpha} \equiv 1(3)$ and that $N^{(q-1)/3} \not\equiv 1 \bmod \alpha$. Then

$$\beta^{\frac{N-1}{3}} \equiv \varpi^j \bmod N, \ j \in \{1,2\}.$$

Proof: Let $N = \pi\overline{\pi}$, where π is a prime of R. We may assume that π is primary. Now

$$N^{\frac{q-1}{3}} = N^{\frac{\mathcal{N}(\alpha)-1}{3}} = (\pi\overline{\pi})^{\frac{\mathcal{N}(\alpha)-1}{3}} \equiv \left(\frac{\pi}{\alpha}\right)_3 \left(\frac{\overline{\pi}}{\alpha}\right)_3 \bmod \alpha.$$

By cubic reciprocity $1 \neq \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\alpha}{\overline{\pi}}\right)_3$. This implies in particular $\alpha^{(N-1)/3} \not\equiv 1 \bmod N$. For, otherwise $\alpha^{(N-1)/3} \equiv 1 \bmod \pi$ and $\alpha^{(N-1)/3} \equiv 1 \bmod \overline{\pi}$, which means

$$\left(\frac{\alpha}{\pi}\right)_3 = 1 = \left(\frac{\alpha}{\overline{\pi}}\right)_3.$$

Therefore $\alpha^{(N-1)/3} \equiv \varpi^j \bmod N$, $j \in \{1,2\}$. But then $\overline{\alpha}^{(N-1)/3} \equiv \varpi^{-j} \not\equiv \varpi^j \bmod N$, and we are done.

We are prepared to give the analogue of Proth's theorem:

Theorem 3: Let $N = k \cdot 3^n + 1$, where $0 < k < 3^n - 2$ and k is even and not divisible by 3. Let q be a prime number with $q \equiv 1(3)$ and $(q, N) = 1$. Let $\alpha \in R$

be a primary prime element such that $q = \mathcal{N}(\alpha)$ and $N^{(q-1)/3} \not\equiv 1 \bmod \alpha$. Finally define $\beta \in R$ by $\beta \equiv \alpha\overline{\alpha}^{-1} \bmod N$.

Then N is prime if, and only if,

$$\beta^{\frac{N-1}{3}} \equiv \varpi^j \bmod N,\ j \in \{1,2\}.$$

Proof: If N is prime the statement follows from Theorem 2. Conversely, assume that the last congruence holds. Let $\pi \in R$ be any prime dividing N and set $p = \mathcal{N}(\pi)$. Since $\overline{\alpha}$ is prime to N, we may define $\beta_0 \equiv \alpha\overline{\alpha}^{-1}(\pi)$. Then $\beta_0^{N-1} \equiv 1(\pi)$ because $\beta^{N-1} \equiv 1(N)$. Hence, if r denotes the order of $\beta_0 \bmod \pi$, we have $r|N-1 = k3^n$. But $\beta_0^{(N-1)/3} \equiv \beta^{(N-1)/3} \equiv \varpi^j \not\equiv 1(\pi)$ (otherwise π would divide $\varpi^j - 1$). So r does not divide $\frac{N-1}{3} = k3^{n-1}$. This implies $3^n|p-1$. Now we have to distinguish two cases. If $\pi \in \mathbf{Z}$ then $\pi \equiv 2(3)$ and $\mathcal{N}(\pi) = p = \pi^2$. Since $3^n|p-1$ we get $3^n|\pi+1$ and in particular $\pi \geq 3^n - 1$. On the other hand, if $\pi \notin \mathbf{Z}$ then $\mathcal{N}(\pi) = \pi\overline{\pi} = p$ and we see that $3^n|p-1$. Thus in any case $s \geq 3^n - 1$ for each rational prime s dividing N. So, if N were composite $N \geq (3^n-1)^2 = (3^n-2)3^n + 1 > N$, a contradiction. Hence N is prime.

4. PRIMALITY TESTS FOR INTEGERS OF THE FORM $N = k2^m3^n + 1$.

Now we want to combine our test (Theorem 3) with Proth's. The theorems in this section are exactly parallel to those of section 2.

Theorem 4: Let N be a prime number with $N \equiv 1(6)$. Let $\alpha \in R$, $q = \mathcal{N}(\alpha) = \alpha\overline{\alpha}$ prime such that $(q, N) = 1$, $\beta \in R$ where $\beta \equiv \alpha\overline{\alpha}^{-1}(N)$. Then

$$\beta^{\frac{N-1}{6}} \equiv (-1)^l\varpi^j,\ l \in \{0,1\},\ j \in \{0,1,2\}.$$

Proof: We have $N = \pi\overline{\pi}$, where π is a prime element of R. Since $R/\pi R \simeq GF(N)$, the equation $x^6 \equiv 1(\pi)$ has exactly six solutions, namely $x \equiv (-1)^l\varpi^j$, $l \in \{0,1\}$, $j \in \{0,1,2\}$. Since $\beta^{(N-1)/6}$ is a solution, $\beta^{(N-1)/6} \equiv (-1)^l\varpi^j$ for some l and j. Conjugation gives $(-1)^l\varpi^{-j} \equiv \overline{\beta}^{(N-1)/6} \equiv (\beta^{-1})^{(N-1)/6} \bmod \overline{\pi}$. Thus $\beta^{(N-1)/6} \equiv (-1)^l\varpi^j \bmod \overline{\pi}$ too, and the conclusion follows.

Of course, we again want to have $l \neq 0$ and $j \neq 0$. This is furnished by

Theorem 5: Let $N \equiv 1(6)$ be prime, $\alpha \in R$ be a primary prime with $q = \mathcal{N}(\alpha)$ prime, $(q, N) = 1$ and $\beta \in R$ with $\beta \equiv \alpha\overline{\alpha}^{-1}(N)$. Assume further that

$$N^{\frac{q-1}{3}} \not\equiv 1 \bmod \alpha \text{ and } \left(\frac{q}{N}\right) = -1.$$

Then

$$\beta^{\frac{N-1}{6}} \equiv -\varpi^j, \; j \in \{1,2\}.$$

Proof: From Theorem 4 we get

$$\beta^{\frac{N-1}{6}} \equiv (-1)^l \varpi^j, \; l \in \{0,1\}, \; j \in \{0,1,2\}.$$

If $j = 0$, then $\beta^{(N-1)/3} \equiv 1(N)$, contradicting Theorem 2. Hence $j \neq 0$. If $l = 0$, then $\beta^{(N-1)/2} \equiv 1(N)$. Since $\beta \equiv \alpha\overline{\alpha}^{-1} \equiv \alpha^2 q^{-1}(N)$, this would give

$$1 \equiv (\alpha^2 q^{-1})^{\frac{N-1}{2}} = \alpha^{N-1}\left(q^{\frac{N-1}{2}}\right)^{-1} \equiv \left(\frac{q}{N}\right)^{-1} \equiv \left(\frac{q}{N}\right) \bmod N,$$

contrary to our hypothesis, q.e.d.

Finally, we have the following test for primality.

Theorem 6: Let $N = k\cdot 2^m 3^n + 1$, where $mn \geq 1$, $(k,6) = 1$, and $0 < k < 2^m 3^n - 2$. Let $\alpha \in R$ with $q = \alpha\overline{\alpha}$ a prime and

$$N^{\frac{q-1}{3}} \not\equiv 1 \bmod \alpha, \quad \left(\frac{q}{N}\right) = -1.$$

Define $\beta \in R$ by $\beta \equiv \alpha\overline{\alpha}^{-1} \bmod N$. Then N is prime if, and only if,

$$\beta^{\frac{N-1}{6}} \equiv -\varpi^j \bmod N, \; j \in \{1,2\}.$$

Proof: If N is prime, the conclusion follows from Theorem 5. Conversely, assume that the congruence holds. Suppose that $\pi \in R$ is a prime dividing N. Let $\beta_0 \equiv \beta \bmod \pi$ and let r be the order of $\beta_0 \bmod \pi$. Then $\beta_0^{N-1} \equiv 1(\pi)$, but $\beta_0^{(N-1)/2} \equiv -1(\pi)$. Therefore, r divides $k \cdot 2^m 3^n$ but not $k \cdot 2^{m-1} 3^n$. Hence $2^m | r$. Similarly, $\beta_0^{(N-1)/3} \equiv \varpi^{2j} \not\equiv 1 \bmod \pi$, so $3^n | r$.

This implies that $2^m 3^n$ is a divisor of $\mathcal{N}(\pi)$. If $\pi\overline{\pi} = p$ is a prime, then $p \equiv 1 \bmod 2^m 3^n$, in particular $p \geq 1 + 2^m 3^n$. Since $p^2 \geq (2^m 3^n + 1)^2 > k\cdot 2^m 3^n + 1 = N$, we must have $p = N$. On the other hand, if $\pi = p$ is a rational prime, then $p \equiv 2(3)$ and $\mathcal{N}(p) - 1 = (p-1)(p+1)$, and $2^m 3^n | p + 1$, i.e. $p \geq 2^m 3^n - 1$. Thus $p^2 \geq 2^m 3^n (2^m 3^n - 2) + 1 > N$ which finishes the proof.

5. SOME PRACTICAL CONSIDERATIONS. In Theorem 3 and Theorem 6 it is not necessary to explicitly compute $\overline{\alpha}^{-1} \bmod N$. In fact, assume $\alpha^r \equiv a + b\varpi \bmod N$, where r is a positive integer. Then $\beta^r \equiv \varpi^j \bmod N$ is equivalent to

$\alpha^r \equiv \overline{\alpha}^{-1}\varpi^j(N)$ or $a + b\varpi \equiv (a - b - b\varpi)\varpi^j(N)$. A moment's reflection reveals that

$$\begin{aligned}
\beta^{\frac{N-1}{3}} &\equiv \varpi \bmod N &&\Longleftrightarrow & \alpha^{\frac{N-1}{3}} &\equiv a + a\varpi \bmod N,\\
\beta^{\frac{N-1}{3}} &\equiv \varpi^2 \bmod N &&\Longleftrightarrow & \alpha^{\frac{N-1}{3}} &\equiv \quad a\varpi \bmod N,\\
\beta^{\frac{N-1}{6}} &\equiv -\varpi \bmod N &&\Longleftrightarrow & \alpha^{\frac{N-1}{6}} &\equiv a - a\varpi \bmod N,\\
\beta^{\frac{N-1}{6}} &\equiv -\varpi^2 \bmod N &&\Longleftrightarrow & \alpha^{\frac{N-1}{6}} &\equiv 2a + a\varpi \bmod N,
\end{aligned}$$

where a is a certain integer.

Usually, it is easy to find the appropriate α required in the theorems. To give an example for Theorem 3, let $k = 40$. We look for primes N of the form $N = 40\cdot 3^n + 1$. For $n \leq 325$ all these have been found by Williams and Zarnke [4]. Let $q = 7$ in Theorem 3. Then $\alpha = 2 + 3\varpi$ and $(7, N) > 1$ iff $n \equiv 4 \bmod 6$. These n can be excluded. Moreover, we need $N^2 \not\equiv 1 \bmod \alpha$. Since $R/\alpha R \simeq GF(7)$ this condition is satisfied if $N \not\equiv \pm 1(7)$. Hence $\alpha = 2 + 3\varpi$ suffices if $n \not\equiv 0(6)$. For $n = 543$ (not in Williams' and Zarnke's list) we find $\alpha^{(N-1)/3} \equiv a\varpi \bmod N$ for some integer a, hence $N = 40 \cdot 3^{543} + 1$ is prime.

If now $n \equiv 0(6)$ we may choose $q = 13$, where $\alpha - 1 + 3\varpi$. In this case, N is of the form $N = 40 \cdot 3^{6n} + 1 \equiv 2(13)$ and the condition $N^4 \not\equiv 1(13)$ is always satisfied. Hence, for $N = 40 \cdot 3^n + 1$ either $q = 7$ or $q = 13$ works.

Finally, we give an application of Theorem 6. Assume $k = 5$, i.e. $N = 5 \cdot 2^m 3^n + 1$. We may again choose $q = 7$, provided $N^2 \not\equiv 1(7)$ and $(\frac{7}{N}) = (\frac{N}{7}) \equiv N^3 \equiv -1(7)$. Here we have tacitly assumed that $m \geq 2$. Both conditions are met iff $N \bmod 7 \in \{3, 5\}$. Since $5 \equiv 3^5(7)$ and $2 \equiv 3^2(7)$, we must have $3^{2m+n+5} \bmod 7 \in \{2, 4\}$ or $2m + n \bmod 6 \in \{3, 5\}$.

For instance, take $m = 54$ and $n = 57$. We find $\alpha^{(N-1)/6} \equiv a - a\varpi \bmod N$ for some integer a. Hence $N = 5 \cdot 2^{54}3^{57} + 1$ is a prime number.

BIBLIOGRAPHY

1. Ireland, K., Rosen, M., A Classical Introduction to Modern Number Theory, Springer 1982.

2. Riesel, H., Prime Numbers and Computer Methods for Factorization, Birkhäuser 1985.

3. Robinson, R.M., The Converse of Fermat's Theorem, Amer. Math. Monthly **64**, 703-710 (1957).

4. 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).

5. Williams, H.C., A Note on the Primality of $6^{2^n}+1$ and $10^{2^n}+1$, Fibonacci Quarterly **26**, 296-305 (1988).