ACTA ARITHMETICA
110.2 (2003)

A generalization of Proth's theorem

by

Pedro Berrizbeitia (Caracas), T. G. Berry (Caracas)
and Juan Tena-Ayuso (Valladolid)

1. Introduction. Recall the celebrated

Theorem (Proth 1878). *Let $n = A \cdot 2^s + 1$ where A is odd and $A < 2^s$. Suppose $a \in \mathbb{Z}$ and $\left(\frac{a}{n}\right) = -1$ where $\left(\frac{a}{n}\right)$ is the Jacobi symbol. Then n is prime if and only if $a^{(n-1)/2} \equiv -1 \bmod n$.*

Proth's theorem gives a primality test for the numbers $A \cdot 2^s + 1$, $A < 2^s$, generalizing Pépin's test for primality of the Fermat numbers $2^{2^s} + 1$. In this paper we generalize Proth's theorem to give a test for primality of numbers of the form $n = Am^s + w_{m,s}$, where $m \in \mathbb{N}$, $w_{m,s} = \pm 1$ or certain other values depending on m and s (a full description of n is given in Proposition 2.2); the generalization is Theorem 2. We describe primality tests derived from this generalization and analyze their complexity. In the statement and proof of Theorem 2 properties of the higher power-residue symbols replace properties of the Jacobi symbol, and in the applications results relating to the Eisenstein reciprocity law replace the quadratic reciprocity law which is used in applications of the original Proth theorem to find the number a.

Primality tests for numbers of the form $Ap^s \pm 1$, p prime, have been extensively studied for at least two centuries. Lucas gave his famous test for Mersenne numbers $2^s - 1$, and also a test for determining primality of $A \cdot 3^s - 1$, using properties of the sequences now known as Lucas sequences. Hugh Williams and collaborators, in a series of papers beginning in the 70's, extended Lucas's methods to arbitrary p and gave many concrete algorithms; an overview of this work can be found in Williams's book [9]. More recently, primality tests for numbers $Ap^s \pm 1$ based on Proth's theorem and/or reciprocity rather than Lucas sequences have been given for small primes p. (See [7], [4], [6], [1], [2] for $p = 2, 3, 3, 3, 5$ respectively.) The present paper

2000 *Mathematics Subject Classification*: 11A51, 11Y11.
Key words and phrases: primality test, Eisenstein reciprocity, Proth's theorem.
Research of J. Tena-Ayuso partially supported by the Spanish grant DGICYT TIC2001-2235.

generalizes this line of attack, which applies to a larger family of numbers, and in many respects is simpler than the Lucas sequence approach.

2. Preliminaries. Notation introduced in this section will be used throughout the paper without further comment.

Let $f, r \in \mathbb{N}$. We define

$$\mathbb{N}_{f,r} = \{n \in \mathbb{N} : n^f \equiv 1 \bmod r\},$$
$$\mathbb{A}_{f,r} = \{n \in \mathbb{N}_{f,r} : \text{ if } l \mid n \text{ then } l \in \mathbb{N}_{f,r}\}.$$

PROPOSITION 2.1. *If $n \in \mathbb{A}_{f,r}$ where $r > \sqrt{n}$ and none of the solutions of $x^f \equiv 1 \bmod r$, $1 < x < r$, divides n, then n is prime.*

Proof. If $l \mid n$, $l \neq 1$, then $l^f \equiv 1 \bmod r$, so, by the hypotheses, $l > r > \sqrt{n}$. Thus every non-trivial divisor of n is greater than $\sqrt{n}$, hence n is prime. ∎

Let $m, n \in \mathbb{N}, m \geq 2$, $(n, m) = 1$, and let f be the order of $n \bmod m$. For $t \in \mathbb{N}$ we set $\nu_m(t) = v$ if m^v divides t but m^{v+1} does not divide t.

PROPOSITION 2.2. *The following are equivalent*:

(1) $\nu_m(n^f - 1) \geq (\log_m n)/2$.

(2) $n \in \mathbb{N}_{f,m^s}$ *where* $m^s > \sqrt{n}$.

(3) $n = Am^s + w$ *where* $0 < A \leq m^s$, w *satisfies the conditions* $|w| \leq m^s/2$ *and* $w^f \equiv 1 \bmod m^s$, *and* $A = m^s$ *can occur only if* $w < 0$.

Proof. (1)⇒(2). Set $s = \nu_m(n^f - 1)$. Then (1) says $m^s > m^{(\log_m n)/2} = \sqrt{n}$.

(2)⇒(3). Dividing n by m^s, we have $n = Am^s + w$ with $|w| \leq m^s/2$. Since $n \equiv w \bmod m^s$ and $n \in \mathbb{N}_{f,m^s}$ we also have $w^f \equiv 1 \bmod m^s$. Now $m^s > \sqrt{n}$, so $m^{2s} > n = Am^s + w$; if $w > 0$ this implies $A < m^s$. If $w < 0$, then since $|w| \leq m^s/2$, we obtain $m^{2s} \geq Am^s - m^s/2$, whence $m^s \geq A - 1/2$. Since A is an integer, $A \leq m^s$ follows.

(3)⇒(1). It is enough to show $n < m^{2s}$, since this translates immediately to (1). If $w > 0$, then $n = Am^s + w \leq (A+1)m^s \leq m^{2s}$. If $w < 0$, then $n = Am^s + w < Am^s \leq m^{2s}$ (since $A \leq m^s$). ∎

In the rest of this paper, n always denotes an integer satisfying the equivalent conditions of Proposition 2.2.

Set $\zeta_m = e^{2\pi i/m}$. Let $K = \mathbb{Q}(\zeta_m)$ and $D = \mathbb{Z}[\zeta_m]$, so D is the ring of integers of the cyclotomic field K. Let $G = \mathrm{Gal}(K/\mathbb{Q})$. Recall G is isomorphic to $\mathbb{Z}_m^* = (\mathbb{Z}/m\mathbb{Z})^*$ via $i \mapsto \sigma_i$ where $\sigma_i(\zeta_m) = \zeta_m^i$. Following a fairly common notation, if $\tau \in \mathbb{Z}[G]$, say $\tau = \sum_{j \in J} n_j \sigma_j$ where J is some index set, then for $x \in K$, x^τ denotes $\prod_{j \in J} \sigma_j(x)^{n_j}$.

LEMMA 2.3. *Let $\alpha \in K$ and let $l \in \mathbb{Z}$ be prime. Then $\alpha^l \equiv \sigma_l(\alpha) \bmod l$, hence if $g \in \mathbb{Z}[x]$ then $\alpha^{g(l)} \equiv \alpha^{g(\sigma_l)} \bmod l$.*

The proof of this well-known result is immediate.

Finally, I denotes a set of coset representatives of $\mathbb{Z}_m^*/(n)$. Thus, if n is a rational prime, and η is any prime ideal of D lying over n, then the ideal nD is $\prod_{i\in I}\sigma_i(\eta)$.

2.1. *Power-residue symbols and Eisenstein reciprocity.* Throughout this section, l denotes a rational prime not dividing m, k is the order of l mod m, and $\mathcal{L}$ is a prime ideal of D, lying over l. Take $a \in D$, $a \notin \mathcal{L}$. There is a unique mth root of 1 in K, call it ζ, such that

$$a^{(l^k-1)/m} \equiv \zeta \bmod \mathcal{L}.$$

In these circumstances, the mth power-residue symbol is defined as

$$\left(\frac{a}{\mathcal{L}}\right)_m = \zeta.$$

The definition is extended to arbitrary ideals $J \subseteq D$, coprime with m and a, by multiplicativity. That is, we have $J = \prod_i \mathcal{L}_i^{n_i}$ for prime ideals $\mathcal{L}_i$ and positive integers n_i and define

$$\left(\frac{a}{J}\right)_m = \prod_i \left(\frac{a}{\mathcal{L}_i}\right)_m^{n_i}.$$

If (d) is the principal ideal generated by $d \in D$, then we write $\left(\frac{a}{d}\right)_m$ instead of $\left(\frac{a}{(d)}\right)_m$.

We shall use the following properties of the power-residue symbol, which can be found in [5, Props. 14.2.2–14.4.4]):

Proposition 2.4. *Let $a \in D$. Then*:

$$\left(\frac{a}{\mathcal{L}}\right)_m = 1 \quad \textit{if and only if } a \textit{ is an } m\textit{th power} \bmod \mathcal{L}, \tag{2.1}$$

$$\left(\frac{ab}{J}\right)_m = \left(\frac{a}{J}\right)_m \left(\frac{b}{J}\right)_m, \tag{2.2}$$

$$\left(\frac{a}{JJ'}\right)_m = \left(\frac{a}{J}\right)_m \left(\frac{a}{J'}\right)_m, \tag{2.3}$$

$$\left(\frac{a}{J}\right)_m^{\sigma} = \left(\frac{a^\sigma}{J^\sigma}\right)_m \quad \forall \sigma \in G, \tag{2.4}$$

$$\left(\frac{a}{J}\right)_m^{\sigma_i} = \left(\frac{a}{J}\right)_m^{i} \quad \textit{for } \sigma_i \in G \textit{ as defined above.} \tag{2.5}$$

We shall not make use of the Eisenstein reciprocity law, but rather the following theorem, of which the reciprocity law is a corollary.

Theorem 1 ([5, Cor. 2, p. 218]). *Suppose $\alpha \in D$ is prime to m and $B \subseteq D$ is an ideal prime to m and such that* $\operatorname{Nm} B$ *is prime to α, where*

$\operatorname{Nm} B$ *is the ideal norm of* B. *Then*

$$\left(\frac{\operatorname{Nm} B}{\alpha}\right)_m = \left(\frac{\alpha}{\operatorname{Nm} B}\right)_m \left(\frac{\varepsilon(\alpha)}{B}\right)_m,$$

where $\varepsilon(\alpha)$ *is* $\pm\zeta_m^i$ *for some* i. ∎

3. The generalized Proth theorem. Let ϕ denote the Euler ϕ-function, and Φ_k the kth cyclotomic polynomial.

THEOREM 2. *Suppose* $n = Am^s + w$ *satisfies the conditions of Proposition* 2.2. *In particular* n *has order* f *mod* m. *Suppose further that if* $x^{\phi(m)} \equiv 1 \bmod m^s$ *and* $1 < x < m^s$ *then* x *does not divide* n. *Let* $a \in D$ *be such that* $\left(\frac{a}{n}\right)_m$ *is a primitive* m*th root of* 1. *Then the following are equivalent*:

(1) n *is prime.*

(2) $(a^\tau)^{(n^f-1)/m} \equiv \left(\frac{a}{n}\right)_m \bmod n$, *where* $\tau = \sum_{i\in I} i\sigma_{i^{-1}}$.

(3) $(a^{\tau\gamma})^{\Phi_f(n)/m} \equiv \left(\frac{a}{n}\right)_m \bmod n$, τ *as above, and* $\gamma = \prod_{d|f,\, d<f} \Phi_d(\sigma_w)$.

(4) *The same as* (3), *except that the congruence is taken mod* η *where* $\eta \subseteq D$ *is some ideal lying over* n (*i.e. such that* $\eta \cap \mathbb{Z} = n\mathbb{Z}$).

(5) $n \in \mathbb{A}_{\phi(m),m^s}$.

Proof. We shall show (1)⇒(2)⇒(5)⇒(1), and (1)⇒(3)⇒(4)⇒(5).

(1)⇒(2). Since n is prime, $nD = \prod_{i\in I} \sigma_i(\eta)$ where η is any prime ideal of D lying over n and I is a set of coset representatives of $\mathbb{Z}_m^*/(n)$, as defined in Section 2.

By the properties (2.1)–(2.5) of the power-residue symbol,

$$\left(\frac{a}{n}\right)_m = \left(\frac{a}{\prod_i \sigma_i(\eta)}\right)_m = \prod_{i\in I} \left(\frac{a}{\sigma_i(\eta)}\right)_m.$$

But

$$\left(\frac{a}{\sigma_i(\eta)}\right)_m = \sigma_i\left(\frac{\sigma_{i^{-1}}a}{\eta}\right)_m = \left(\frac{\sigma_{i^{-1}}a}{\eta}\right)_m^i$$

so that

$$\left(\frac{a}{n}\right)_m = \prod_{i\in I} \left(\frac{\sigma_{i^{-1}}a}{\eta}\right)_m^i = \left(\frac{a^{\sum_{i\in I} i\sigma_{i^{-1}}}}{\eta}\right)_m = \left(\frac{a^\tau}{\eta}\right)_m$$

with τ defined as in (2). Then

$$\left(\frac{a^\tau}{\eta}\right)_m \equiv (a^\tau)^{(n^f-1)/m} \bmod \eta.$$

Since η is an arbitrary prime ideal lying over n, this congruence holds for all prime ideals η lying over n. Therefore, by the Chinese remainder theorem, it holds mod n. Thus (1)⇒(2).

(1)⇒(3). We may assume (2). Now $n^f - 1 = (\prod_{d|f,\, d<f} \Phi_d(n)) \cdot \Phi_f(n)$. But m does not divide $\Phi_d(n)$ if $d < f$: if m divides $\Phi_d(n)$ then m divides $n^d - 1$, which, since n has order exactly f mod m, implies that f divides d, a contradiction. Moreover, by Lemma 2.3, $a^{\Phi_d(n)} = a^{\Phi_d(\sigma_n)} = a^{\Phi_d(\sigma_w)}$ (the last equality since $n \equiv w \bmod m$). With these observations (3) is a rewriting of (2).

(3)⇒(4) is clear.

(4)⇒(5). Let $b = (a^{\tau\gamma})^{\Phi_f(n)/m^s}$. Let $l > 1$ be a prime divisor of n. Then we claim that there is a prime ideal $\mathcal{L} \subseteq D$ lying over l and containing η. (To see this it is enough to show $(l) + \eta \neq D$, which is standard.) Then the hypothesis implies that $b^{m^{s-1}} \equiv \left(\frac{a}{n}\right)_m \bmod \mathcal{L}$. Since $\left(\frac{a}{n}\right)_m$ is a primitive mth root of 1, this implies that b has order m^s mod $\mathcal{L}$. Thus $m^s \mid l^k - 1$, where k is the order of l mod m. Since k divides $\phi(m)$ we obtain $l^{\phi(m)} \equiv 1 \bmod m^s$. This holds for any prime divisor l of n, so $n \in A_{\phi(m),m^s}$.

(2)⇒(5) follows the same line as (4)⇒(5), with $b' = (a^{\tau})^{(n^f-1)/m^s}$ instead of b.

(5)⇒(1). By hypothesis no solution of $x^{\phi(m)} \equiv 1 \bmod m^s$ satisfying $1 < x < m^s$ is a divisor of n. Thus, by Proposition 2.1, n is prime. ∎

When $m = 2$ the condition on solutions of $x^{\phi(m)} \equiv 1 \bmod m^s$ is empty, and the case (1)⇔(2) of Theorem 2 is the original Proth theorem.

4. Applications to primality testing. The basic primality test comes from computing both sides of Theorem 2(2), once a suitable a has been found. Since the Galois action on $a \in D$ is easy to compute, using (3) instead of (2) gives a speedup by a factor ≤ 2 (since $f/2 \leq \phi(f) \leq f$) (see Theorem 4). Theorem 2(4) suggests that if an ideal η is known, exponentiation can be done in a module of rank f instead of $\phi(m)$, which is a significant improvement. Methods of exploiting this idea, and implementation details in general, will be discussed in a sequel to this paper. Here we restrict ourselves to discussing methods for finding a, and some basic estimates of complexity.

In the primality tests for $A \cdot 2^s + 1$ based on the original Proth theorem, the quadratic reciprocity law makes it easy to find the integer a necessary for the test. The following shows how Eisenstein reciprocity, more precisely Theorem 1, plays a similar role for the generalized Proth theorem.

PROPOSITION 4.1. *Suppose $p \in \mathbb{N}_{f,m^s}$ is an odd prime of order f mod m, where $s \geq 2$. Suppose also that $(f, m) = 1$. If $a \in D$ is coprime with m and p then*

$$\left(\frac{a}{p}\right)_m = \left(\frac{p}{a}\right)_m.$$

Proof. Take B as a prime ideal lying over p. Thus $\operatorname{Nm} B = p^f$. Applying Theorem 1 with $\alpha = a$ gives

$$\left(\frac{p}{a}\right)_m^f = \left(\frac{a}{p}\right)_m^f \left(\frac{\varepsilon(a)}{B}\right)_m.$$

But

$$\left(\frac{\varepsilon(a)}{B}\right)_m \equiv \varepsilon(a)^{(p^f-1)/m} \bmod B.$$

Recall that $\varepsilon(a) = \pm\zeta_m^i$ for some i. The exponent on the right-hand side is a multiple of m if $s \geq 2$. Moreover, the exponent is always even, since p is an odd prime. Thus $\left(\frac{\varepsilon(a)}{B}\right)_m = 1$ and we have

$$\left(\frac{p}{a}\right)_m^f = \left(\frac{a}{p}\right)_m^f.$$

But, by hypothesis, $(m, f) = 1$ so raising to the fth power is an automorphism of the group of mth roots of 1, and the proposition follows. ∎

We note that if m is prime, then $(m, f) = 1$ is always satisfied, since f is a divisor of $\phi(m) = m - 1$.

LEMMA 4.2. *Let $\mathcal{L}$ be a prime ideal of D lying over the prime $l \in \mathbb{Z}$. Suppose l is coprime with n and m. Then*

$$\left(\frac{n}{\mathcal{L}}\right)_m = 1 \quad \textit{iff} \quad n^{(l-1)/\gcd(l-1,m)} \equiv 1 \bmod l.$$

Note that this condition is automatically satisfied if $\gcd(n, l-1) = 1$.

Proof. We first note $\left(\frac{n}{\mathcal{L}}\right)_m = 1$ iff n is an mth power mod l. Indeed, if n is an mth power mod l, then it is an mth power mod $\mathcal{L}$ (since $\mathcal{L}$ divides l), hence $\left(\frac{n}{\mathcal{L}}\right)_m = 1$. Conversely, $\left(\frac{n}{\mathcal{L}}\right)_m = 1$ implies n is an mth power mod $\mathcal{L}$. Then, since $(l, m) = 1$, l is unramified in D, hence a product of distinct primes, all of them conjugates of $\mathcal{L}$. It is easy to verify that n is also an mth power mod each of the conjugates, so, by the Chinese remainder theorem, an mth power mod l. The fact that n is an mth power mod l iff $n^{(l-1)/\gcd(l-1,m)} \equiv 1 \bmod l$ is an exercise in elementary group theory, based on the fact that $(\mathbb{Z}/l\mathbb{Z})^*$ is cyclic of order $l - 1$. ∎

PROPOSITION 4.3. *Let q be a prime, $q \equiv 1 \bmod m$, and suppose $n^{(q-1)/m}$ has order m mod q. Let $a \in D$ be such that* $\operatorname{Nm} a = tq$, *where every prime divisor l of t satisfies $n^{(l-1)/\gcd(l-1,m)} \equiv 1 \bmod l$. Then $\left(\frac{n}{a}\right)_m$ is a primitive mth root of* 1.

Proof. The ideal generated by a must be $aD = TQ$, where T has norm t and Q is a prime ideal of D lying over q. Since $\left(\frac{n}{Q}\right)_m \equiv n^{(q-1)/m} \bmod Q$ the hypothesis implies that $\left(\frac{n}{Q}\right)_m$ is a primitive mth root of 1. Also, each prime

ideal $\mathcal{L}$ dividing T lies over a prime dividing t, hence the hypothesis allows us to apply Lemma 4.2, and thus obtain $\left(\frac{n}{\mathcal{L}}\right)_m = 1$. By multiplicativity of the symbol this implies $\left(\frac{n}{T}\right)_m = 1$. The result follows since $\left(\frac{n}{a}\right)_m = \left(\frac{n}{T}\right)_m \left(\frac{n}{Q}\right)_m$. ∎

From Proposition 4.1 it follows that to be able to apply the generalized Proth theorem, it suffices to find a such that $\left(\frac{n}{a}\right)_m$ is a primitive mth root of 1. To do this, Proposition 4.3 shows us how to proceed. First, find a prime $q \equiv 1 \bmod m$ such that $u = n^{(q-1)/m}$ has order m mod q. Next, choose a from the ideal Q generated by q and $\zeta_m - u$, compute $\operatorname{Nm} a$ and see if it satisfies the hypotheses of Proposition 4.3. Our philosophy is that A, m are fixed, while s (and hence w) vary. Then a prime $q \equiv 1 \bmod m$ should satisfy the hypotheses of Proposition 4.3 for many (though not all) s. Experiments indicate that this is not a vain hope, and that once q is found, a is easy to find.

Finally, we record the following generalization of Theorem 2 which extends the scope of the corresponding primality tests.

THEOREM 3. *Let* $n = Am_1^{s_1} m_2^{s_2} \dots m_t^{s_t} + w$, *where* $\gcd(m_i, m_j) = 1$, $i \neq j$, $A < M = \prod_{i=1}^t m_i^{s_i}$, $2|w| < M$, *and* w *satisfies the system*

$$w^{f_i} \equiv 1 \bmod m_i^{s_i}$$

where f_i *is the order of* n *mod* m_i. *Assume further that no solution of* $x^{\phi(m_i)} \equiv 1 \bmod m_i^{s_i}$, $1 < x < M$, *divides* n. *Suppose that for* $i = 1, \dots, t$, $a_i \in \mathbb{Z}[\zeta_{m_i}]$ *is such that* $\left(\frac{a_i}{n}\right)_{m_i}$ *is a primitive* m_i*th root of* 1. *Then the following are equivalent*:

(1) n *is prime.*

(2) *For* $i = 1, \dots, t$, $(a_i^{\tau_i})^{(n^{f_i}-1)/m_i} \equiv \left(\frac{a_i}{n}\right)_{m_i} \bmod m_i$, *where* $\tau_i = \sum_{j \in I_i} j\sigma_{j^{-1}}$, *and* I_i *is a set of coset representatives of* $\mathbb{Z}_{m_i}^*/(n)$.

(3) *For* $i = 1, \dots, t$, $(a_i^{\tau_i \gamma_i})^{\Phi_{f_i}(n)/m} \equiv \left(\frac{a_i}{n}\right)_{m_i} \bmod n$ *with* τ_i *as above and* $\gamma_i = \prod_{d|f_i,\, d<f_i} \Phi_d(\sigma_w)$.

(4) *The same as* (3), *except that the congruences are taken mod* η *where* $\eta \subseteq D$ *is some ideal lying over* n (*i.e. such that* $\eta \cap \mathbb{Z} = n\mathbb{Z}$).

(5) $n \in \bigcap_{i=1}^t \mathbb{A}_{\phi(m_i), m_i^{s_i}}$.

The proof is essentially the same as the proof of Theorem 2. For (5)⇒(1), observe that the hypothesis implies that $n \in \mathbb{A}_{\phi(m_1 \dots m_t), M}$, $M > \sqrt{n}$, and apply Proposition 2.1.

4.1. *Complexity.* We first record some accountancy involving exponentiation in K. Throughout, log means $\log_2$.

PROPOSITION 4.4. *For* $a \in K = \mathbb{Q}(\zeta_m)$, $j \in \mathbb{Z}$, *the calculation of* a^j *needs at most* $\left(\left(\frac{3}{2}\phi(m)\right)^2 + \phi(m)/2\right) \log j$ *integer multiplications.*

Proof. First observe that, if we write elements of K in the $\mathbb{Q}$-basis ζ_m^i, $i = 0, \ldots, \phi(m)-1$, then multiplying distinct elements needs $\phi(m)^2$ multiplications, while squaring an element needs $\phi(m)+\binom{\phi(m)}{2} = (\phi(m)+1)\phi(m)/2$ multiplications. Calculating a^j in the usual way by writing j in binary form needs at most $\log j$ squarings and at most $\log j$ multiplications of distinct elements of K. The total number of multiplications is thus bounded above by $\left(\left(\frac{3}{2}\phi(m)\right)^2 + \phi(m)/2\right)\log j$, which is the stated result. ∎

In what follows the *cost* of an algorithm means the number of mod n multiplications required by the algorithm. The cost of addition mod n is neglected, since addition is an order of magnitude faster than multiplication.

THEOREM 4. *Assume that an a satisfying the conditions of Proposition* 4.1 *has been found, and that if $1 < x < m^s$ and $x^{\phi(m)} \equiv 1 \bmod m^s$ then x does not divide n. Then the primality of n can be tested with cost bounded above by*

$$\frac{(3\phi(m)^2 + \phi(m))f \log n}{2}$$

using (2) *of Theorem* 2, *and with cost bounded above by*

$$\frac{(3\phi(m)^2 + \phi(m))\phi(f) \log n}{2}$$

using (3).

Proof. The first follows by observing that $j = (n^f - 1)/m < n^f$, and the second by observing that $j = \Phi_f(n)/m < n^{\phi(f)}$, as can be seen fairly easily. ∎

With our philosophy of keeping A and m fixed, Theorem 4 just tells us that the cost is $C \log n$, where C is a constant that depends in principle on m and f. We consider the verification of the condition on solutions of $x^{\phi(m)} \equiv 1 \bmod n$ to be part of the pre-computation, since this is a computation that can be done when finding the $n = Am^s + \omega_s$ to be tested. Once we have q as described in Proposition 4.3, a is easy to find. The problem of finding q when m is prime is dealt with in [8].

We should like to make C as small as possible. With more sophisticated methods of multiplication in K, $\phi(m)^2$ in Theorem 4 can be replaced by $2\phi(m)$ (see [3]). In a sequel to the present paper, we will show that if the factorization of the ideal nD can be obtained, then we can obtain a smaller C that depends only on f.

References

[1] P. Berrizbeitia and T. G. Berry, *Cubic reciprocity and generalised Lucas–Lehmer tests for primality of $a \cdot 3^n \pm 1$*, Proc. Amer. Math. Soc. 26 (1999), 1923–1925.

[2] P. Berrizbeitia, M. Odreman and J. Tena-Ayuso, *Primality test for numbers m with a high power of* 5 *dividing* $m^4 - 1$, Theoret. Comput. Sci. 297 (2003), 25–36.

[3] H. Cohen, *A Course in Computational Algebraic Number Theory*, Grad. Texts in Math. 138, Springer, 1991.

[4] A. Guthmann, *Effective primality tests for integers of the forms* $N = k \cdot 3^n + 1$ *and* $N = k \cdot 2^m 3^n + 1$, BIT 32 (1992), 529–534.

[5] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, 1990.

[6] C. Kirfel and Ø. J. Rødseth, *On the primality of* $2h \cdot 3^n + 1$, Discrete Math. 241 (2001), 395–406.

[7] M. Rosen, *A proof of the Lucas–Lehmer test*, Amer. Math. Monthly 95 (1988), 855–856.

[8] A. Stein and H. C. Williams, *Explicit primality criteria for* $(p-1)p^n - 1$, Math. Comp. 69 (2000), 1721–1734.

[9] H. C. Williams, *Edouard Lucas and Primality Testing*, Canad. Math. Soc. Ser. Monographs Adv. Texts 22, Wiley, 1998.

Departamento de Matemáticas
Puras y Aplicadas
Universidad Simón Bolívar
Caracas, Venezuela
E-mail: pedrob@usb.ve
berry@usb.ve

Departamento de Algebra y Geometria
Facultad de Ciencias
Universidad de Valladolid
Prado de la Magdalena s/n
47005 Valladolid, Spain
E-mail: tena@agt.uva.es

Received on 10.9.2001
and in revised form on 29.3.2002 (4103)