MATHEMATICS OF COMPUTATION
Volume 69, Number 232, Pages 1721–1734
S 0025-5718(00)01212-6
Article electronically published on February 23, 2000

EXPLICIT PRIMALITY CRITERIA FOR $(p-1)\,p^n-1$

ANDREAS STEIN AND H. C. WILLIAMS

Abstract. Deterministic polynomial time primality criteria for 2^n-1 have been known since the work of Lucas in 1876–1878. Little is known, however, about the existence of deterministic polynomial time primality tests for numbers of the more general form $N_n = (p-1)\,p^n-1$, where p is any fixed prime. When $n > (p-1)/2$ we show that it is always possible to produce a Lucas-like deterministic test for the primality of N_n which requires that only $O(q\,(p+\log q)+p^3+\log N_n)$ modular multiplications be performed modulo N_n, as long as we can find a prime q of the form $1+k\,p$ such that N_n^k-1 is not divisible by q. We also show that for all p with $3 < p < 10^7$ such a q can be found very readily, and that the most difficult case in which to find a q appears, somewhat surprisingly, to be that for $p=3$. Some explanation is provided as to why this case is so difficult.

1. Introduction

Let $n\,(>1)$ be an odd integer and put $M_n = 2^n-1$. In 1876 Lucas (see Williams [10, chapter 3] for a discussion and references) produced a test that is sufficient for proving the primality of M_n whenever $n \equiv 3 \pmod 4$. Later he provided another sufficient test in the case of $n \equiv 1 \pmod 4$; this latter test has now become well known as the Lucas-Lehmer test for the primality of the Mersenne numbers M_n. Although this might have been known to Lucas (see [10, pp. 109–110]), it was Lehmer [3] who showed that the test was also necessary for the primality of M_n and that it holds for any odd n. Simply put, it states that M_n is a prime if and only if $M_n | S_{n-2}$, where $S_0 = 4$ and $S_{n-2} \pmod{M_n}$ can be computed recursively by $S_{k+1} \equiv S_k^2-2 \pmod{M_n}$ $(k = 0, 1, 2, \ldots, n-3)$. Because of the historical significance of the Mersenne numbers, the simplicity of this test and its consequent ease of implementation, it has been used to find almost all of the largest known primes within the last century. Indeed the recent (1997) discovery of the current largest known prime $M_{3021377}$ by Clarkson, Woltman and over 2000 other researchers was achieved through the use of Woltman's implementation of the Lucas-Lehmer test.

It is less well known that Lucas [4] also produced a sufficiency test for the primality of $2\cdot 3^n-1$ whenever $4 \nmid n$. Much later Williams ([6], Theorem 4, Corollary) produced a necessary and sufficient test for the primality of $N_n = 2\cdot 3^n-1$ whenever $6 \nmid n$. There is also (Williams [5]) a necessary and sufficient test for the primality

Received by the editor October 24, 1997 and, in revised form, October 23, 1998.
1991 *Mathematics Subject Classification.* Primary 11Y11; Secondary 11Y16.
Key words and phrases. Primality test, Mersenne numbers, Lucas functions, Gauss sums, covering sets.
Research supported by NSERC of Canada Grant #A7649.

of $N_n = 4 \cdot 5^n - 1$ for any positive integral value of n, of $N_n = 6 \cdot 7^n - 1$ (Williams [7]) for any $n \not\equiv 1 \pmod 7$ and of $N_n = 10 \cdot 11^n - 1$ (Williams [7]) for any $n \not\equiv 17 \pmod{22}$. Each of these tests, like the Lucas-Lehmer test, executes in $O(\log N_n)$ modular multiplications modulo N_n. Furthermore, they are all of *Lucas-Lehmer type*, which is to say that they have the following three properties (cf. Williams [8]):

i) The test is restricted to values of N given by some polynomial in a^n, where a is some fixed integer and the exponent n often belongs to some fixed congruence class and exceeds a certain bound.

ii) A sequence $\{S_i : i \geq 0\}$ is employed where S_0 can be computed by a deterministic algorithm that executes in $O(\log N)$ modular multiplications $\pmod N$. Also S_{i+1} is defined $\pmod N$ for $i \geq 0$ by $S_{i+1} = f(S_i)$, where f is a fixed polynomial in $\mathbb{Z}[x]$.

iii) N is a prime if and only if $h(S_{m_1}, S_{m_2}, \ldots, S_{m_k}) \equiv 0 \pmod N$, where the values of the m_i $(i = 1, 2, \ldots, k)$ depend on n, and h is some fixed polynomial in $\mathbb{Z}[x_1, x_2, \ldots, x_k]$ which can be evaluated in $O(\log N)$ modular multiplications $\pmod N$.

The above results suggest the possible existence of Lucas-Lehmer type tests for $N_n = (p-1)\,p^n - 1$, where p is any fixed prime. In this paper we will show that a necessary and sufficient Lucas-Lehmer type test for the primality of N_n exists for any prime p such that $3 < p < 10^7$ and any $n > (p-1)/2$. Also, this test will execute in $O(\log N_n)$ modular multiplications modulo N_n. We emphasize, however, that the practical use of these tests is limited.

2. The Lucas functions

All of the tests mentioned above were derived through the use of the Lucas functions. If we let P, Q denote two coprime integers and α, β the zeros of $x^2 - Px + Q$, then the *Lucas functions* $U_n(P,Q)$ and $V_n(P,Q)$ $(n \in \mathbb{Z})$ are defined by

$$U_n(P,Q) = (\alpha^n - \beta^n)/(\alpha - \beta), \quad V_n(P,Q) = \alpha^n + \beta^n \ .$$

We also define the *discriminant* $\Delta = (\alpha - \beta)^2 = P^2 - 4Q$. If there is no ambiguity concerning the values of the arguments P, Q, they are often omitted and the symbols U_n and V_n are used to represent the Lucas functions. Note that both U_n and V_n satisfy the simple linear recurrence

$$X_{k+1} = PX_k - QX_{k-1} \quad (k \in \mathbb{Z}) \ .$$

When working with the Lucas functions modulo a positive integer N such that $\gcd(N, Q) = 1$, it is often convenient to define

$$W_n = W_n(P,Q) \equiv V_{2n}(P,Q)Q^{-n} \pmod N \quad (n \in \mathbb{Z}) \ .$$

By results in Williams [9], [10, §4.4], we can compute W_n modulo N in $O(\log n)$ modular multiplications and additions $\pmod N$. From this definition and the definition of U_n, V_n it is easy to show that $W_0 = 2$, $W_1 \equiv P^2Q^{-1} - 2$, and $W_{n+1} \equiv W_1W_n - W_{n-1} \pmod N$. Furthermore, we have

$$W_{2n} \equiv W_n^2 - 2 \pmod N \ , \tag{2.1}$$

$$W_n^2 - \Delta(Q^{-n}U_{2n})^2 \equiv 4 \pmod N \ . \tag{2.2}$$

If we define the polynomial $G_n(x)$ by $G_{-1}(x) = -1$, $G_0(x) = 1$, $G_{m+1}(x) = xG_m(x) - G_{m-1}(x)$ $(m \in \mathbb{Z})$, then

$$x^n G_n(x + x^{-1}) = (x^{2n+1} - 1)/(x - 1) \ .$$

Putting $S_0(x) = 0$, $S_1(x) = 1$, $C_0(x) = 2$, $C_1(x) = x$ with both $S_n(x)$ and $C_n(x)$ satisfying the linear recurrence

$$X_{m+1} = xX_m - X_{m-1} \ ,$$

it is easy to see that

$$S_n(x + x^{-1}) = (x^n - x^{-n})/(x - x^{-1}), \quad C_n(x + x^{-1}) = x^n + x^{-n} \ .$$

Also, since $G_n(x) = S_{n+1}(x) + S_n(x)$, we have

$$G_n(x) + G_{n-1}(x) = (x + 2)S_n(x) \ ,$$
$$G_n(x) - G_{n-1}(x) = C_n(x) \ .$$

From these last two results and the easily verified identities $C_{2n}(x) = C_n(x)^2 - 2$, $S_{2n}(x) = S_n(x)C_n(x)$, we can deduce that

$$G_{2n-1}(x) = G_n(x)G_{n-1}(x) - G_{n-1}(x)^2 + 1 \ ,$$
$$G_{2n}(x) = G_n(x)^2 - G_n(x)G_{n-1}(x) - 1 \ .$$

Thus, modulo N, one can use the same ideas as those employed in Williams [9, p.387] to compute $G_n(x) \pmod N$ in only $O(\log n)$ modular multiplications and additions modulo N. The importance of the polynomial $G_n(x)$ in our work derives from the following congruences (see [9]):

$$U_{(2s+1)n} \equiv Q^{ns} U_n G_s(W_n) \pmod N \ , \tag{2.3}$$

$$V_{(2s+1)n} \equiv (-1)^s Q^{ns} V_n G_s(-W_n) \pmod N \ . \tag{2.4}$$

Also, from (2.4), (2.1) and the definition of W_n we get

$$W_{(2s+1)n} \equiv (-1)^s W_n G_s(2 - W_n^2) \pmod N \ . \tag{2.5}$$

We now consider the following result, given as Corollary 11.3.3 of [10].

Theorem 2.1. *Let p be an odd prime, $s = (p-1)/2$ and N an odd integer such that $p \nmid N$. If for some integers P, Q we have $\gcd(Q, N) = 1$ and*

$$G_s\left(W_m(P, Q)\right) \equiv 0 \pmod N \ , \tag{2.6}$$

then if r is any prime divisor of N and $p^k \parallel p\,m$, we must have $r^2 \equiv 1 \pmod{p^k}$.

Thus, in the case that (2.6) holds, we can greatly restrict the possible prime factors of N. Indeed, if we specialize N to $Ap^n - 1$, we can say more.

Corollary 2.2. *Let $N = Ap^n - 1$ $(A < p^n)$, where p is an odd prime. If for some P, Q we have $\gcd(Q, N) = 1$ and*

$$G_s\left(W_{(N+1)/p}(P, Q)\right) \equiv 0 \pmod N \ , \tag{2.7}$$

where $s = (p-1)/2$, then N is a prime.

Proof. Suppose N is composite and r is any prime divisor of N. By the theorem we know that $r^2 \equiv 1 \pmod{p^n}$ or $r \equiv \pm 1 \pmod{p^n}$. Thus, $p^{2n} - 1 > N \geq (-1 + 2p^n)^2$, which is impossible. □

3. Some primality tests

In order to prove a number like N to be a prime by Corollary 2.2, it is necessary to find values for P, Q for which we can guarantee that (2.7) will be true. As pointed out in [5] and [9], one way of approaching the task of ensuring that (2.7) will hold is by making use of Gauss sums. As this is explained at some length in [10, chapter 11], we will simply state most of the results that we will need here.

We first mention that if p, q are distinct odd primes such that $p \mid q-1$, then there exist certain integers $C(i,p,q)$ for $i = 0, 1, 2, \dots, s-1$ ($s = (p-1)/2$) which can be computed by a deterministic algorithm requiring at most $O((p+\log q)\, q) + O(p^3)$ arithmetic operations, where the numbers involved will not exceed $(2q)^{p/2}$ (see p.274 or (11.1.4) of [10]). Some tables of values of $C(i,p,q)$ can be found in [5]. We will now explain why these numbers assume importance in primality testing of $A\,p^n - 1$. Suppose r is any prime such that $r \equiv -1 \pmod{p}$. We know (see, for example, Theorem 9.4.3 of [10]) that $G_s(x)$ has exactly s zeros modulo r. Let R be any one of these and put $P = \sum_{i=0}^{s-1} C(i,p,q)R^i$, $Q = q^{r-2}$; then, if $(r/q)_p \neq 1$, we must have ([10, p.274])

$$r \nmid U_{(r+1)/p}(P,Q) \quad \text{and} \quad r \mid U_{r+1}\ .$$

By (2.3) we get the following theorem.

Theorem 3.1. *Let r be any prime such that $r \equiv -1 \pmod{p}$ and let R be any integer such that $G_s(R) \equiv 0 \pmod{r}$. If $r^{(q-1)/p} \not\equiv 1 \pmod{q}$ and*

$$P \equiv \sum_{i=0}^{s-1} C(i,p,q)R^i\ ,\ Q \equiv q^{p-2} \pmod{r}\ ,$$

then

$$G_s\left(W_{(r+1)/p}\right) \equiv 0 \pmod{r}\ .$$

By combining the results of Theorem 3.1 and Corollary 2.2, we get Theorem 3.2 (cf. Theorem 11.3.6 of [10]).

Theorem 3.2. *Let $N = A\,p^n - 1$, $s = (p-1)/2$, where p is an odd prime, $A < p^n$ and $2 \mid A$. Let q be any prime such that $q \equiv 1 \pmod{p}$ and $(N/q)_p \neq 0, 1$. If R satisfies the congruence*

$$G_s(R) \equiv 0 \pmod{N}$$

and

$$P = \sum_{i=0}^{s-1} C(i,p,q)R^i\ ,\quad Q = q^{p-2}\ ,$$

then N is a prime if and only if $G_s(S_{n-1}) \equiv 0 \pmod{N}$, where $S_0 \equiv W_A \pmod{N}$ and

$$S_{i+1} \equiv (-1)^s G_s(2 - S_i^2) \pmod{N} \quad (i = 0, 1, 2, \dots)\ .$$

Now it is possible to devise a Lucas-Lehmer test for the primality of $N = A\,p^n - 1$ (Algorithm 11.3.7 of [10]).

Algorithm 3.3. *Test for primality of $N = A\,p^n - 1$, where $A < p^n$, p an odd prime, $2 \mid A$. We assume we are given P, Q, q such that $(\Delta/N) = -1$ ($\Delta = P^2 - 4Q$), $N \nmid U_A$ and $(N/q)_p \neq 1$.*

1. *Put* $T_0 = W_A(P,Q)$ *and compute* $T_1, T_2, \ldots$ *by*
$$T_{i+1} \equiv (-1)^s T_i G_s(2 - T_i^2) \pmod{N}$$
until we find the least positive $m \le n$ *such that*
$$T_m \equiv 2 \pmod{N}\ .$$
If no such m *exists, then* N *is composite and the algorithm terminates. Put* $R = T_{m-1} \pmod{N}$. *If* $G_s(R) \not\equiv 0 \pmod{N}$, *then* N *is composite and the algorithm terminates. If* $(2p^m-1)^2 > N$, *then* N *is a prime and the algorithm terminates.*
2. *Put*
$$P' = \sum_{i=0}^{s-1} C(i,p,q)R^i\ , \quad Q' = q^{p-2}, \quad S_0 \equiv W_A(P',Q') \pmod{N}\ .$$
3. *Compute* S_{n-1} *by using*
$$S_{i+1} \equiv (-1)^s S_i G_s(2 - S_i^2) \pmod{N}\ .$$
4. N *is a prime if and only if* $N \mid G_s(S_{n-1})$.

Notice that there are actually two Lucas-Lehmer tests being performed by Algorithm 3.3. We conduct the first test (step 1), and if we are unsuccessful in determining whether N is composite or prime, we nevertheless obtain a piece of information, namely the value for R, which can be used in a second test (steps 2-4) which is guaranteed to resolve the issue of whether N is a prime. If we know values for P, Q, q, the complexity of Algorithm 3.3 is $O((p+\log q)\,q)+O(p^3)+O(n\log s) = O((p+\log q)q + p^3 + \log N)$ modular additions and multiplies modulo N. Also, as noted in [10, p.281], in practice we almost always prove N a prime by the first test. This is because the proportion of values of P for a fixed Δ such that
$$U_{(N+1)/p} \equiv 0 \pmod{N}$$
does not hold when N is prime is $1 - 1/p$.

The problem in using Algorithm 3.3 is the difficulty of producing for a given N values of P, Q, q *a priori* such that $N \nmid U_A(P,Q)$, $(\Delta/N) = -1$, and the prime q is such that $q \equiv 1 \pmod{p}$ and $(N/q)_p \ne 1$. For certain special values of N it is often possible to do this (see [8, 9]), but in general this seems to be a difficult problem. However, in the case of $A = p-1$, it is a rather simple matter to solve a part of this problem. Undoubtedly, this same approach could be valid for other special, small values of A.

We first note that since p is odd, we get $p \equiv \eta \pmod{4}$, where $|\eta| = 1$ and $N_n \equiv -\eta \pmod{4}$. If $P = 2$, $Q = 1 + \eta\,p$, then $\Delta = -4\,\eta\,p$ and $(\Delta/N_n) = (-\eta\,p/N_n) = -1$. In this case we have $U_1 = 1$, $U_2 = 2$, and we can use
$$|U_{n+1}| \le 2|U_n| + (1+p)|U_{n-1}|$$
to show by induction that
$$|U_n| < (2\sqrt{p})^{n-1} \quad (n \ge 1)\ .$$
It follows that $N_n > |U_n|$ when $n > (p-1)/2$, and therefore $N_n \nmid U_{p-1}$. It is a result going back to Lucas that if N_n is a prime, then $N_n \mid U_{N_n+1}$; hence, by (2.2) we find that
$$W_{(N_n+1)/2} \equiv \pm 2 \pmod{N_n}\ .$$

Also, if N_n is a prime, then by (2.3) we must have $G_s(W_m) \equiv 0 \pmod{N_n}$ for some $m = s\,p^k$ with $0 \le k \le n-1$, $s = (p-1)/2$. By making use of (2.5) we can now modify Algorithm 3.3 to produce an algorithm for testing N_n for primality.

Algorithm 3.4. *Test $N_n = (p-1)\,p^n - 1$ for primality. ($n > (p-1)/2$, p prime, $p \equiv \eta \pmod 4$, $|\eta| = 1$).*

1. *Put $s = (p-1)/2$, $T_0 \equiv W_s(2, 1+\eta p) \pmod{N_n}$ and compute $T_1, T_2, \ldots$ by*
$$T_{i+1} \equiv (-1)^s T_i G_s\left(2 - T_i^2\right) \pmod{N_n}$$
until we find the least positive value of h, $1 \le h \le n$, such that
$$T_h \equiv \pm 2 \pmod{N_n}\ .$$
If no such h exists, then N_n is composite and the algorithm terminates; otherwise, put $R \equiv T_{h-1} \pmod{N_n}$.
2. *Find a prime $q \equiv 1 \pmod p$ such that*
$$N_n^{(q-1)/p} \not\equiv 1 \pmod{q}\ . \tag{3.1}$$
If $q \mid N_n$, then N_n is composite and the algorithm terminates.
3. *Put*
$$P' \equiv \sum_{i=0}^{s-1} C(i,p,q) R^i\ ,\ Q' \equiv q^{p-2}\ ,\ S_0 \equiv W_{2s}(P', Q') \pmod{N_n}\ .$$
4. *Compute S_{n-1} by using*
$$S_{i+1} \equiv (-1)^s S_i G_s\left(2 - S_i^2\right) \pmod{N_n}\ .$$
5. *N_n is a prime if and only if*
$$N_n \mid G_s(S_{n-1})\ .$$

Notice that the only nondeterministic portion of this algorithm is step 2. Thus, *if we are given q* such that (3.1) holds, there is a Lucas-Lehmer type test for the primality of N_n that executes in at most $O((p + \log q)\,q + p^3 + \log N_n)$ modular multiplications (and additions) modulo N_n.

4. Nonresidue covering sets

In view of the remarks made at the end of the previous section, we need now to be able to guarantee that we can always find a small q such that (3.1) holds. By a result of [1], we know that under the extended Riemann Hypothesis such a value of q must exist with $q < 2\,(\log N_n)^2$. However, this still produces an algorithm of overall (conditional) complexity $O(p\,(\log N_n)^2)$. We will approach this problem in another way.

Let $\{I_n\}$ be any sequence of integers dependent for their value on that of the single parameter n, and let $\mathcal{C}$ be a set of j primes $\{q_1, q_2, \ldots, q_j\}$ such that $q_i \equiv 1 \pmod p$ $(i = 1, 2, \ldots, j)$, where p is some fixed prime. We say $\mathcal{C}$ is a *(pth power) nonresidue covering set* for $\{I_n\}$ if for any n there exists some $q \in \mathcal{C}$ such that
$$I_n^{(q-1)/p} \not\equiv 1 \pmod{q}\ .$$
(In this paper we will always assume that the value of p is specified, and we use the simpler expression *nonresidue covering set* or *nonresidue cover*.) For example, if $p = 11$ and $I_n = N_n$, then $N_n^2 \equiv 1 \pmod{23}$ only if $N_n \equiv 1 \pmod{23}$, i.e. $n \equiv 17$

(mod 22). This means that $n \equiv 17, 39, 61, 83 \pmod{88}$; but for these values of n we get

$$N_n^{(89-1)/11} = N_n^8 \not\equiv 1 \pmod{89}\ .$$

Thus, $\{23, 89\}$ is a nonresidue cover for $\{10 \cdot 11^n - 1\}$. Notice that this means that there is always a value for $q \le 89$ such that $N_n^{(q-1)/11} \not\equiv 1 \pmod{q}$ no matter how large n (or N_n) becomes, a much better result than $q < 2\,(\log N_n)^2$.

At first it might seem rather remarkable that these nonresidue covering sets exist, but actually, as we shall see, they appear to be very common. The reason for this can be explained by the following heuristic. If we let $q = 1 + kp$, where $2 \mid k$, and let g be a primitive root of q, then the pth power residues modulo q are all given by

$$1, r, r^2, \dots, r^{k-1}\ ,$$

where $r \equiv g^p \pmod{q}$. Notice that $r^{k/2} \equiv g^{(q-1)/2} \equiv -1 \pmod{q}$. If

$$N_n^{(q-1)/p} \equiv 1 \pmod{q}\ , \tag{4.1}$$

then

$$(p-1)\,p^n \in \left\{1 \pm r^j\ :\ j = 0, 1, 2, \dots, k/2-1\right\} \pmod{q};$$

hence,

$$\operatorname{ind}_g(p-1) + n \operatorname{ind}_g p \equiv \operatorname{ind}_g\left(1 \pm r^j\right) \pmod{q-1} \quad (j = 0, 1, 2, \dots, k/2-1)\ . \tag{4.2}$$

As there are at most $k-1$ values for n modulo $q-1$, there can only be at most $k-1$ values of n modulo p. For sufficiently many values of q we would expect that no values of n would survive such that (4.1) holds for all of them. Also, since the number of primes of the form $1 + kp$ less than or equal to x is asymptotic to $x/((p-1)\log x)$, many small ($< p^2$, say) q values should exist.

It must be emphasized, however, that although this reasoning is compelling, it is also naive. Consider, for example, the sequence $\{P_n\}$, where $P_n = A\,p^n + \eta$, $|\eta| = 1$, $A = \eta(x^p - p^{p\,k})$, $|x| = 1$. There can never exist a nonresidue cover for $\{P_n\}$. For suppose $\mathcal{C}$ is such a cover; let $q \in \mathcal{C}$ and let $\omega(q)$ be the multiplicative order of p modulo q. Select n such that $p \mid n$ and $n \equiv -p\,k \pmod{\omega(q)}$ for all $q \in \mathcal{C}$. This can be done simply by solving $n \equiv -p\,k \pmod{h}$, where h is the least common multiple of p and all the $\omega(q)$ values. Now

$$P_n = \eta\left(\pm p^n - p^{n+kp} + 1\right) \equiv \pm\eta p^n \pmod{q}$$

for each $q \in \mathcal{C}$. Hence

$$P_n^{(q-1)/p} \equiv (\pm\eta p)^{n(q-1)/p} \equiv 1 \pmod{q}$$

for each $q \in \mathcal{C}$, contradicting the definition of $\mathcal{C}$. This sort of observation was first made by Bosma [2] in connection with the sequences $\{(4^k - 1)2^n \pm 1\}$. Notice that if we put $p = 3$, $\eta = -1$, $k = 0$, $x = -1$, we get $A = 2$; hence, there cannot exist a nonresidue cover for $\{2 \cdot 3^n - 1\}$. However for any other value of p, it is easy to show that we can never represent $p - 1$ in the form given for A above.

5. Numerical procedures and results

In an attempt to verify numerically that the heuristic mentioned earlier would often lead to a nonresidue cover for $\{N_n\}$ whenever $p > 3$, a computer program was written to employ this heuristic and tested on all primes p such that $3 < p < 30000$. The computer succeeded in producing a cover for each such prime; the largest value of q required was $q = 9315571$ for $p = 28229$ ($k = 330$). Of much greater interest, however, was the cardinality of the covers the computer produced: for the 3243 primes tested, 681 of the covers contained only a single prime; the remaining 2562 primes required only 2 primes in the cover. That is, the computer never needed more than 2 primes to produce a nonresidue cover. To explain why this phenomenon occurred, we first note that if, as before, $\omega = \omega(q)$, the multiplicative order of p modulo q, we have

$$\omega = (q-1)/d \ ,$$

where $d = \gcd(q-1, \operatorname{ind}_g p)$. It follows from (4.2) that if (4.1) holds, then

$$\operatorname{ind}_g(p-1) \equiv \operatorname{ind}_g\left(1 \pm r^j\right) \pmod{d} \quad (j = 0, 1, 2, \ldots, k/2-1) \ . \tag{5.1}$$

Set $a = \operatorname{ind}_g(p-1)$. If j is a solution of (5.1), then by (4.2) we must have

$$n \operatorname{ind}_g p \equiv \operatorname{ind}_g\left(1 \pm r^j\right) - a \pmod{q-1}$$

and

$$n(\operatorname{ind}_g p)/d \equiv \left(\operatorname{ind}_g\left(1 \pm r^j\right) - a\right)/d \pmod{\omega} \ .$$

Since $\gcd(\omega, (\operatorname{ind}_g p)/d) = 1$, there is one and only one solution for n modulo ω for each solution j of (5.1).

One expects that the number of values of j for which (5.1) holds would be bounded above by the total number of possibilities for j (in this case $k-1$) divided by the modulus, i.e. $(1 - 1/k)\,\omega/p$. Thus, the expected number of values of n modulo ω for which (4.1) holds is $(1 - 1/k)\,\omega/p$. Indeed, in those cases where $\#\mathcal{C} = 1$, we found that $q \mid p^p - 1$ or $q \mid p^p + 1$ ($\omega = p$ or $2p$). We noticed that in almost all the cases where the computer produced $\mathcal{C}$ with $\#\mathcal{C} = 2$, the condition $\omega_1 \mid \omega_2$ held, where $\omega_i = \omega(q_i)$ $(i = 1, 2)$ and $\mathcal{C} = \{q_1, q_2\}$. Now, since the expected number of values of $n \pmod{\omega}$ such that (4.1) holds is $(1 - 1/k)\,\omega/p$, we would expect to have $(1 - 1/k_1)(1 - 1/k_2)\,\omega_1\omega_2/p^2$ ($k_i = (q_i - 1)/p; i = 1, 2$) pairs (s_1, s_2) with s_i randomly selected between 1 and ω_i $(i = 1, 2)$ such that (4.1) would hold for $n \equiv s_i \pmod{\omega_i}$. If, however, (4.1) must hold for *both* q_1 and q_2, and $\omega_1 \mid \omega_2$, then $n \equiv s_1 \equiv s_2 \pmod{\omega_1}$. We would expect this to happen only for $1/\omega_1$ of all the pairs (s_1, s_2). Thus, we would only expect

$$(1 - 1/k_1)(1 - 1/k_2)\,\omega_2/p^2 \le (1 - 1/k_1)(1 - 1/k_2)k_2/p$$

values of n modulo ω_1 for which (4.1) would hold for both q_1 and q_2. Since k_2 is usually much smaller than p, this means that we would not expect (4.1) to hold for q_1 and q_2, and this is exactly what the computer results revealed.

We made use of the above observations to produce a much faster computer program to search for $\mathcal{C}$.

Procedure 5.1. *Given p, find a nonresidue cover $\mathcal{C}$ for $\{N_n\}$.*

1. *Find two primes* q_1, q_2 *such that* $q_1 \equiv q_2 \equiv 1 \pmod{p}$ *and primitive roots* g_1 *of* q_1 *and* g_2 *of* q_2. *Compute* $\operatorname{ind}_{g_1} p$, $\operatorname{ind}_{g_2} p$ *for the moduli* q_1, q_2 *respectively by using the baby-step giant-step method of Shanks.*
2. *Compute* $d_i = \gcd(\operatorname{ind}_{g_i} p, q_i - 1)$ *and* $\omega_i = (q_i - 1)/d_i$, $i = 1, 2$.
3. *If* $\omega_1 \nmid \omega_2$, *go to* 1.
4. *For each* $q \in \{q_1, q_2\}$ *compute*
$$b_j \equiv \left(\left(1 \pm r^j\right)(p-1)^{-1}\right)^{\omega} \pmod{q},$$
where $r \equiv g^p \pmod{q}$, $j = 0, 1, 2, \ldots, k/2 - 1$, $k = (q-1)/p$.
Retain those values of j *such that* $b_j \equiv 1 \pmod{q}$;
if there is no value of j *for which this holds,*
then put $\mathcal{C} = \{q\}$ *and terminate the procedure.*
5. *For each* q *and its retained values of* j *compute*
$$n \equiv (\operatorname{ind}_g p/d)^{-1}\left(\operatorname{ind}_g\left(1 \pm r^j\right) - a\right)/d \pmod{\omega},$$
where $a = \operatorname{ind}_g(p-1)$.
6. *If the set of* n *values for* q_1 *and the set of* n *values for* q_2 *modulo* ω_1 *have a nil intersection, put* $\mathcal{C} = \{q_1, q_2\}$ *and terminate the procedure; otherwise, return to* 1.

Notice that the condition that $b_j \equiv 1 \pmod{q}$ is equivalent to the condition (5.1), but permits us to avoid the expensive computation of the indices $\operatorname{ind}_g(1 \pm r^j)$, $j = 1, 2, \ldots, k/2 - 1$.

To determine the effectiveness of this (nondeterministic) procedure we implemented it on a computer and ran it on all primes p with $3 < p < 10^7$. For each value of p, the computer was successful in producing a nonresidue cover. The largest q ever needed was $q = 8861411701$ for $p = 9846013$ ($k = 900$). For the total of 664577 primes examined, a single prime cover was found 109677 times and a double prime cover was produced for the remaining 554900. Also, the maximum value of k needed for any cover was always such that $k < 5(\log p)^2$, and when $p > 10^4$, this $k < 4(\log p)^2$. While we have no proof of this, the data and the heuristics strongly suggest that for any prime $p > 3$ we should always be able to find a nonresidue cover $\mathcal{C}$ for N_n with $\#\mathcal{C} \le 2$.

6. Covers containing a single prime

Almost 1/5 of all the covers $\mathcal{C}$ found by our procedure were such that $\#\mathcal{C} = 1$. In this section we will show how in several instances one can find such a cover without conducting a search. First, however, it is useful to mention that it is often possible to find a single prime nonresidue cover, even when a two prime cover has been found first. For example, the computer found the cover $\{29, 113\}$ for $p = 7$, but note that $\{911\}$ is also a cover for $p = 7$. Note further that $911 \mid 7^7 + 1$. In Table 6.1 below we give the results of a search for single prime covers for $p < 100$. This search was conducted for all $k = (q-1)/p < 10^6$ except in the case of $p = 23$, where we also tried factors of $23^{23} \pm 1$. Here, $k_1 = (q_1 - 1)/p$, $k_2 = (q_2 - 1)/p$, for $\mathcal{C} = \{q_1, q_2\}$ and $k = (q-1)/p$ for $\mathcal{C} = \{q\}$.

Of course the difficulty with some of these single prime covers is that the value of q is very large, something that for the primality testing Algorithm 3.4 is not desirable. If we examine small values of $k = (q-1)/p$ for which Procedure 5.1 produced single prime nonresidue covers $\{q\}$, we get Table 6.2.

TABLE 6.1.

p	k_1, k_2	k	p	k_1, k_2	k
5		2	47	6, 14	
7	4, 16	130	53		2
11	2, 6	1436	59	12, 18	
13		4	61	6, 12	16
17	6, 8	644	67		4
19	12, 24	55222	71	8, 12	1488
23	2, 6	66175184	73	4, 6	772294
29		2	79	4, 28	442
31	10, 12		83	2, 6	32
37		4	89		2
41		2	97	4, 10	
43		4			

TABLE 6.2.

k	number of covers	k	number of covers
2	27940	12	6215
4	17931	14	1658
6	4714	16	10015
8	7523	18	2486
10	3085		

Indeed, we noticed that all the single element covers of the form $\{2p+1\}$ ($k = 2$) were such that $p \equiv 5 \pmod{12}$, for example $p = 5$, 29, 41, 53, 89, 113, 173, 233, etc.

Theorem 6.1. *If $q = 2p + 1$ is a prime and $p \equiv 5 \pmod{12}$, then $\{q\}$ is a nonresidue cover for $\{N_n\}$, where $N_n = (p-1)\,p^n - 1$.*

Proof. Suppose $N_n^{(q-1)/p} \equiv 1 \pmod{q}$; then $(p-1)\,p^n - 1 \equiv \pm 1 \pmod{q}$, which means that $2\,(p-1)\,p^n \equiv 4 \pmod{q}$. But $(p/q) = (q/p) = (1/p) = 1$ and $((2p-2)/q) = ((q-3)/q) = (-3/q) = -1$, the latter result holding because $q \equiv -1 \pmod{3}$. It follows that $(2(p-1)\,p^n/q) = -1 \neq (4/q) = 1$, a contradiction. □

All the single element nonresidue covers of the forms $\{4p + 1\}$ and $\{6p + 1\}$ respectively satisfied the conditions of the much more complicated Theorems 6.2 and 6.3.

Theorem 6.2. *Let $q = 4p + 1$ be a prime and $q = A^2 + B^2$, where $A \equiv -1 \pmod{4}$, $2 \mid B$ and the sign of B is selected such that $((A + B)/q) = 1$. $\mathcal{C} = \{q\}$ is a nonresidue cover for $\{N_n\}$ if either* (i) *or* (ii) *holds.*

(i) $p \equiv 2 \pmod{5}$ *and*

$$A - B \not\equiv 5 \pmod{16} \quad , 5 \mid B \ ,$$

or

$$A - B \not\equiv 13 \pmod{16} \ , 5 \mid A \ .$$

(ii) $p \equiv 3,4 \pmod 5$ *and*

$$B \not\equiv 2 \pmod 8\ ,\ A+B \not\equiv 9 \pmod{16}\ ,\ A \not\equiv B \pmod 5\ ,$$

or

$$B \not\equiv 6 \pmod 8\ ,\ A+B \not\equiv 1 \pmod{16}\ ,\ A \equiv B \pmod 5\ .$$

Small examples of such values of p satisfying the conditions of Theorem 6.2 are $p = 13,\ 37,\ 43,\ 43,\ 67,\ 127,\ 193,\ 199$.

Theorem 6.3. *Let* $p \equiv 1 \pmod 4$, $q = 6p+1$, $4q = L^2 + 27M^2$, *where* $L \equiv 1 \pmod 3$ *and the sign of* M *is determined by* $\left(\left(L^2 - 3ML\right)/q\right) = 1$. $\mathcal{C} = \{q\}$ *is a nonresidue cover for* $\{N_n\}$ *when* $p \equiv 2,3,5 \pmod 7$ *if either (i) or (ii) holds.*

(i) $p \equiv -1 \pmod 3$ *and*

$$6 \mid M\ ,\ L \equiv 5M \pmod 7\ ,$$

or

$$M \equiv 1 \pmod 6\ ,\ L \equiv M \pmod 4\ ,\ 7 \mid LM\ ,$$

or

$$M \equiv -1 \pmod 6\ ,\ L \equiv -M \pmod 4\ ,\ L \equiv 2M \pmod 7\ .$$

(ii) $p \equiv 1 \pmod 3$ *and*

$$6 \mid M\ ,\ L \equiv 2M \pmod 7\ ,$$

or

$$M \equiv 1 \pmod 6\ ,\ L \equiv M \pmod 4\ ,\ L \equiv 5M \pmod 7\ ,$$

or

$$M \equiv -1 \pmod 6\ ,\ L \equiv -M \pmod 4\ ,\ 7 \mid LM\ .$$

When $p \equiv 4,6 \pmod 7$, $\mathcal{C}$ *is a nonresidue cover for* $\{N_n\}$ *if*

$$6 \mid M\ ,\ 7 \mid LM\ ,$$

or

$$p \equiv 1 \pmod 3\ ,\ M \equiv 1 \pmod 6\ ,\ L \equiv M \pmod 4\ ,\ 7 \mid LM\ ,$$

or

$$p \equiv -1 \pmod 3\ ,\ M \equiv -1 \pmod 6\ ,\ L \equiv -M \pmod 4\ ,\ 7 \mid LM\ .$$

Small examples of values of p satisfying this theorem are $p = 181,\ 241,\ 1193,\ 2357,\ 2861,\ 2897,\ 3181,\ 3433$.

The proofs of Theorem 6.2 and 6.3 can be derived by making use of well known 4th and 3rd power residuacity results involving prime numbers in $\mathbb{Z}[\zeta_4]$ and $\mathbb{Z}[\zeta_3]$ respectively. Here ζ_4 and ζ_3 denote primitive fourth and cube roots of unity in $\mathbb{C}$, i.e. $\zeta_4^2 + 1 = 0$, $\zeta_3^2 + \zeta_3 + 1 = 0$. We illustrate the proof technique by proving (i) of Theorem 6.3.

Proof of (i) *of Theorem 6.3.* Since $q = 6p + 1$ is a prime, we must be able to represent $4q$ by $4q = L^2 + 27M^2$ with $L \equiv 1 \pmod 3$. Furthermore, since $p \equiv -1 \pmod 3$, we must have $L \equiv 4 \pmod q$. If $t^2 + t + 1 \equiv 0 \pmod q$, then

$$((p-1)\,p^n - 1)^{(q-1)/p} \equiv 1 \pmod q \tag{6.1}$$

means that

$$(p-1)\,p^n \in \left\{2, 1+t, 1+t^2, 1-t, 1-t^2\right\} \pmod q\ .$$

Hence,

$$\left(\frac{p-1}{q}\right)\left(\frac{p}{q}\right)^n \in \left\{\left(\frac{2}{q}\right), \left(\frac{1+t}{q}\right), \left(\frac{1+t^2}{q}\right), \left(\frac{1-t}{q}\right), \left(\frac{1-t^2}{q}\right)\right\}\ .$$

Now $(p/q) = (q/p) = 1$, $((p-1)/q) = (-42/q) = (-6/q)(7/q) = (7/q) = -(q/7) = 1$. Also,

$$\begin{aligned}((1+t)/q) &= \left(-t^2/q\right) = -1\ ,\\ \left((1+t^2)/q\right) &= \left(-t^4/q\right) = -1\ ,\\ \left((1-t)(1-t^2)/q\right) &= \left(-(1-t)^2t^2/q\right) = -1\ .\end{aligned}$$

Thus, one of $((1-t)/q)$ or $\left((1-t^2)/q\right)$ is equal to -1.

Putting $t \equiv L(6M)^{-1} - 2^{-1} \pmod q$, we see that $t^2 + t + 1 \equiv 0 \pmod q$ and

$$\begin{aligned}((1-t)/q) &= \left((3\cdot 2^{-1} - L(6M)^{-1})/q\right) = -\left((-LM + 9M^2)/q\right)\\ &= (3/q)\left((-LM + 9M^2)/q\right) = \left((-L^2 - 3LM)/q\right)\\ &= -\left((L^2 + 3ML)/q\right) = \left((L^2 - 3ML)/q\right)\ .\end{aligned}$$

Hence, we can only have

$$(p-1)\,p^n \in \{2, 1-t\} \pmod q \tag{6.2}$$

if (6.1) holds.

Let ρ be any primary prime factor of q in $\mathbb{Z}[\zeta_3]$. We have $q = \rho\overline{\rho}$, where $\rho = 3\,a - 1 + 3\,b\,\zeta_3$ $(a, b \in \mathbb{Z})$ and we may assume that $\zeta_3 \equiv t \pmod\rho$. We get $\rho = (L - 3M)/2 - 3M\zeta_3$, which means that $b = -M$, $a = (L - 3M + 2)/6$. If we use the symbol $[\alpha/\beta]$ to denote the value of $\zeta_3^i \equiv \alpha^{(\beta\overline{\beta}-1)/3} \pmod\beta$ for a prime β in $\mathbb{Z}[\zeta_3]$, then it is well known that

$$[(1-t)/\rho] = [(1-\zeta_3)/\rho] = \zeta_3^{2a} = \zeta_3^{2M-1}\ . \tag{6.3}$$

Also, $3 \equiv (1-t)(1-t^2) \pmod q$; hence, $[3/\rho] = [(1-t)^2t^2/\rho] = \zeta_3^{a+2\,(q-1)/3}$ and

$$[3/\rho] = \zeta_3^M\ .$$

Now $[2/\rho] = [\rho/2] \equiv \rho \pmod 2$; hence,

$$\left[\frac{2}{\rho}\right] = \begin{cases}1, & 2 \mid M\ ,\\ \zeta_3, & 2 \nmid M,\ L \equiv -M \pmod 4\ ,\\ \zeta_3^2, & 2 \nmid M,\ L \equiv M \pmod 4\ .\end{cases} \tag{6.4}$$

It follows that $[6/\rho] = 1$ under any one of the following conditions:

1. $6 \mid M$,
2. $M \equiv 1 \pmod 6$, $L \equiv M \pmod 4$,
3. $M \equiv -1 \pmod 6$, $L \equiv -M \pmod 4$.

Since $6\rho \equiv -1 \pmod{q}$, we see that under any of these three conditions we must have $[p/\rho] = 1$ and

$$\left[\frac{p-1}{\rho}\right] = \left[\frac{2}{\rho}\right] \quad \text{or} \quad \left[\frac{1-t}{\rho}\right] \tag{6.5}$$

if (6.2) is to hold.

Now $6(p-1) \equiv -7 \pmod{q}$; thus, under any one of conditions 1, 2, or 3,

$$\left[\frac{p-1}{\rho}\right] = \left[\frac{7}{\rho}\right] = \left[\frac{\pi_1}{\rho}\right]\left[\frac{\pi_2}{\rho}\right] = \left[\frac{\rho}{\pi_1}\right]\left[\frac{\rho}{\pi_2}\right] ,$$

where $\pi_1 = -1 - 3\zeta_3$, $\pi_2 = -1 - 3\zeta_3^2$. Since $3\zeta_3 \equiv -1 \pmod{\pi_1}$ and $3\zeta_3 \equiv -2 \pmod{\pi_2}$, it is easy to see that

$$[\rho/\pi_1] \equiv (L-M)^2/4 \pmod{\pi_1}, \quad [\rho/\pi_2] \equiv (L+M)^2/4 \pmod{\pi_2} .$$

Also, $(L+M)^2/4$, $(L-M)^2/4 \in \{1,2,4\} \pmod 7$. and $\zeta_3 \equiv 2 \pmod{\pi_1}$, $\zeta_3^2 \equiv 4 \pmod{\pi_1}$, $\zeta_3 \equiv 4 \pmod{\pi_2}$, $\zeta_3^2 \equiv 2 \pmod{\pi_2}$. It follows that if $(L-M)^2 \equiv (L+M)^2 \pmod 7$ or, equivalently, $7 \mid LM$, then $[\rho/\pi_1][\rho/\pi_2] = 1$ and $[7/\rho] = 1$. Similarly, if $L \equiv 3M, 5M \pmod 7$ ($(L-M)^2 \equiv 2\,(L+M)^2 \pmod 7$), then $[7/\rho] = \zeta_3$, and if $L \equiv 2M, 4M \pmod 7$, then $[7/\rho] = \zeta_3^2$. Since $4q \equiv L^2 + 27M^2 \pmod 7$, we can never have $L \equiv 3M, 4M \pmod 7$ because under condition (i) $(4q/7)$ must be -1. By combining these results with (6.3) and (6.4), we see that under any of the conditions in (i) we can never have (6.5), and therefore (6.1) cannot hold. □

In spite of results like the above theorems, it seems still to be rather difficult to show that there exists an infinitude of primes p such that $\{(p-1)\,p^n-1\}$ will have a nonresidue cover.

References

[1] E. Bach. Explicit bounds for primality testing and related problems. *Mathematics of Computation*, 55:355–380, 1990. MR **91m:**11096

[2] W. Bosma. Explicit primality criteria for $h \cdot 2^k \pm 1$. *Mathematics of Computation*, 61:97–109, 1993. MR **94c:**11005

[3] D. H. Lehmer. An extended theory of Lucas' functions. *Annals of Mathematics*, 31:419–448, 1930.

[4] E. Lucas. Nouveaux théoremes d'arithmétique supérieure. *Comptes Rendus Acad. des Sciences, Paris*, 83:1286–1288, 1876.

[5] H. C. Williams. An algorithm for determining certain large primes. Proc. Second Louisiana Conf. Combinatorics, Graph Theory and Computing, Louisiana State Univ., Baton Rouge, LA, 1971, pp. 533–556. MR **47:**8415

[6] H. C. Williams. The primality of $2A3^n - 1$. *Canadian Math. Bull.*, 15:585–589, 1972. MR **47:**121

[7] H. C. Williams. The primality of certain integers of the form $2Ar^n - 1$. *Acta Arith.*, 39:7–17, 1981. MR **84h:**10012

[8] H. C. Williams. A class of primality tests for trinomials which includes the Lucas-Lehmer test. *Pacific J. Math.*, 98:477–494, 1982. MR **83f:**10008

[9] H. C. Williams. Effective primality tests for some integers of the form $A5^n - 1$ and $A7^n - 1$. *Mathematics of Computation*, 48:385–403, 1987. MR **88b:**11089

[10] H. C. Williams. *Édouard Lucas and Primality Testing*, volume 22 of *Canadian Mathematical Society Series of Monographs and Advanced Texts*. Wiley, NY, 1998. CMP 98:15

University of Waterloo, Department of Combinatorics and Optimization, Waterloo, Ontario, Canada N2L 3G1
E-mail address: astein@cacr.math.uwaterloo.ca

University of Manitoba, Department of Computer Science, Winnipeg, Manitoba, Canada R3T 2N2
E-mail address: williams@cs.umanitoba.ca