MATHEMATICS OF COMPUTATION
Volume 73, Number 247, Pages 1559–1564
S 0025-5718(03)01575-8
Article electronically published on July 1, 2003

BIQUADRATIC RECIPROCITY AND A LUCASIAN PRIMALITY TEST

PEDRO BERRIZBEITIA AND T. G. BERRY

ABSTRACT. Let $\{s_k, k \geq 0\}$ be the sequence defined from a given initial value, *the seed*, s_0, by the recurrence $s_{k+1} = s_k^2 - 2, k \geq 0$. Then, for a suitable seed s_0, the number $M_{h,n} = h \cdot 2^n - 1$ (where $h < 2^n$ is odd) is prime iff $s_{n-2} \equiv 0 \bmod M_{h,n}$. In general s_0 depends both on h and on n. We describe a slight modification of this test which determines primality of numbers $h \cdot 2^n \pm 1$ with a seed which depends only on h, provided $h \not\equiv 0 \bmod 5$. In particular, when $h = 4^m - 1$, m odd, we have a test with a single seed depending only on h, in contrast with the unmodified test, which, as proved by W. Bosma in *Explicit primality criteria for* $h \cdot 2^k \pm 1$, Math. Comp. **61** (1993), 97–109, needs infinitely many seeds. The proof of validity uses biquadratic reciprocity.

The Lucasian sequence with seed s_0 is the sequence $\{s_k\}$ defined from the given initial value s_0 by the recurrence $s_{k+1} = s_k^2 - 2$, $k \geq 0$. A *Lucasian primality test* is a primality test involving a Lucasian sequence. The terminology comes from the Lucas-Lehmer test for Mersenne primes (see [4] for historical details):

Theorem 1 (Lucas-Lehmer)**.** *Let p be an odd prime, and let $M_p = 2^p - 1$ be the corresponding Mersenne number. Let $\{s_k\}$ be the Lucasian sequence with seed 4. Then M_p is prime iff $s_{p-2} \equiv 0 \bmod M_p$.*

Let $n, h \in \mathbb{N}$ with h odd, $h < 2^n$, and let $M_{n,h} = h \cdot 2^n - 1$. The Lucas-Lehmer test generalizes to a Lucasian primality test for $M = M_{h,n}$ as follows:

Theorem 2. *Suppose $n \geq 2$. Let $d \in \mathbb{Z}$ satisfy $\left(\frac{d}{M}\right) = -1$, where $\left(\frac{\cdot}{M}\right)$ is the Jacobi symbol. Let $K = \mathbb{Q}(\sqrt{d})$, and let $\mathcal{O}_K$ be the ring of integers of K. Let $\alpha \in \mathcal{O}_K$ satisfy $\left(\frac{\alpha\overline{\alpha}}{M}\right) = -1$, where $\overline{\alpha}$ denotes the conjugate of α in K. Then the following are equivalent:*

(1) *M is prime.*
(2) $(\alpha/\overline{\alpha})^{(M+1)/2} \equiv -1 \bmod M$.
(3) *$s_{n-2} \equiv 0 \bmod M$, where s_k is the Lucasian sequence with seed $s_0 = (\alpha/\overline{\alpha})^h + (\overline{\alpha}/\alpha)^h = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha/\overline{\alpha})^h$.*

For a proof see [3]. The Lucas-Lehmer test is the special case $d = 3$, $\alpha = -1 + \sqrt{3}$ of this theorem. For then $\mathrm{Tr}_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}}(\alpha) = -4$ whence (the sign being clearly irrelevant) $s_0 = 4$. The generalization differs from the original Lucas-Lehmer test in two respects. First, in the generalized test the seed is a rational number, which may not be an integer; this is not a serious difficulty, since, by inverting the denominator $\bmod M$, one can replace the rational seed by an integer seed. Second,

Received by the editor May 3, 2002 and, in revised form, January 10, 2003.
2000 *Mathematics Subject Classification.* Primary 11A51, 11Y11.

in the generalized test, the seed s_0 depends on n as well as h, while in the Lucas-Lehmer test the seed 4 works for all odd p. It is usually easy to find a seed by trial and error. However, following the analogy with Mersenne numbers, our philosophy is to fix h and search for primes in the family $M_{h,n}$ with n increasing. Thus it is certainly desirable to have a seed independent of n, if possible. We will have a seed independent of n if we can solve the following problem:

For given h, find $d \in \mathbb{Z}$, $\alpha \in \mathcal{O}_K$ where $K = \mathbb{Q}(\sqrt{d})$, such that

$$\forall n\,, \left(\tfrac{d}{M_{h,n}}\right) \neq 1; \left(\tfrac{\alpha\overline{\alpha}}{M_{h,n}}\right) \neq 1.$$

All the above considerations apply also, mutatis mutandis, to numbers of the form $M^+_{h,n} = h \cdot 2^n + 1$, when the primality test in question is Proth's generalization of Pépin's test for Fermat numbers: let $M^+ = M^+_{h,n}$, and let d be an integer such that $\left(\frac{d}{M^+}\right) = -1$. Then M^+ is prime iff $d^{(M^+-1)/2} \equiv -1 \bmod M^+$. The problem in this case is to find d, depending only on h, such that $\forall n$, $\left(\frac{d}{M^+_{h,n}}\right) \neq 1$.

If $n \geq 3$, $h \not\equiv 0 \bmod 3$, then it is easy to see that, for the generalized Mersenne numbers $M_{h,n}$, as for Mersenne numbers, $d = 3$, $\alpha = -1 + \sqrt{3}$ solves the problem; for the $M^+_{h,n}$ the corresponding problem is solved by $d = 3$. The case $h \equiv 0 \bmod 3$ is studied in [1] and [3]. In [3] tables of seeds are given for $M_{h,n}$. In [1] for each $h \equiv 0 \bmod 3$, $h < 10^5$, but h not of the form $4^m - 1$, Bosma exhibits a finite set of pairs (d_k, α_k), $d_k \in \mathbb{Z}, \alpha_k \in \mathbb{Q}(\sqrt{d_k})$, such that, for any n, one of the pairs solves the problem for $M_{h,n}$. On the other hand, for h of the form $4^m - 1$ he proves there is no such finite set of pairs. Similar results are obtained for the $M^+_{h,n}$.

We shall show that, despite Bosma's results, a small modification of the algorithm of Theorem 2 allows us, for fixed $h \not\equiv 0 \bmod 5$, to test primality of $M_{h,n}$ and $M^+_{h,n}$ by means of a Lucasian sequence with a seed independent of n. In particular when $h = 4^m - 1$, m odd, we have a single seed.

For any odd integer k we set $k^* = \left(\frac{-1}{k}\right)k$. This notation allows us to treat the cases $h \cdot 2^n \pm 1$ simultaneously. Note that, if $M = h \cdot 2^n \pm 1$, then $M^* = (\pm h)2^n + 1$. We shall prove:

Theorem 3. *Let $M = M_{h,n} = h \cdot 2^n \pm 1$, where $h < 2^{n-2} - 1$ is odd, $h \not\equiv 0 \bmod 5$, and $n \geq 3$. Let $\alpha = -1 + 2i \in \mathbb{Z}[i]$ and let $\{s_k\}$ be the Lucasian sequence with seed $s_0 = (\alpha/\overline{\alpha})^h + (\overline{\alpha}/\alpha)^h$. Then M is prime iff*

- *either $M^* \equiv \pm 2 \bmod 5$ and $s_{n-2} \equiv 0 \bmod M$*
- *or $M^* \equiv -1 \bmod 5$ and $s_{n-3} \equiv 0 \bmod M$.*

The proof of the theorem uses the biquadratic power residue symbol, whose properties we summarize in the following section. Details can be found in [2], Chapter 9.

Biquadratic reciprocity. Let $K = \mathbb{Q}[i]$, and let $R = \mathbb{Z}[i]$ be the ring of integers. Recall that a rational prime q splits in R iff $q \equiv 1 \bmod 4$. Let $\mathfrak{p}$ be a prime ideal of R lying over an odd rational prime, and let $\beta \in R$. The biquadratic residue symbol $\left(\dfrac{\beta}{\mathfrak{p}}\right)_4$ is defined by:

(1) If $\beta \in \mathfrak{p}$, then $\left(\dfrac{\beta}{\mathfrak{p}}\right)_4 = 0$.

(2) If $\beta \notin \mathfrak{p}$, then $\left(\frac{\beta}{\mathfrak{p}}\right)_4 = \omega$, where ω is the unique fourth root of 1 in K such that

$$\beta^{\frac{\mathrm{Nm}\,\mathfrak{p}-1}{4}} \equiv \omega \bmod \mathfrak{p},$$

where $\mathrm{Nm}\,\mathfrak{p}$ is the norm of the ideal $\mathfrak{p}$.

(3) If $J \in R$ is an arbitrary ideal and $J = \prod \mathfrak{p}_i^{n_i}$ is its factorization as a product of prime ideals, then

$$\left(\frac{\beta}{J}\right)_4 = \prod \left(\frac{\beta}{\mathfrak{p}_i}\right)_4^{n_i}.$$

Since R is a principal ideal domain, $\mathfrak{p} = (\pi)$ for some irreducible $\pi \in R$, and we normally write $\left(\frac{\beta}{\pi}\right)_4$ instead of $\left(\frac{\beta}{\mathfrak{p}}\right)_4$. By its very definition the symbol when written in this form depends only on the ideal generated by π.

We note the following properties:

$$\left(\frac{\beta\gamma}{\pi}\right)_4 = \left(\frac{\beta}{\pi}\right)_4 \left(\frac{\gamma}{\pi}\right)_4, \tag{1}$$

$$\left(\frac{\beta}{\pi\eta}\right)_4 = \left(\frac{\beta}{\pi}\right)_4 \left(\frac{\beta}{\eta}\right)_4, \tag{2}$$

$$\overline{\left(\frac{\beta}{\pi}\right)_4} = \left(\frac{\overline{\beta}}{\overline{\pi}}\right)_4, \tag{3}$$

$$\left(\frac{\beta/\gamma}{\pi}\right)_4 = \left(\frac{\beta}{\pi}\right)_4 \left(\frac{\gamma}{\pi}\right)_4^{-1}. \tag{4}$$

We do not need biquadratic reciprocity in full generality, but rather the following proposition (from which the general law can in fact be deduced). An element $\pi \in R$ is *primary* if $\pi \equiv 1 \bmod (1+i)^3$.

Proposition 4. *Let q be an odd rational prime and let $\pi \in R$, $\pi \notin \mathbb{Z}$, be irreducible and primary. Then*

$$\left(\frac{q^*}{\pi}\right)_4 = \left(\frac{\pi}{q}\right)_4.$$

For a proof, see Propositions 9.9.6 and 9.9.7 of [2]. We use this result in the following form.

Corollary 5. *With the hypotheses of Proposition 4*

$$\left(\frac{q^*}{\pi}\right)_4 \equiv (\pi/\overline{\pi})^{\frac{q^*-1}{4}} \bmod q.$$

Proof. Suppose $q \equiv 3 \bmod 4$ so that $q^* = -q$ and q is irreducible in R. Then

$$\begin{aligned}
\left(\frac{q^*}{\pi}\right)_4 &= \left(\frac{\pi}{q}\right)_4 \text{ (Proposition 4)},\\
\left(\frac{\pi}{q}\right)_4 &\equiv \pi^{\frac{q^2-1}{4}} \bmod q \text{ (definition of the biquadratic symbol, and using } \operatorname{Nm} q = q^2)\\
&\equiv \left(\pi^{q-1}\right)^{\frac{q+1}{4}} \bmod q\\
&\equiv (\overline{\pi}/\pi)^{\frac{q+1}{4}} \bmod q \text{ (since } \pi^q \equiv \overline{\pi} \bmod q, \text{ as is easily seen)}\\
&\equiv (\pi/\overline{\pi})^{\frac{q^*-1}{4}} \bmod q \text{ (since } q^* = -q).
\end{aligned}$$

Suppose now $q \equiv 1 \bmod 4$. Then $q^* = q$ and q splits in R, say $q = \lambda\overline{\lambda}$. We have

$$\begin{aligned}
\left(\frac{q^*}{\pi}\right)_4 &= \left(\frac{\pi}{q}\right)_4 \text{ (Proposition 4)},\\
\left(\frac{\pi}{q}\right)_4 &= \left(\frac{\pi}{\lambda\overline{\lambda}}\right)_4\\
&= \left(\frac{\pi}{\lambda}\right)_4 \left(\frac{\pi}{\overline{\lambda}}\right)_4\\
&= \left(\frac{\pi}{\lambda}\right)_4 \overline{\left(\frac{\overline{\pi}}{\lambda}\right)_4}\\
&= \left(\frac{\pi}{\lambda}\right)_4 \left(\frac{\overline{\pi}}{\lambda}\right)_4^{-1}\\
&= \left(\frac{\pi/\overline{\pi}}{\lambda}\right)_4\\
&\equiv (\pi/\overline{\pi})^{\frac{q-1}{4}} \bmod q \text{ since } \operatorname{Nm}(\lambda) = q
\end{aligned}$$

which is the desired result, since $q^* = q$. □

Proof of Theorem 3. The underlying reason for the appearance of Lucasian sequences is the following easily verified proposition. □

Proposition 6. *Let τ be an element of norm 1 in a quadratic extension K of $\mathbb{Q}$ and let s_k be the Lucasian sequence with seed $\operatorname{Tr}_{K/\mathbb{Q}}(\tau)$. Then $s_k = \operatorname{Tr}_{K/\mathbb{Q}}(\tau^{2^k})$.*

We shall also need the following for the proof of sufficiency of Theorem 3.

Lemma 7. *Let K be a quadratic extension of $\mathbb{Q}$, let q be an odd rational prime and let $\alpha \in \mathcal{O}_K$ be prime to q. Set $\tau = \alpha/\bar{\alpha}$. Let $\{s_k\}$ be the Lucas sequence with seed $\operatorname{Tr}(\tau)$. Suppose that, for some j, $s_j \equiv 0 \bmod q$. Then $q \equiv \pm 1 \bmod 2^{j+2}$.*

Proof. By Proposition 6, $s_j \equiv 0 \bmod q$ means $\operatorname{Tr}(\tau^{2^j}) \equiv 0 \bmod q$, i.e., $\tau^{2^j} + \overline{\tau}^{2^j} \equiv 0 \bmod q$. Multiplying both sides of the congruence by $\tau^{2^j} = \overline{\tau}^{-2^j}$ gives

$$\tau^{2^{j+1}} \equiv -1 \bmod q. \tag{5}$$

Suppose first that q splits in K, say $q = \lambda\overline{\lambda}$, where λ is an irreducible element of $\mathcal{O}_K$ (the ring of integers of K) with norm q. The congruence (5) holds mod λ, which implies that the image of τ has order 2^{j+2} in the group $(\mathcal{O}_K/\lambda\mathcal{O}_K)^*$. This group has order $\operatorname{Nm}\lambda - 1 = q - 1$, so we conclude 2^{j+2} divides $q-1$, i.e., $q \equiv 1 \bmod 2^{j+2}$.

Suppose q does not split in K. From (5) we see that the image of τ has order 2^{j+2} in $(\mathcal{O}_K/q\mathcal{O}_K)^*$, which is a group of order q^2-1. But $\tau = \alpha/\bar{\alpha}$ and $\alpha^q \equiv \overline{\alpha} \bmod q$, so that $\tau \equiv \alpha^{1-q} \bmod q$, and the image of τ belongs to the unique subgroup of $(\mathcal{O}_K/q\mathcal{O}_K)^*$ of order $q+1$. Therefore 2^{j+2} divides $q+1$, i.e., $q \equiv -1 \bmod 2^{j+2}$. $\square$

From now on, we work in $K = \mathbb{Q}(i)$ and we set $\alpha = -1+2i$. We note that α is a primary prime in $R = \mathcal{O}_K$ and that $2 \equiv -i \bmod \alpha$. Observe also that, since $\alpha\overline{\alpha} = 5$, any congruence mod 5 in R implies the same congruence mod α.

Now we prove Theorem 3, so that from now on M satisfies the hypotheses of the theorem. We first show that the Lucasian conditions are necessary for primality of M. Suppose then that M is prime. Since $n \geq 3$, we have $M \neq 5$, so the hypotheses allow $M^* \equiv -1, \pm 2 \bmod 5$, hence mod α. Suppose first that $M^* \equiv \pm 2 \bmod \alpha$. Then $\left(\dfrac{M^*}{\alpha}\right)_4 \equiv (M^*)^{\frac{\mathrm{Nm}\,\alpha-1}{4}} \equiv M^* \equiv \pm 2 \equiv \mp i \bmod \alpha$. Thus, by definition of the biquadratic symbol, $\left(\dfrac{M^*}{\alpha}\right)_4 = \mp i$. Applying Corollary 5,

$$(\alpha/\overline{\alpha})^{\frac{M^*-1}{4}} \equiv \mp i \bmod M$$

whence

$$(\alpha/\overline{\alpha})^{\frac{M^*-1}{2}} \equiv -1 \bmod M.$$

Since $(M^*-1)/2 = (\pm h)\cdot 2^{n-1}$, this gives $(\alpha/\overline{\alpha})^{(\pm h)\cdot 2^{n-1}} \equiv -1 \bmod M$. We thus find $\mathrm{Tr}(\alpha/\overline{\alpha})^{(\pm h)\cdot 2^{n-1}} = \mathrm{Tr}(\alpha/\overline{\alpha})^{h\cdot 2^{n-1}} \equiv -2 \bmod M$. By Proposition 6, this is equivalent to $s_{n-1} \equiv -2 \bmod M$, and $s_{n-2} \equiv 0 \bmod M$ follows from the recurrence satisfied by the s_k.

Suppose now that $M^* \equiv -1 \bmod 5$. Then, direct calculation of the biquadratic symbol, as in the first case, gives $\left(\dfrac{M^*}{\alpha}\right)_4 = -1$. By Corollary 5 again

$$(\alpha/\overline{\alpha})^{\frac{M^*-1}{4}} \equiv -1 \bmod M,$$

i.e., $(\alpha/\overline{\alpha})^{(\pm h)\cdot 2^{n-2}} \equiv -1 \bmod M$ from which, arguing as in the first case, $s_{n-3} \equiv 0 \bmod M$ follows. This completes the proof of necessity.

We now turn to the proof of sufficiency. This uses a standard method, which is, to prove that the hypotheses imply that if q is an arbitrary prime divisor of M, then $q > \sqrt{M}$.

With the notation of the theorem assume one or other of the possible congruences on the s_k is satisfied. Let q be a prime divisor of M, and let $\tau = \alpha/\bar{\alpha}$. Then the hypotheses imply $q \neq 5$ so Lemma 7 applies, and either $q \equiv \pm 1 \bmod 2^{n-1}$ or $q \equiv \pm 1 \bmod 2^n$. From these congruences it follows easily that in all cases $q \geq 2^{n-1}-1$, whence $q^2 \geq 2^{2n-2} - 2^n + 1$. On the other hand $M = h\cdot 2^n \pm 1 \leq h \cdot 2^n + 1$. But $h < 2^{n-2}-1$ by hypothesis, whence $M < 2^{2n-2} - 2^n + 1 \leq q^2$, as we wished to prove.

References

1. Wieb Bosma. Explicit primality criteria for $h \cdot 2^k \pm 1$. *Math. Comp.*, 61(203):97–109, S7–S9, 1993. MR **94c:**11005
2. K. Ireland and M. Rosen. *A classical introduction to modern number theory*. Springer Verlag, 1990. MR **92e:**11001
3. Hans Riesel. Lucasian criteria for the primality of $N = h \cdot 2^n - 1$. *Math. Comp.*, 23:869–875, 1969. MR **41:**6773
4. Hugh C. Williams. *Édouard Lucas and Primality Testing*, volume 22 of *Canadian Math. Society Series of Advanced Texts*. John Wiley and Sons, 1998. MR **2000b:**11139

Departamento de Matemáticas Puras y Aplicadas, Universidad Simón Bolívar, Caracas, Venezuela

E-mail address: pedrob@usb.ve

Departamento de Matemáticas Puras y Aplicadas, Universidad Simón Bolívar, Caracas, Venezuela

E-mail address: berry@usb.ve