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 \( s_0 \), then number \( M_{h,n} = h \cdot 2^n - 1 \) (where \( h < 2^n \) is odd) is prime iff \( s_{n-2} \equiv 0 \mod M_{h,n} \). 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 \( h \not\equiv 0 \mod 5 \). 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 \( s_{n-2} \equiv 0 \mod M_p \).

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 \( M = M_{n,h} \) as follows:

Theorem 2. Suppose \( n \geq 2 \). Let \( d \in \mathbb{Z} \) satisfy \( (\frac{d}{M}) = -1 \), where \( (\frac{\cdot}{M}) \) 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 \( \left(\frac{\alpha}{M}\right) = -1 \), where \( \bar{\alpha} \) denotes the conjugate of \( \alpha \) in \( K \). Then the following are equivalent:

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

For a proof see \[3\]. The Lucas-Lehmer test is the special case \( d = 3 \), \( \alpha = -1 + \sqrt{3} \) of this theorem. For then \( \text{Tr}_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}}(\alpha) = -4 \) 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 \( \mod M \), one can replace the rational seed by an integer seed. Second,
Theorem 3. Let $h$ of Theorem 2 allows us, for fixed $d$ in this case is to find $M$ numbers $h$ for the form

$$h^n \equiv 1 \mod n,$$

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

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

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 $(\frac{d}{M^+}) = -1$. Then $M^+$ is prime iff $d^{(M^+ - 1)/2} \equiv -1 \mod M^+$. 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 $n \geq 3$, $h \equiv 0 \mod 3$, 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 $h \equiv 0 \mod 3$ is studied in [1] and [3]. In [3] tables of seeds are given for $M_{h,n}$. In [1] for each $h \equiv 0 \mod 3$, $h < 10^5$, but $h$ not of the form $4^m - 1$, Bosma exhibits a finite set of pairs $(d_k, \alpha_k)$, $d_k \in \mathbb{Z}, \alpha_k \in \mathbb{Q}(\sqrt{d_k})$, 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 $h \equiv 0 \mod 5$, 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 $k^* = (\frac{-1}{k})k$. This notation allows us to treat the cases $h \cdot 2^n \equiv 1 \mod n$ 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, $h \equiv 0 \mod 5$, and $n \geq 3$. Let $\alpha = -1 + 2i \in \mathbb{Z}[i]$ and let $\{s_k\}$ be the Lucasian sequence with seed $s_0 = (\alpha/\tau)^h + (\tau/\alpha)^h$. Then $M$ is prime iff

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

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 $q \equiv 1 \mod 4$. Let $p$ be a prime ideal of $R$ lying over an odd rational prime, and let $\beta \in R$. The biquadratic residue symbol $(\frac{\beta}{p})_4$ is defined by:

1. If $\beta \in p$, then $(\frac{\beta}{p})_4 = 0$. 

(2) If $\beta \not\in p$, then $\left( \frac{\beta}{p} \right)_4 = \omega$, where $\omega$ is the unique fourth root of 1 in $K$ such that

$$\beta \frac{Nm p^{-1}}{p} \equiv \omega \mod p,$$

where $Nm p$ is the norm of the ideal $p$.

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

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

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

We note the following properties:

1. $\left( \frac{\beta \gamma}{\pi} \right)_4 = \left( \frac{\beta}{\pi} \right)_4 \left( \frac{\gamma}{\pi} \right)_4$.
2. $\left( \frac{\beta}{\pi \eta} \right)_4 = \left( \frac{\beta}{\pi} \right)_4 \left( \frac{\eta}{\pi} \right)_4$.
3. $\left( \frac{\beta}{\pi} \right)_4 = \left( \frac{\pi}{\pi} \right)_4$.
4. $\left( \frac{\beta \gamma}{\pi} \right)_4 = \left( \frac{\beta}{\pi} \right)_4 \left( \frac{\gamma}{\pi} \right)_4^{(-1)}$.

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 $\pi \equiv 1 \mod (1 + i)^3$.

**Proposition 4.** Let $q$ be an odd rational prime and let $\pi \in R$, $\pi \not\in \mathbb{Z}$, 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,

$$\left( \frac{q^*}{\pi} \right)_4 \equiv (\pi/\pi)^{\frac{q^*}{q} - 1} \mod q.$$
Proof. Suppose \( q \equiv 3 \mod 4 \) so that \( q^* = -q \) and \( q \) is irreducible in \( R \). Then
\[
\left( \frac{q^*}{\pi} \right)_4 = \left( \frac{\pi}{q} \right)_4 \quad \text{(Proposition 4),}
\]
\[
\left( \frac{\pi}{q} \right)_4 \equiv \pi^{\frac{q-1}{2}} \mod q \quad \text{(definition of the biquadratic symbol, and using \( \text{Nm} q = q^2 \))}
\]
\[
\equiv \left( \frac{\pi^{q-1}}{\pi} \right)^{\frac{q+1}{2}} \mod q
\]
\[
\equiv \left( \frac{\pi}{\pi^{q+1}} \right)^{\frac{q-1}{4}} \mod q \quad \text{(since \( \pi^q \equiv \pi \mod q \), as is easily seen)}
\]
\[
\equiv \left( \frac{\pi}{\pi^{q+1}} \right)^{\frac{q-1}{4}} \mod q \quad \text{(since \( q^* = -q \)).}
\]
Suppose now \( q \equiv 1 \mod 4 \). Then \( q^* = q \) and \( q \) splits in \( R \), say \( q = \lambda \bar{x} \). We have
\[
\left( \frac{q^*}{\pi} \right)_4 = \left( \frac{\pi}{q} \right)_4 \quad \text{(Proposition 4),}
\]
\[
\left( \frac{\pi}{q} \right)_4 = \left( \frac{\pi}{\lambda \bar{x}} \right)_4
\]
\[
= \left( \frac{\pi}{\lambda} \right)_4 \left( \frac{\pi}{\bar{x}} \right)_4
\]
\[
= \left( \frac{\pi}{\lambda} \right)_4 \left( \frac{\pi}{\bar{x}} \right)_4
\]
\[
= \left( \frac{\pi}{\lambda} \right)_4 \left( \frac{\pi}{\bar{x}} \right)_4
\]
\[
= \left( \frac{\pi}{\lambda} \right)_4 \left( \frac{\pi}{\bar{x}} \right)_4
\]
\[
\equiv \left( \frac{\pi}{\pi} \right)^{\frac{1}{2}} \mod q \quad \text{since \( \text{Nm} (\lambda) = q \)}
\]
which is the desired result, since \( q^* = q \). \( \square \)

Proof of Theorem 3. The underlying reason for the appearance of Lucasian sequences is the following easily verified proposition. \( \square \)

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

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 \( \text{Tr}(\tau) \). Suppose that, for some \( j, s_j \equiv 0 \mod q \). Then \( q \equiv \pm 1 \mod 2^{j+2} \).

**Proof.** By Proposition 4, \( s_j \equiv 0 \mod q \) means \( \text{Tr}(\tau^{2^j}) \equiv 0 \mod q \), i.e., \( \tau^{2^j} + \bar{\tau}^{2^j} \equiv 0 \mod q \). Multiplying both sides of the congruence by \( \tau^{2^j} = \bar{\tau}^{-2^j} \) gives
\[
\tau^{2^{j+1}} \equiv -1 \mod q.
\]
Suppose first that \( q \) splits in \( K \), say \( q = \lambda \bar{x} \), where \( \lambda \) is an irreducible element of \( \mathcal{O}_K \) (the ring of integers of \( K \)) with norm \( q \). The congruence holds mod \( \lambda \), which implies that the image of \( \tau \) has order \( 2^{j+2} \) in the group \( \left( \mathcal{O}_K/\lambda \mathcal{O}_K \right)^* \). This group has order \( \text{Nm} \lambda - 1 = q - 1 \), so we conclude \( 2^{j+2} \) divides \( q - 1 \), i.e., \( q \equiv 1 \mod 2^{j+2} \).
Suppose $q$ does not split in $K$. From [3] we see that the image of $\tau$ has order $2^{j+2}$ in $(O_K/qO_K)^*$, which is a group of order $q^2 - 1$. But $\tau = \alpha/\bar{\alpha}$ and $\alpha^q \equiv \bar{\alpha} \mod q$, so that $\tau \equiv \alpha^{1-q} \mod q$, and the image of $\tau$ belongs to the unique subgroup of $(O_K/qO_K)^*$ of order $q + 1$. Therefore $2^{j+2}$ divides $q + 1$, i.e., $q \equiv -1 \mod 2^{j+2}$. \hfill \square

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

Now we prove Theorem [5] 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 $M^* \equiv -1, \pm 2 \mod 5$, hence mod $\alpha$. Suppose first that $M^* \equiv \pm 2 \mod \alpha$. Then \[ (M^*/\alpha)^{\frac{2n-1}{(M^*/\alpha)^{\frac{2n-1}{2}}} \equiv M^* \equiv \pm 2 \equiv \mp i \mod \alpha. \] Thus, by definition of the biquadratic symbol, \[ (M^*/\alpha)^{\frac{2n-1}{2}} \equiv \mp i \mod M \]
whence \[ (\alpha/\bar{\alpha})^{\frac{M^*-1}{2}} \equiv -1 \mod M. \]

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

Suppose now that $M^* \equiv -1 \mod 5$. Then, direct calculation of the biquadratic symbol, as in the first case, gives \[ (M^*/\alpha)^{\frac{2n-1}{2}} = -1. \] By Corollary [5] again \[ (\alpha/\bar{\alpha})^{\frac{M^*-1}{2}} \equiv -1 \mod M, \] i.e., $(\alpha/\bar{\alpha})^{(\pm h) \cdot 2^{n-2}} \equiv -1 \mod M$ from which, arguing as in the first case, $s_{n-3} \equiv 0 \mod M$ 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 $q \equiv \pm 1 \mod 2^{n-1}$ or $q \equiv \pm 1 \mod 2^n$. 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


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