Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Yingpu DENG et Dandan HUANG

Explicit primality criteria for $h \cdot 2^n \pm 1$

Tome 28, nº 1 (2016), p. 55-74.

<http://jtnb.cedram.org/item?id=JTNB_2016__28_1_55_0>

Journal de Théorie des Nombres
de Bordeaux **28** (2016), 55–74

Explicit primality criteria for $h \cdot 2^n \pm 1$

par Yingpu DENG et Dandan HUANG

Résumé. Soit $\{(T_k^1, \dots, T_k^f)\}_{k \geq 0}$ une suite de f-uplets de nombres rationnels définie à partir d'une valeur initiale: une semence $(T_0^1, \dots, T_0^f)$, par f relations de récurrence qui sont des polynômes à f variables déduisant le $(k+1)$-ième terme par le k-ième terme, $k \geq 0$. Nous obtenons un algorithme ayant besoin de deux suites avec des semences convenables pour déterminer la primalité des nombres $h \cdot 2^n \pm 1$, si $h \not\equiv 0 \pmod{17}$, et cela en temps quasi-quadratique déterministe. En particulier, quand $h = 16^m - 1$ avec m impair, nous avons un test avec deux semences dépendant seulement de h, et pas de n, alors que les résultats de Berrizbeitia et Berry (2004) impliquent qu'aucune famille finie de semences dans leur test lucasien de primalité n'est suffisante pour tester la primalité de $h \cdot 2^n \pm 1$ pour tous n. Les techniques utilisées sont les lois de réciprocité octique et bi-octique.

Abstract. Let $\{(T_k^1, \dots, T_k^f)\}_{k \geq 0}$ be a sequence of f-tuples of rational numbers defined from a seed $(T_0^1, \dots, T_0^f)$, which is a given initial value, by f recurrences which are polynomials in f variables from the k-th term to deduce the $(k+1)$-th term, $k \geq 0$. We describe an algorithm which needs two such sequences with two suitable seeds to determine the primality of numbers $h \cdot 2^n \pm 1$, provided $h \not\equiv 0 \pmod{17}$, and it runs in deterministic quasi-quadratic time. In particular, when $h = 16^m - 1$, m odd, we have a test with two seeds depending only on h, not on n, while the result of Berrizbeitia and Berry (2004) implied that no finite family of seeds for their Lucasian primality test would suffice to test the primality of $h \cdot 2^n \pm 1$ for all n. The techniques which we used are Octic and Bioctic Reciprocity Laws.

Manuscrit reçu le 1$^{\text{er}}$ août 2013, révisé le 21 janvier 2015, accepté le 11 octobre 2015.

Mathematics Subject Classification. 11A51, 11Y11.

Mots-clefs. Primality test, Generalized Lucasian sequence, Reciprocity Law, Computational complexity.

We would like to thank the referee for their kind comments. The work of this paper was supported by the NNSF of China (Grant No. 11471314), NSFC (No. 11401312), NSF of the Jiangsu Higher Education Institutions (No. 14KJB110012), and the National Center for Mathematics and Interdisciplinary Sciences, CAS.

1. Introduction

Fast deterministic primality tests for numbers of the form $h \cdot 2^n \pm 1$, h odd, have been studied by Lucas [6], Lehmer [5], Bosma [3], Berrizbeitia and Berry [2] and many others. What this paper mainly concerns is that for fixed odd positive integer h, how to obtain explicit primality criteria for the family of numbers $h \cdot 2^n \pm 1$ with n increasing. Actually, this problem was also proposed by Bosma in [3], who dealt with the case $h \cdot 2^n + 1$ and the case $h \cdot 2^n - 1$ separately.

The earliest result related to the above problem could date back to Lucas and Lehmer. Before introducing their result, we give several relevant definitions. A *generalized Lucasian sequence with seed* $(T_0^1, \ldots, T_0^f)$ is a sequence $\{(T_k^1, \ldots, T_k^f)\}_{k\geq 0}$ of f-tuples of rational numbers defined from the given initial value $(T_0^1, \ldots, T_0^f)$ by f recurrences which are polynomials in f variables from the k-th term $(T_k^1, \ldots, T_k^f)$ to deduce the $(k+1)$-th term $(T_{k+1}^1, \ldots, T_{k+1}^f)$, $k \geq 0$. A *generalized Lucasian primality test* is a primality test involving finitely many generalized Lucasian sequences. In particular, if we take $f = 1$, $T_{k+1}^1 = (T_k^1)^2 - 2$ in previous definitions, then one can get *the Lucasian sequence* and *Lucasian primality test*, which are exactly the ones defined in [2].

The following theorem is the celebrated Lucas-Lehmer test for Mersenne primes, which are the special case of numbers $h \cdot 2^n - 1$, that is, the case of $h = 1$ (see [5, 6] for details).

Theorem 1.1 (Lucas-Lehmer). *Let $M_p = 2^p - 1$ be a Mersenne number, where p is an odd prime. Let $\{u_k\}_{k\geq 0}$ be the Lucasian sequence with seed $u_0 = 4$. Then M_p is prime if and only if $u_{p-2} \equiv 0 \pmod{M_p}$.*

In [3], Bosma generalized the Lucas-Lehmer test to a Lucasian primality test for numbers $h \cdot 2^n - 1$, provided that h is not divisible by 3, as follows:

Theorem 1.2 ([3]). *Let $M = h \cdot 2^n - 1$, where $h < 2^n$ is odd, $h \not\equiv 0 \pmod 3$ and $n \geq 3$. Let $\{u_k\}_{k\geq 0}$ be the Lucasian sequence with seed $u_0 = -((2+\sqrt{3})^h + (2-\sqrt{3})^h)$. Then M is prime if and only if $u_{n-2} \equiv 0 \pmod{M}$.*

One can see that the seed of this test is no longer a constant, but it depends only on h, not on n. Hence, for fixed h, $h \not\equiv 0 \pmod 3$, Theorem 1.2 leads to explicit primality criteria for all numbers $h \cdot 2^n - 1$ with n increasing by using only one seed. Bosma [3] also produced explicit primality criteria for numbers of the form $h \cdot 2^n + 1$ with $h \not\equiv 0 \pmod 3$, as follows:

Theorem 1.3 ([3]). *Let $M = h \cdot 2^n + 1$, where $h < 2^n$ is odd, $h \not\equiv 0 \pmod 3$, and $n \geq 2$. Then M is prime if and only if $3^{(M-1)/2} \equiv -1 \pmod{M}$.*

We can rewrite Theorem 1.3 as a form of generalized Lucasian primality test defined above. For that, let $\{T_k\}_{k\geq 0}$ be a generalized Lucasian sequence with seed $T_0 = 3^h$ and the recurrence $T_{k+1} = T_k^2$ for $k \geq 0$. Hence, $3^{(M-1)/2} \equiv -1 \pmod{M}$ if and only if $T_{n-1} \equiv -1 \pmod{M}$. In other words, for fixed h, $h \not\equiv 0 \pmod{3}$, Theorem 1.3 leads to a generalized Lucasian primality test for the family of numbers $h \cdot 2^n + 1$ with n varying by using a single seed $T_0 = 3^h$. In [2], Berrizbeitia and Berry first treated the cases $h \cdot 2^n \pm 1$ simultaneously in the following way:

Theorem 1.4 ([2])**.** *Let $M = h \cdot 2^n \pm 1$, where $h < 2^{n-2} - 1$ is odd, $h \not\equiv 0 \pmod{5}$, and $n \geq 4$. Let $\alpha = -1 + 2i \in \mathbb{Z}[i]$ and let $\{u_k\}_{k\geq 0}$ be the Lucasian sequence with seed $u_0 = (\alpha/\bar{\alpha})^h + (\bar{\alpha}/\alpha)^h$, where $i = \sqrt{-1}$ is a fourth complex primitive root of unity and a bar denotes the complex conjugation. Set $M^* = (-1)^{(M-1)/2}M$. Then M is prime if and only if*

(1) *either $M^* \equiv \pm 2 \pmod{5}$ and $u_{n-2} \equiv 0 \pmod{M}$*
(2) *or $M^* \equiv -1 \pmod{5}$ and $u_{n-3} \equiv 0 \pmod{M}$.*

For any odd integer k, we set $k^* = (-1)^{(k-1)/2}k$ in this paper. Theorem 1.4 is a Lucasian primality test, which leads to explicit primality criteria for all numbers $h \cdot 2^n \pm 1$ with fixed h, $h \not\equiv 0 \pmod{5}$, by using a single seed. When $h = 4^m - 1$, $m \in \mathbb{Z}$, $m > 0$, Theorem 3.3 (resp. Theorem 3.4) of [3] proved by Bosma implies that his test needs infinitely many seeds to test primality of $h \cdot 2^n + 1$ (resp. $h \cdot 2^n - 1$) for these h. Nevertheless, for $h = 4^m - 1$ with odd m (implying that $h \equiv -2 \not\equiv 0 \pmod{5}$), Theorem 1.4 allows the use of only one seed u_0, which improves the results of Bosma [3].

Until now we see that, for fixed $h \not\equiv 0 \pmod{15}$, Theorem 1.4, together with the results known to Bosma, imply that a generalized Lucasian primality test can test the primality of $h \cdot 2^n \pm 1$ with at most two sequences with two seeds. While for $h = 15$, this is the first case for which both the primality tests of [2] and [3] need infinitely many seeds. We will prove this later in Propositions 3.2 and 3.3.

The results of [2] or [3] are mainly based on the Quadratic or Biquadratic Reciprocity Law. In this paper, we make use of higher order reciprocity laws, that is Eisenstein's Reciprocity Laws of order 8 and 16, to deduce a generalized Lucasian primality test for the cases $h \cdot 2^n \pm 1$ simultaneously, provided $h \not\equiv 0 \pmod{17}$, by means of two generalized Lucasian sequences with two seeds. Moreover, the two seeds depend only on h, not on n. Thus, for $h = 16^m - 1$ with odd m, such as $h = 15$, our test implies that finitely many seeds (actually only two seeds) are needed to test the primality of $h \cdot 2^n \pm 1$ for all n large enough. Hence, our test improves the results of Berrizbeitia and Berry [2] and Bosma [3].

Bosma [3] proved Theorem 1.2 (or Theorem 1.3) by finding an integer $D = 12$ (or $D = 3$), such that the quadratic symbol $(\frac{D}{h \cdot 2^n - 1}) \neq 1$ (or

$(\frac{D}{h\cdot 2^n+1}) \neq 1)$ for all odd $h \not\equiv 0 \pmod 3$ and for all $n \geq 3$. Berrizbeitia and Berry [2] proved Theorem 1.4 by finding a primary irreducible element π in $\mathbb{Z}[i]$ of norm 5, such that the biquadratic symbol $(\frac{\pi}{h\cdot 2^n\pm 1})_4 \neq 1$ for all odd $h \not\equiv 0 \pmod 5$ and for all $n \geq 4$. To obtain the suitable seeds in our primality test, we exploit the knowledge of algebraic number theory to find a primary irreducible element $\pi_1 \in \mathbb{Z}[\zeta_8]$, of norm 17, and an irreducible element $\pi_2 \in \mathbb{Z}[\zeta_{16}]$, also of norm 17, such that for all odd $h \not\equiv 0 \pmod{17}$ and for all $n \geq 7$, either the 8−th power residue symbol $(\frac{\pi_1}{h\cdot 2^n\pm 1})_8 \neq 1$ or the 16−th power residue symbol $\left(\frac{\mu\pi_2}{h\cdot 2^n\pm 1}\right)_{16} \neq 1$, where μ is a 16-th root of unity such that $\mu\pi_2$ is a primary element in $\mathbb{Z}[\zeta_{16}]$.

The paper is organized as follows. In Section 2, we introduce the high order power residue symbol and recall Eisenstein's Reciprocity Laws, especially for the Octic and Bioctic Reciprocity Laws. In Section 3, we first state the facts we need from the arithmetic of the eighth and sixteenth cyclotomic fields, then we describe the main result of this paper. We prove this result in Section 4. Computational complexity of the generalized Lucasian primality test related to our main result is analyzed in Section 5. We end this paper with an opened problem.

2. Octic and Bioctic reciprocity

What we state in this section can be found in [4, Chapter 14] and [1, Chapter 14].

For a positive integer m, let $\zeta_m = e^{2\pi\sqrt{-1}/m}$ be a complex primitive m-th root of unity, and let $D = \mathbb{Z}[\zeta_m]$ be the ring of integers of the cyclotomic field $\mathbb{Q}(\zeta_m)$. Let $\mathfrak{p}$ be a prime ideal of D lying over a rational prime p with $\gcd(p, m) = 1$. For every $\alpha \in D$, the m-th power residue symbol $\left(\frac{\alpha}{\mathfrak{p}}\right)_m$ is defined by:

(1) If $\alpha \in \mathfrak{p}$, then $\left(\frac{\alpha}{\mathfrak{p}}\right)_m = 0$.

(2) If $\alpha \notin \mathfrak{p}$, then $\left(\frac{\alpha}{\mathfrak{p}}\right)_m = \zeta_m^i$ with $i \in \mathbb{Z}$, where ζ_m^i is the unique m-th root of unity in D such that

$$\alpha^{(\mathrm{Nm}(\mathfrak{p})-1)/m} \equiv \zeta_m^i \pmod{\mathfrak{p}},$$

where $\mathrm{Nm}(\mathfrak{p})$ is the absolute norm of the ideal $\mathfrak{p}$.

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

$$\left(\frac{\alpha}{\mathfrak{a}}\right)_m = \prod \left(\frac{\alpha}{\mathfrak{p}_i}\right)_m^{n_i}.$$

We set $\left(\frac{\alpha}{D}\right)_m = 1$.

(4) If $\beta \in D$ and β is prime to m define $\left(\frac{\alpha}{\beta}\right)_m = \left(\frac{\alpha}{\beta D}\right)_m$.

Suppose that $m = 4$, then $D = \mathbb{Z}[i]$ with $i = \sqrt{-1}$. A nonunit $\alpha \in D$ is called *primary* if $\alpha \equiv 1 \pmod{(1+i)^3}$. The next two propositions of biquadratic residue are used in Section 3. For the proofs, see Propositions 9.8.4, 9.9.6 and 9.9.7 in [4].

Proposition 2.1. *Let q be a rational prime with $q \equiv 3 \pmod 4$. Then $\left(\frac{a}{q}\right)_4 = 1$ for $a \in \mathbb{Z}$, $q \nmid a$.*

Proposition 2.2 (Biquadratic Reciprocity Law)**.** *Let q be an odd rational prime and let $\alpha \in \mathbb{Z}[i]$, $\alpha \notin \mathbb{Z}$, be irreducible and primary. Then*

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

Let $m = l^n$ ($\neq 2,\ 4$), where l is a prime and n is a positive integer. An element $\alpha \in D$ is said to be *primary* if α is coprime with m and $\epsilon_c(\alpha) = (-1)^M$, where $M = (\mathrm{N}(\alpha D) - 1)/m$, c is some given integer, and $\epsilon_c(\alpha)$ is a power of ζ_m of which the definition can be found in [1, Chapter 14]. The following crucial theorem originates from [1, Th. 14.3.1, p. 474].

Theorem 2.3 (Eisenstein's Reciprocity Law)**.** *Let $m = l^n$ ($\neq 2,\ 4$), where l is a prime and n is a positive integer. Let a be a rational prime and prime to m, and let α be a primary integer in $L = \mathbb{Q}(\zeta_m)$. Then*

(1) $\left(\frac{\alpha}{a}\right)_m = \left(\frac{a}{\alpha}\right)_m$, *if* $l > 2$,

(2) $\left(\frac{\alpha}{a}\right)_m = \left(\frac{a^*}{\alpha}\right)_m$, *if* $l = 2$.

Remark.

(1) When $m = 8$, let $\alpha \in \mathbb{Z}[\zeta_8]$ be prime to 8, then α is primary if and only if $\alpha \equiv 1$ or $1 + \zeta_8 + \zeta_8^3 \pmod 2$ (see [1, Th. 14.2.1] for details).

(2) Let $m = 2^n$ with $n \geq 3$ and let $\alpha \in \mathbb{Z}[\zeta_m]$ be prime to 2. There are exactly two m-th roots of unity μ_i such that $\mu_i\alpha$ is primary, $i = 1, 2$ (see [1, Th. 14.6.2]).

(3) It is sufficient to apply Theorem 2.3 with the cases $m = 8$ and $m = 16$ in this paper, that is, Octic and Bioctic Reciprocity Laws.

3. Explicit primality test

From now on we will deduce explicit primality criteria for numbers $M = h \cdot 2^n \pm 1$ with $n \geq 2$, provided that $h \not\equiv 0 \pmod{17}$. First, we introduce some notations which are used through the full text.

Let $\zeta_8 = e^{2\pi\sqrt{-1}/8}$ and $\zeta_{16} = e^{2\pi\sqrt{-1}/16}$, and let $L_1 = \mathbb{Q}(\zeta_8)$, $L_2 = \mathbb{Q}(\zeta_{16})$ be the eighth, sixteenth cyclotomic fields respectively. Let $D_1 = \mathbb{Z}[\zeta_8]$, $D_2 = \mathbb{Z}[\zeta_{16}]$ be the corresponding cyclotomic rings. Let G be the Galois group of $\mathbb{Q}(\zeta_{16})$ over $\mathbb{Q}$, i.e., $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{16})/\mathbb{Q})$. Then use the fact of algebraic number theory,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{16})/\mathbb{Q}) = \{\sigma_{\pm i} \mid i = 1, 3, 5, 7\}$$

where σ_c is the element of G that sends ζ_{16} to ζ_{16}^c for every odd integer c. We can also denote the element of $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$, which sends ζ_8 to ζ_8^c, by σ_c. Thus $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) = \{\sigma_{\pm i} \mid i = 1, 3\}$. Let $K_1 = \mathbb{Q}(\zeta_8 + \zeta_8^{-1})$, $K_2 = \mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$ be the maximal real subfield of L_1 and L_2 respectively. Then we have

$$\mathrm{Gal}(K_1/\mathbb{Q}) = \{\sigma_i|_{K_1} \mid i = 1, 3\},\ \mathrm{Gal}(K_2/\mathbb{Q}) = \{\sigma_i|_{K_2} \mid i = 1, 3, 5, 7\}$$

For τ in the group ring $\mathbb{Z}[G]$ and α in L_2 with $\alpha \neq 0$, we denote by α^τ to the action of the element τ of $\mathbb{Z}[G]$ on the element α of L_2, and

$$\alpha^\tau = \prod_{\sigma\in G} \sigma(\alpha)^{k_\sigma},\ \text{if } \tau = \sum_{\sigma\in G} k_\sigma \sigma \text{ where } k_\sigma \in \mathbb{Z}.$$

If $\tau \in G$, we will either write α^τ or $\tau(\alpha)$. Set $\sigma_1 = 1$ in $\mathbb{Z}[G]$.

Next we define two generalized Lucasian sequences which are used to testing primality of $M = h \cdot 2^n \pm 1$ in our explicit test. The definition of a generalized Lucasian sequence is as in the introduction.

(1) $\{(T_k, N_k)\}_{k\geq 0}$ with seed (T_0, N_0). For $k \geq 0$ define (T_{k+1}, N_{k+1}) recursively by the formulas:

$$T_{k+1} = T_k^2 - 2N_k - 4, \tag{3.1}$$

$$N_{k+1} = N_k^2 - 2T_k^2 + 4N_k + 4. \tag{3.2}$$

(2) $\{(X_k, Y_k, Z_k, W_k)\}_{k\geq 0}$ with seed (X_0, Y_0, Z_0, W_0). For $k \geq 0$ define $(X_{k+1}, Y_{k+1}, Z_{k+1}, W_{k+1})$ recursively by the formulas:

$$X_{k+1} = X_k^2 - 2Y_k - 8, \tag{3.3}$$

$$Y_{k+1} = Y_k^2 - 2X_kZ_k + 2W_k - 6X_k^2 + 12Y_k + 24, \tag{3.4}$$

$$Z_{k+1} = Z_k^2 - 2W_kY_k - 4Y_k^2 + 8X_kZ_k - 8W_k + 12X_k^2 - 24Y_k - 32, \tag{3.5}$$

$$W_{k+1} = W_k^2 - 2Z_k^2 + 4W_kY_k + 4Y_K^2 - 8X_kZ_k + 8W_k - 8X_k^2 + 16Y_k + 16. \tag{3.6}$$

The reader will see the underlying reason for the appearance of generalized Lucasian sequences $\{(T_k, N_k)\}_{k\geq 0}$ and $\{(X_k, Y_k, Z_k, W_k)\}_{k\geq 0}$, by the later Propositions 4.3 and 4.4. The elementary symmetric polynomials in variables $x_1, \ldots, x_m$, written $S_k(x_1, \ldots, x_m)$ for $k = 1, \ldots, m$, are defined by

$$S_k(x_1, \ldots, x_m) = \sum_{1\leq j_1<\ldots<j_k\leq m} x_{j_1} \ldots x_{j_k}.$$

We will need the cases of $m = 2, 4$ later. Finally, our explicit primality test is described as follows, which treats the cases $h \cdot 2^n \pm 1$ simultaneously.

Theorem 3.1. *Let $M = h \cdot 2^n \pm 1$, $n \geq 7$, where $h \not\equiv 0 \pmod{17}$, and $0 < h < 2^{n-6}$ is odd. Let $\pi_1 = 1 + 2\zeta_8^3$ and $\pi_2 = 1 - \zeta_{16} + \zeta_{16}^5$. Let*

$\{(T_k, N_k)\}_{k \geq 0}$ and $\{(X_k, Y_k, Z_k, W_k)\}_{k \geq 0}$ be two generalized Lucasian sequences defined as (3.1), (3.2) *and* (3.3), (3.4), (3.5), (3.6) *respectively, with seeds*

$$(T_0, N_0) = (\mathrm{Tr}_{K_1/\mathbb{Q}}(\alpha_1^h + \bar{\alpha_1}^h), \mathrm{Nm}_{K_1/\mathbb{Q}}(\alpha_1^h + \bar{\alpha_1}^h)),$$

and

$$\begin{aligned}(X_0, Y_0, Z_0, W_0) = (&\mathrm{Tr}_{K_2/\mathbb{Q}}(\eta), S_2(\eta, \sigma_3(\eta), \sigma_5(\eta), \sigma_7(\eta)), \\ &\qquad S_3(\eta, \sigma_3(\eta), \sigma_5(\eta), \sigma_7(\eta)), \mathrm{Nm}_{K_2/\mathbb{Q}}(\eta)),\end{aligned}$$

where $\alpha_1 = (\pi_1/\bar{\pi_1})^{1+3\sigma_3}$, $\alpha_2 = (\pi_2/\bar{\pi_2})^{1+3\sigma_{-5}+5\sigma_{-3}+7\sigma_7}$, $\eta = \alpha_2^h + \bar{\alpha_2}^h$, and a bar indicates the complex conjugation.

Then M is prime if and only if M is not divisible by any of the solutions of the equation $x^4 \equiv 1 \pmod{2^{n-3}}$ in the range $1 < x < 2^{n-3}$, and one of the followings holds:

1. $M^* \equiv \pm 4 \pmod{17}$, *and* $T_{n-3} \equiv -N_{n-3} \equiv -4 \pmod{M}$
2. $M^* \equiv \pm 2,\ \pm 8 \pmod{17}$, *and* $T_{n-3} \equiv N_{n-3} \equiv 0 \pmod{M}$
3. $M^* \equiv \pm 3,\ \pm 5,\ \pm 6,\ \pm 7 \pmod{17}$, *and* $T_{n-3} \equiv 0 \pmod{M}$, $N_{n-3} \equiv -2 \pmod{M}$
4. $M^* \equiv -1 \pmod{17}$, *and* $X_{n-4} \equiv -8 \pmod{M}$, $Y_{n-4} \equiv 24 \pmod{M}$, $Z_{n-4} \equiv -32 \pmod{M}$, $W_{n-4} \equiv 16 \pmod{M}$.

We will show Theorem 3.1 in the next section. Note that, the two seeds ((T_0, N_0) and (X_0, Y_0, Z_0, W_0)) of Theorem 3.1 depend only on h, not on n. Especially when $h = 16^m - 1$ with odd m, we have $h \equiv -2 \not\equiv 0 \pmod{17}$, so Theorem 3.1 implies that only two seeds are needed to test the primality of $h \cdot 2^n \pm 1$ for all n large enough. Nevertheless, the following Propositions 3.2 and 3.3 show that no finite family of seeds for the biquadratic test in [2] would suffice to test primality of $h \cdot 2^n \pm 1$ for all n large enough. Besides, Theorems 3.3 and 3.4 in [3] imply that Bosma's quadratic test needs infinitely many seeds to test primality of $h \cdot 2^n \pm 1$, provided that $h = 4^k - 1,\ k \geq 1$. Thereby, our generalized Lucasian primality test improves the results of Berrizbeitia and Berry [2] and Bosma [3].

Proposition 3.2. *Let m be a positive integer. Then, for every finite set of primary elements $S \subset \mathbb{Z}[i]$ with $i = \sqrt{-1}$, there exists $n \geq 2$ such that*

$$\left(\frac{\alpha}{(16^m - 1) \cdot 2^n + 1}\right)_4 = 1 \ for\ every\ \alpha \in S.$$

Proof. Let $\mathcal{P}$ be the finite set of primary irreducibles dividing at least one $\alpha \in S$:

$$\mathcal{P} = \{\pi \mid \pi \text{ primary irreducible},\ \exists\ \alpha \in S \text{ such that } \pi \mid \alpha\}.$$

Employing the fact that a primary element can be written as the product of primary irreducibles and the multiplicativity of the biquadratic symbol, it suffices to prove that there exists $n \geq 2$ such that

$$\left(\frac{\pi}{(16^m-1)\cdot 2^n+1}\right)_4 = 1 \text{ for every } \pi \in \mathcal{P}.$$

Let P be the finite set of prime numbers being divided by at least one $\pi \in \mathcal{P}$ in the ring $\mathbb{Z}[i]$:

$$P = \{p \mid p \text{ prime}, \ \exists\ \pi \in \mathcal{P} \text{ such that } \pi \mid p\}.$$

Clearly, $2 \notin P$. Next we choose $n \geq 2$ such that n is a multiple of $\mathrm{ord}_p(2)$ for every $p \in P$, where $\mathrm{ord}_p(2)$ denotes the multiplicative order of 2 modulo p. Thus for every $\pi \in \mathcal{P}$, there exists a unique $p \in P$ such that $\pi \mid p$. Suppose that $p \equiv 3 \pmod 4$, then $\pi = -p$. By Biquadratic Reciprocity Law, we have

$$\begin{aligned}\left(\frac{\pi}{(16^m-1)\cdot 2^n+1}\right)_4 &= \left(\frac{(16^m-1)\cdot 2^n+1}{\pi}\right)_4 = \left(\frac{(16^m-1)\cdot 2^n+1}{p}\right)_4 \\ &= \left(\frac{(16^m-1)\cdot 1+1}{p}\right)_4 = \left(\frac{16^m}{p}\right)_4 = 1.\end{aligned}$$

The last equality holds because $\gcd(p, 16^m) = 1$ and Proposition 2.1 applies.

Suppose now that $p \equiv 1 \pmod 4$, then $p = \pi\bar{\pi}$. By Biquadratic Reciprocity Law, we have

$$\begin{aligned}\left(\frac{\pi}{(16^m-1)\cdot 2^n+1}\right)_4 &= \left(\frac{(16^m-1)\cdot 2^n+1}{\pi}\right)_4 \equiv ((16^m-1)\cdot 2^n+1)^{(p-1)/4} \\ &\equiv ((16^m-1)\cdot 1+1)^{(p-1)/4} = 2^{m(p-1)} \equiv 1 \pmod{\pi}.\end{aligned}$$

The last congruence holds since $2^{p-1} \equiv 1 \pmod p$. Therefore,

$$\left(\frac{\pi}{(16^m-1)\cdot 2^n+1}\right)_4 = 1$$

in all cases. This proves the proposition. □

Proposition 3.3. *Let m be a positive integer. Then, for every finite set of primary elements $S \subset \mathbb{Z}[i]$ with $i = \sqrt{-1}$, there exists $n \geq 2$ such that*

$$\left(\frac{\alpha}{(16^m-1)\cdot 2^n-1}\right)_4 = 1 \ for\ every\ \alpha \in S.$$

Proof. Let $\mathcal{P}$ be the finite set of primary irreducibles dividing at least one $\alpha \in S$:

$$\mathcal{P} = \{\pi \mid \pi \text{ primary irreducible}, \ \exists\ \alpha \in S \text{ such that } \pi \mid \alpha\}.$$

By multiplicativity of the biquadratic symbol, it suffices to prove that there exists $n \geq 2$ such that

$$\left(\frac{\pi}{(16^m-1)\cdot 2^n-1}\right)_4 = 1 \text{ for every } \pi \in \mathcal{P}.$$

Let P be the finite set of prime numbers being divided by at least one $\pi \in \mathcal{P}$ in the ring $\mathbb{Z}[i]$:

$$P = \{p \mid p \text{ prime}, \ \exists\ \pi \in \mathcal{P} \text{ such that } \pi \mid p\}.$$

Clearly, $2 \notin P$. Next we can choose $n \geq 2$ such that $n \equiv -4m \pmod{\mathrm{ord}_p(2)}$ for every $p \in P$, where $\mathrm{ord}_p(2)$ denotes the multiplicative order of 2 modulo p. Thus for every $\pi \in \mathcal{P}$, there exists an unique $p \in P$ such that $\pi \mid p$. Suppose that $p \equiv 3 \pmod 4$, then $\pi = -p$. By Biquadratic Reciprocity Law, we have

$$\begin{aligned}\left(\frac{\pi}{(16^m-1)\cdot 2^n-1}\right)_4 &= \left(\frac{-(16^m-1)\cdot 2^n+1}{\pi}\right)_4 = \left(\frac{-(16^m-1)\cdot 2^n+1}{p}\right)_4 \\ &= \left(\frac{-(16^m-1)\cdot 16^{-m}+1}{p}\right)_4 = \left(\frac{16^{-m}}{p}\right)_4 = 1.\end{aligned}$$

The last equality holds since $\gcd(p, 16^m) = 1$ and Proposition 2.1 applies.

Suppose now that $p \equiv 1 \pmod 4$, then $p = \pi\bar{\pi}$. By Biquadratic Reciprocity Law, we have

$$\begin{aligned}\left(\frac{\pi}{(16^m-1)\cdot 2^n-1}\right)_4 &= \left(\frac{-(16^m-1)\cdot 2^n+1}{\pi}\right)_4 \\ &\equiv (-(16^m-1)\cdot 2^n+1)^{(p-1)/4} \\ &\equiv (-(16^m-1)\cdot 16^{-m}+1)^{(p-1)/4} \\ &\equiv 2^{-m(p-1)} \equiv 1 \pmod{\pi}.\end{aligned}$$

The last congruence makes use of the fact that $2^{p-1} \equiv 1 \pmod p$. Therefore,

$$\left(\frac{\pi}{(16^m-1)\cdot 2^n-1}\right)_4 = 1$$

in all cases. This proves the proposition. □

4. Proof of Theorem 3.1

The proof of Theorem 3.1 consists of several steps. Firstly, the next two Lemmas 4.1 and 4.2 derive two congruent relations of 8−th and 16−th power residue symbols, which are crucial to the proof of necessity of Theorem 3.1. Secondly, the proof of sufficiency of the congruences on the generalized Lucasian sequences is mainly based on Lemmas 4.5 and 4.6. Besides, we will use the Octic and Bioctic Reciprocity Laws in the proof, which need primary elements of $\mathbb{Z}[\zeta_8]$ and $\mathbb{Z}[\zeta_{16}]$ respectively. Corollary 4.8 is used in the final proof, instead of Lemma 4.2, since that we need not verify if the element $\pi_2 = 1 - \zeta_{16} + \zeta_{16}^5$ is primary or not.

Lemma 4.1. *Let q be an odd prime such that $q^* \equiv 1 \pmod 8$, and let $\pi \neq 0$ be an integer in $L_1 = \mathbb{Q}(\zeta_8)$. Then*

$$\left(\frac{\pi}{q}\right)_8 \equiv \alpha^{\frac{q^*-1}{8}} \pmod q$$

where $\alpha = (\pi/\bar{\pi})^{1+3\sigma_3}$.

Proof. Suppose $q^* = q$, that is, $q \equiv 1 \pmod 8$. Then the ideal qD_1 factorizes into a product of 4 distinct prime ideals in the ring D_1, written as $qD_1 = (\mathfrak{p}\bar{\mathfrak{p}})^{1+\sigma_3}$. By the definition of 8−th residue symbol, we have

$$\begin{aligned}\left(\frac{\pi}{q}\right)_8 &= \left(\frac{\pi}{(\mathfrak{p}\bar{\mathfrak{p}})^{1+\sigma_3}}\right)_8 = \left(\frac{\pi}{\mathfrak{p}\bar{\mathfrak{p}}(\mathfrak{p}\bar{\mathfrak{p}})^{\sigma_3}}\right)_8 \\ &= \left(\frac{\pi/\bar{\pi}}{\mathfrak{p}}\right)_8 \left(\frac{(\pi/\bar{\pi})^{3\sigma_3}}{\mathfrak{p}}\right)_8 = \left(\frac{\alpha}{\mathfrak{p}}\right)_8 \equiv \alpha^{\frac{q-1}{8}} \pmod{\mathfrak{p}}.\end{aligned}$$

Since $\mathfrak{p}$ is an arbitrary prime ideal lying over q, we have

$$\left(\frac{\pi}{q}\right)_8 \equiv \alpha^{\frac{q^*-1}{8}} \pmod q.$$

Suppose now $q^* = -q$, that is, $q \equiv -1 \pmod 8$. Then the ideal qD_1 factorizes into a product of 2 distinct prime ideals, written as $qD_1 = \mathfrak{p}\mathfrak{p}^{\sigma_3}$. Thus

$$\begin{aligned}\left(\frac{\pi}{q}\right)_8 &= \left(\frac{\pi}{\mathfrak{p}\mathfrak{p}^{\sigma_3}}\right)_8 = \left(\frac{\pi}{\mathfrak{p}}\right)_8 \left(\frac{\pi}{\mathfrak{p}^{\sigma_3}}\right)_8 \\ &= \left(\frac{\pi^{1+3\sigma_3}}{\mathfrak{p}}\right)_8 \equiv (\pi^{1+3\sigma_3})^{\frac{q^2-1}{8}} \equiv \bar{\alpha}^{\frac{q+1}{8}} \pmod{\mathfrak{p}}.\end{aligned}$$

The last congruence holds because of $\pi^q \equiv \bar{\pi} \pmod{\mathfrak{p}}$, which can be seen by observing that the complex conjugation coincides with the Frobenius automorphism of $D_1/\mathfrak{p}$. Hence

$$\left(\frac{\pi}{q}\right)_8 \equiv \bar{\alpha}^{\frac{-q^*+1}{8}} = \alpha^{\frac{q^*-1}{8}} \pmod q.$$

The last equality makes use of the fact $\alpha\bar{\alpha} = 1$. This ends the proof. □

Lemma 4.2. *Let q be an odd prime such that $q^* \equiv 1 \pmod{16}$, and let $\pi \neq 0$ be an integer in $L_2 = \mathbb{Q}(\zeta_{16})$. Then*

$$\left(\frac{\pi}{q}\right)_{16} \equiv \alpha^{\frac{q^*-1}{16}} \pmod q$$

where $\alpha = (\pi/\bar{\pi})^{1+3\sigma_{-5}+5\sigma_{-3}+7\sigma_7}$.

Proof. Suppose $q^* = q$, i.e., $q \equiv 1 \pmod{16}$, Thus the ideal qD_2 factorizes into the product of 8 distinct prime ideals in the ring D_2, written as $qD_2 =$

$(\mathfrak{p}\bar{\mathfrak{p}})^{1+\sigma_3+\sigma_5+\sigma_7}$. According to the definition of 16-th residue symbol, we have

$$\begin{aligned}\left(\frac{\pi}{q}\right)_{16} &= \left(\frac{\pi}{(\mathfrak{p}\bar{\mathfrak{p}})^{1+\sigma_3+\sigma_5+\sigma_7}}\right)_{16} = \left(\frac{(\pi/\bar{\pi})^{1+3\sigma_{-5}+5\sigma_{-3}+7\sigma_7}}{\mathfrak{p}}\right)_{16}\\ &= \left(\frac{\alpha}{\mathfrak{p}}\right)_{16} \equiv \alpha^{\frac{q-1}{16}} \pmod{\mathfrak{p}}.\end{aligned}$$

Since $\mathfrak{p}$ is an arbitrary prime ideal lying over q, we get

$$\left(\frac{\pi}{q}\right)_{16} \equiv \alpha^{\frac{q^*-1}{16}} \pmod{q}.$$

Suppose now $q^* = -q$, i.e., $q \equiv -1 \pmod{16}$. Then the ideal qD_2 could be written as a product of 4 distinct prime ideals, written as $qD_2 = \mathfrak{p}^{1+\sigma_3+\sigma_5+\sigma_7}$. Thus we have

$$\begin{aligned}\left(\frac{\pi}{q}\right)_{16} &= \left(\frac{\pi}{\mathfrak{p}}\right)_{16}\left(\frac{\pi}{\mathfrak{p}^{\sigma_3}}\right)_{16}\left(\frac{\pi}{\mathfrak{p}^{\sigma_5}}\right)_{16}\left(\frac{\pi}{\mathfrak{p}^{\sigma_7}}\right)_{16} = \left(\frac{\pi^{1+3\sigma_{-5}+5\sigma_{-3}+7\sigma_7}}{\mathfrak{p}}\right)_{16}\\ &\equiv \left(\pi^{1+3\sigma_{-5}+5\sigma_{-3}+7\sigma_7}\right)^{(q^2-1)/16} \equiv \bar{\alpha}^{(q+1)/16} \pmod{\mathfrak{p}}.\end{aligned}$$

The last congruence uses the fact that $\pi^q \equiv \bar{\pi} \pmod{\mathfrak{p}}$, which can be seen by observing that the complex conjugation coincides with the Frobenius automorphism of $D_2/\mathfrak{p}$. Therefore

$$\left(\frac{\pi}{q}\right)_{16} \equiv \bar{\alpha}^{(-q^*+1)/16} = \alpha^{(q^*-1)/16} \pmod{q}.$$

The last equality holds since $\alpha\bar{\alpha} = 1$. □

The following two propositions explain the appearance of generalized Lucasian sequences $\{(T_k, N_k)\}$ and $\{(X_k, Y_k, Z_k, W_k)\}$ in Theorem 3.1.

Proposition 4.3. *Let α be an element satisfying $\alpha\bar{\alpha} = 1$ in the field $L_1 = \mathbb{Q}(\zeta_8)$. Let $\{(T_k, N_k)\}_{k\geq 0}$ be the generalized Lucasian sequence defined as* (3.1) *and* (3.2) *with seed $(T_0, N_0) = (\mathrm{Tr}_{K_1/\mathbb{Q}}(\alpha + \bar{\alpha}), \mathrm{Nm}_{K_1/\mathbb{Q}}(\alpha + \bar{\alpha}))$. Then $T_k = \mathrm{Tr}_{K_1/\mathbb{Q}}(\alpha^{2^k} + \bar{\alpha}^{2^k})$ and $N_k = \mathrm{Nm}_{K_1/\mathbb{Q}}(\alpha^{2^k} + \bar{\alpha}^{2^k})$, for $k \geq 0$.*

Proof. It suffices to prove that $\mathcal{T}_k := \mathrm{Tr}_{K_1/\mathbb{Q}}(\alpha^{2^k} + \bar{\alpha}^{2^k})$ and $\mathcal{N}_k := \mathrm{Nm}_{K_1/\mathbb{Q}}(\alpha^{2^k} + \bar{\alpha}^{2^k})$ satisfy the recurrent relations given by (3.1) and (3.2). To see this, let $A_k = \alpha^{2^k} + \bar{\alpha}^{2^k}$ and $B_k = \sigma_3(A_k)$. Thus $\mathcal{T}_k = A_k + B_k$, $\mathcal{N}_k = A_k B_k$.

Since $\alpha\bar{\alpha}=1$, we get $A_{k+1}=A_k^2-2$, $B_{k+1}=B_k^2-2$. Substituting them in $\mathcal{T}_{k+1}$ and $\mathcal{N}_{k+1}$, one may obtain

$$\begin{aligned}
\mathcal{T}_{k+1} &= A_k^2+B_k^2-4=\mathcal{T}_k^2-2\mathcal{N}_k-4,\\
\mathcal{N}_{k+1} &= (A_k^2-2)(B_k^2-2)=\mathcal{N}_k^2-2(\mathcal{T}_k^2-2\mathcal{N}_k)+4\\
&\qquad\qquad\qquad\qquad\quad =\mathcal{N}_k^2-2\mathcal{T}_k^2+4\mathcal{N}_k+4.
\end{aligned}$$

This is exactly what we want. □

Proposition 4.4. *Let α be an element satisfying $\alpha\bar{\alpha}=1$ in the field $L_2=\mathbb{Q}(\zeta_{16})$ and $\eta=\alpha+\bar{\alpha}$. Let $\{(X_k,Y_k,Z_k,W_k)\}_{k\geq 0}$ be the generalized Lucasian sequence defined as* (3.3), (3.4), (3.5) *and* (3.6) *with seed $X_0=\mathrm{Tr}_{K_2/\mathbb{Q}}(\eta)$, $Y_0=S_2(\eta,\sigma_3(\eta),\sigma_5(\eta),\sigma_7(\eta))$, $Z_0=S_3(\eta,\sigma_3(\eta),\sigma_5(\eta),\sigma_7(\eta))$ and $W_0=\mathrm{Nm}_{K_2/\mathbb{Q}}(\eta)$. Then $X_k=\mathrm{Tr}_{K_2/\mathbb{Q}}(\eta_k)$, $Y_k=S_2(\eta_k,\sigma_3(\eta_k),\sigma_5(\eta_k),\sigma_7(\eta_k))$, $Z_k=S_3(\eta_k,\sigma_3(\eta_k),\sigma_5(\eta_k),\sigma_7(\eta_k))$ and $W_k=\mathrm{Nm}_{K_2/\mathbb{Q}}(\eta_k)$, where $\eta_k=\alpha^{2^k}+\bar{\alpha}^{2^k}$, for $k\geq 0$.*

Proof. It suffices to prove that $\mathcal{X}_k=\mathrm{Tr}_{K_2/\mathbb{Q}}(\eta_k)$, $\mathcal{W}_k=\mathrm{Nm}_{K_2/\mathbb{Q}}(\eta_k)$, $\mathcal{Y}_k=S_2(\eta_k,\sigma_3(\eta_k),\sigma_5(\eta_k),\sigma_7(\eta_k))$, and $\mathcal{Z}_k=S_3(\eta_k,\sigma_3(\eta_k),\sigma_5(\eta_k),\sigma_7(\eta_k))$ satisfy the recurrences (3.3), (3.4), (3.5) and (3.6).

To see this, let $A_k=\eta_k$, $B_k=\sigma_3(\eta_k)$, $C_k=\sigma_5(\eta_k)$ and $D_k=\sigma_7(\eta_k)$. As in Proposition 4.3, we have $A_{k+1}=A_k^2-2$, $B_{k+1}=B_k^2-2$, $C_{k+1}=C_k^2-2$ and $D_{k+1}=D_k^2-2$. Substituting all of them in $\mathcal{X}_{k+1}$, $\mathcal{Y}_{k+1}$, $\mathcal{Z}_{k+1}$ and $\mathcal{W}_{k+1}$, one may obtain

$$\begin{aligned}
\mathcal{X}_{k+1} &= A_k^2+B_k^2+C_k^2+D_k^2-8\\
&= \mathcal{X}_k^2-2\mathcal{Y}_k-8,\\
\mathcal{Y}_{k+1} &= (A_kB_k)^2+(A_kC_k)^2+(A_kD_k)^2+(B_kC_k)^2+(B_kD_k)^2+(C_kD_k)^2\\
&\quad -6(A_k^2+B_k^2+C_k^2+D_k^2)+24\\
&= \mathcal{Y}_k^2-2(\mathcal{X}_k\mathcal{Z}_k-\mathcal{W}_k)-6(\mathcal{X}_k^2-2\mathcal{Y}_k)+24,\\
\mathcal{Z}_{k+1} &= (A_kB_kC_k)^2+(A_kB_kD_k)^2+(A_kC_kD_k)^2+(B_kC_kD_k)^2\\
&\quad -4[(A_kB_k)^2+(A_kC_k)^2+(A_kD_k)^2+(B_kC_k)^2+(B_kD_k)^2\\
&\quad +(C_kD_k)^2]+12(A_k^2+B_k^2+C_k^2+D_k^2)-32\\
&= \mathcal{Z}_k^2-2\mathcal{W}_k\mathcal{Y}_k-4\mathcal{Y}_k^2+8(\mathcal{X}_k\mathcal{Z}_k-\mathcal{W}_k)+12\mathcal{X}_k^2-24\mathcal{Y}_k-32,\\
\mathcal{W}_{k+1} &= (A_k^2-2)(B_k^2-2)(C_k^2-2)(D_k^2-2)\\
&= \mathcal{W}_k^2-2\mathcal{Z}_k^2+4\mathcal{W}_k\mathcal{Y}_k+4\mathcal{Y}_k^2-8(\mathcal{X}_k\mathcal{Z}_k-\mathcal{W}_k)-8\mathcal{X}_k^2+16\mathcal{Y}_k+16.
\end{aligned}$$

This is exactly what we want. □

By Proposition 4.3, we obtain $T_k = S_1(\eta_k, \sigma_3(\eta_k)),\ N_k = S_2(\eta_k, \sigma_3(\eta_k))$, where $\eta_k = \alpha^{2^k} + \bar{\alpha}^{2^k}$. Thereby, T_k and N_k are the coefficients of the characteristic polynomial of η_k with respect to the field extension $K_1/\mathbb{Q}$. Also, applying Proposition 4.4, we get $X_k = S_1(\eta_k, \sigma_3(\eta_k), \sigma_5(\eta_k), \sigma_7(\eta_k))$, $Y_k = S_2(\eta_k, \sigma_3(\eta_k), \sigma_5(\eta_k), \sigma_7(\eta_k))$, $Z_k = S_3(\eta_k, \sigma_3(\eta_k), \sigma_5(\eta_k), \sigma_7(\eta_k))$ and $W_k = S_4(\eta_k, \sigma_3(\eta_k), \sigma_5(\eta_k), \sigma_7(\eta_k))$. Thus X_k, Y_k, Z_k and W_k are exactly the coefficients of the characteristic polynomial of η_k with respect to the field extension $K_2/\mathbb{Q}$.

After we made clear these generalized Lucasian sequences, we need the following two lemmas for the proof of sufficiency of Theorem 3.1.

Lemma 4.5. *Let fields L_1 and K_1 be as before, let q be an odd prime and let $\pi \in D_1$ be prime to q. Set $\alpha = \pi/\bar{\pi}$. Let $\{(T_k, N_k)\}_{k \geq 0}$ be the generalized Lucasian sequence defined as* (3.1) *and* (3.2) *with seed* $(T_0, N_0) = (\mathrm{Tr}_{K_1/\mathbb{Q}}(\alpha + \bar{\alpha}), \mathrm{Nm}_{K_1/\mathbb{Q}}(\alpha + \bar{\alpha}))$*. Suppose that for some $j \geq 0$, one of the followings holds:*

(1) $T_j \equiv -N_j \equiv -4 \pmod{q}$,
(2) $T_j \equiv N_j \equiv 0 \pmod{q}$,
(3) $T_j \equiv 0 \pmod{q}$ *and* $N_j \equiv -2 \pmod{q}$.

Then $q^2 \equiv 1 \pmod{2^{j+1}}$.

Proof. We have $T_j = \mathrm{Tr}_{K_1/\mathbb{Q}}(\alpha^{2^j} + \bar{\alpha}^{2^j})$, $N_j = \mathrm{Nm}_{K_1/\mathbb{Q}}(\alpha^{2^j} + \bar{\alpha}^{2^j})$ using Proposition 4.3. Let $\mathfrak{q}$ be a prime ideal of the ring of integers of K_1 lying over q, and $\mathfrak{Q}$ be a prime ideal of D_1 lying over $\mathfrak{q}$. Let $\beta = \alpha^{2^j} + \bar{\alpha}^{2^j}$.

Suppose (1) holds, that is, $\mathrm{Tr}_{K_1/\mathbb{Q}}(\beta) \equiv -4 \equiv -\mathrm{Nm}_{K_1/\mathbb{Q}}(\beta) \pmod{\mathfrak{q}}$. Using the property of the characteristic polynomial of β, we get

$$\beta^2 + 4\beta + 4 \equiv 0 \pmod{\mathfrak{q}},\ \textit{i.e.},\ \alpha^{2^j} + \bar{\alpha}^{2^j} \equiv -2 \pmod{\mathfrak{Q}},$$

since $\alpha\bar{\alpha} = 1$ and π is prime to q. Multiplying both sides of the above congruence by $\alpha^{2^j} = \bar{\alpha}^{-2^j}$, we have

$$\alpha^{2^j} \equiv -1 \pmod{\mathfrak{Q}}.$$

That is to say, the image of α has order 2^{j+1} in the multiplicative group $(D_1/\mathfrak{Q})^*$. We already know the order of this group is $\mathrm{N}(\mathfrak{Q})-1$ which divides $q^2 - 1$. Thus $q^2 \equiv 1 \pmod{2^{j+1}}$.

Suppose (2) holds, that is, $\mathrm{Tr}_{K_1/\mathbb{Q}}(\beta) \equiv 0 \equiv \mathrm{Nm}_{K_1/\mathbb{Q}}(\beta) \pmod{\mathfrak{q}}$. Similarly, we get

$$\beta^2 \equiv 0 \pmod{\mathfrak{q}},\ \textit{i.e.},\ \alpha^{2^j} + \bar{\alpha}^{2^j} \equiv 0 \pmod{\mathfrak{Q}}.$$

Multiplying both sides of the last congruence by $\alpha^{2^j} = \bar{\alpha}^{-2^j}$, we have

$$\alpha^{2^{j+1}} \equiv -1 \pmod{\mathfrak{Q}}.$$

That is to say, the image of α has order 2^{j+2} in the group $(D_1/\mathfrak{Q})^*$, so $q^2 \equiv 1 \pmod{2^{j+2}}$.

Suppose now (3) holds, that is, $\mathrm{Tr}_{K_1/\mathbb{Q}}(\beta) \equiv 0 \pmod{\mathfrak{q}}$ and $\mathrm{Nm}_{K_1/\mathbb{Q}}(\beta) \equiv -2 \pmod{\mathfrak{q}}$. Thus

$$\beta^2 - 2 \equiv 0 \pmod{\mathfrak{q}}, \ \textit{i.e.}, \ \alpha^{2^{j+1}} + \bar{\alpha}^{2^{j+1}} \equiv 0 \pmod{\mathfrak{Q}}.$$

Multiplying both sides of the above congruence by $\alpha^{2^{j+1}} = \bar{\alpha}^{-2^{j+1}}$, we get

$$\alpha^{2^{j+2}} \equiv -1 \pmod{\mathfrak{Q}}.$$

In this case the order of the image of α in $(D_1/\mathfrak{Q})^*$ is 2^{j+3}. Hence we have $q^2 \equiv 1 \pmod{2^{j+3}}$. This ends the proof. □

Lemma 4.6. *Let fields L_2 and K_2 be as before, let q be an odd prime and let $\pi \in D_2$ be prime to q. Set $\alpha = \pi/\bar{\pi}$. Let $\{(X_k, Y_k, Z_k, W_k)\}_{k\geq 0}$ be the generalized Lucasian sequence defined as* (3.3), (3.4), (3.5) *and* (3.6) *with seed*

$$(X_0, Y_0, Z_0, W_0) = (\mathrm{Tr}_{K_2/\mathbb{Q}}(\eta), S_2(\eta, \sigma_3(\eta), \sigma_5(\eta), \sigma_7(\eta)),$$
$$S_3(\eta, \sigma_3(\eta), \sigma_5(\eta), \sigma_7(\eta)), \mathrm{Nm}_{K_2/\mathbb{Q}}(\eta)),$$

where $\eta = \alpha + \bar{\alpha}$. Suppose that for some $j \geq 0$, $X_j \equiv -8 \pmod{q}$, $Y_j \equiv 24 \pmod{q}$, $Z_j \equiv -32 \pmod{q}$ and $W_j \equiv 16 \pmod{q}$. Then $q^4 \equiv 1 \pmod{2^{j+1}}$.

Proof. We have $X_j = \mathrm{Nm}_{K_2/\mathbb{Q}}(\beta)$, $Y_j = S_2(\beta, \sigma_3(\beta), \sigma_5(\beta), \sigma_7(\beta))$, $Z_j = S_3(\beta, \sigma_3(\beta), \sigma_5(\beta), \sigma_7(\beta))$, and $W_j = \mathrm{Nm}_{K_2/\mathbb{Q}}(\beta)$ using Proposition 4.4, where $\beta = \alpha^{2^j} + \bar{\alpha}^{2^j} \in K_2$. Let $\mathfrak{q}$ be a prime ideal of the ring of integers of K_2 lying over q, and $\mathfrak{Q}$ be a prime ideal of D_2 lying over $\mathfrak{q}$. Thus the assumption tells us that the characteristic polynomial of β has the following property:

$$(\beta + 2)^4 = \beta^4 + 8\beta^3 + 24\beta^2 + 32\beta + 16 \equiv 0 \pmod{\mathfrak{q}},$$

i.e.,

$$\alpha^{2^j} + \bar{\alpha}^{2^j} \equiv -2 \pmod{\mathfrak{Q}}.$$

Multiplying both sides of the above congruence by $\alpha^{2^j} = \bar{\alpha}^{-2^j}$, we have

$$\alpha^{2^j} \equiv -1 \pmod{\mathfrak{Q}}.$$

That is to say, the image of α has order 2^{j+1} in the multiplicative group $(D_2/\mathfrak{Q})^*$. Since this group is of order $\mathrm{N}(\mathfrak{Q}) - 1$ which divides $q^4 - 1$, we obtain $q^4 \equiv 1 \pmod{2^{j+1}}$ as desired. □

From now on, we set $\pi_1 = 1 + 2\zeta_8^3$ and $\pi_2 = 1 - \zeta_{16} + \zeta_{16}^5$. Since $\pi_1 \equiv 1 \pmod{2}$, π_1 is a primary element in $D_1 = \mathbb{Z}[\zeta_8]$ by Remark 2 (i). Note that $2 - \zeta_8 = -\pi_1 \cdot \zeta_8$ implies $2 \equiv \zeta_8 \pmod{\pi_1}$. According to the definition of a primary element, it may be troublesome to verify if π_2 is primary or not in the ring $D_2 = \mathbb{Z}[\zeta_{16}]$. But we know that there exists a 16-th root of unity μ such that $\mu\pi_2$ is primary in D_2 by Remark 2 (ii). It is enough to deduce our main result (Theorem 3.1) with the choice of the element π_2 because of this fact and the following key proposition, no matter π_2 is primary or not.

Proposition 4.7. *Let q be an odd prime such that $q^* \equiv 1 \pmod{2^7}$, and let $\tau_1,\ \tau_2$ be two nonzero elements in D_2 with $\tau_1 = \mu\tau_2$, where μ is a 16-th root of unity. Then*

$$\alpha_1^{\frac{q^*-1}{16}} = \alpha_2^{\frac{q^*-1}{16}}$$

where $\alpha_1 = \tau_1/\bar{\tau}_1,\ \alpha_2 = \tau_2/\bar{\tau}_2$.

Proof. Under direct computation, we have

$$\begin{aligned}\alpha_1^{\frac{q^*-1}{16}} &= \left(\frac{\tau_1}{\bar{\tau}_1}\right)^{\frac{q^*-1}{16}} = \left(\frac{\mu}{\bar{\mu}}\right)^{\frac{q^*-1}{16}} \left(\frac{\tau_2}{\bar{\tau}_2}\right)^{\frac{q^*-1}{16}} \\ &= \mu^{\frac{q^*-1}{8}} \alpha_2^{\frac{q^*-1}{16}} = \alpha_2^{\frac{q^*-1}{16}}.\end{aligned}$$

The last two equalities hold since $\mu\bar{\mu} = 1$ and $16 \mid \frac{q^*-1}{8}$, that is, $\mu^{\frac{q^*-1}{8}} = 1$. □

Combining Lemma 4.2 with Proposition 4.7, it is easy to deduce the following corollary.

Corollary 4.8. *Let q be an odd prime with $q^* \equiv 1 \pmod{2^7}$, and let $\tau_1,\ \tau_2$ be two nonzero elements in D_2 with $\tau_1 = \mu\tau_2$, where μ is a 16-th root of unity. Then*

$$\left(\frac{\tau_1}{q}\right)_{16} \equiv \alpha_2^{\frac{q^*-1}{16}} \pmod{q}$$

where $\alpha_2 = (\tau_2/\bar{\tau}_2)^{1+3\sigma_{-5}+5\sigma_{-3}+7\sigma_7}$.

Observe also that, $\mathrm{Nm}_{L_1/\mathbb{Q}}(\pi_1) = \mathrm{Nm}_{L_2/\mathbb{Q}}(\pi_2) = 17$, thus any congruence mod 17 in D_1 or D_2 implies the same congruence mod π_1 or mod π_2. In fact, using a little knowledge of algebraic number theory, and the important fact that both of D_1 and D_2 are principal ideal domains (see [8, Th. 11.1]), we can factorize the number 17 as follows:

$$17 = (1+4i)(1-4i) = (1+2\zeta_8^3)(1-2\zeta_8^3)(1+2\zeta_8)(1-2\zeta_8),\ \textit{where } i = \sqrt{-1}.$$

And $1+2\zeta_8^3,\ \sqrt{2}$ can be expressed as $1+2\zeta_8^3 = (1+\sqrt{2}\zeta_{16}^7)(1-\sqrt{2}\zeta_{16}^7)$ and $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$. Thereby, we obtain the possible choices of π_1 and π_2.

Remark. Let $M = h \cdot 2^n \pm 1$, where $n \geq 2$ and $h \not\equiv 0 \pmod{17}$, thus $M^* \not\equiv 1 \pmod{17}$. Moreover, if $M^* \not\equiv -1 \pmod{17}$, then $(\frac{\pi_1}{M})_8 \neq 1$. If $M^* \equiv -1 \pmod{17}$, then $(\frac{\pi}{M})_{16} \neq 1$ but $(\frac{\pi_1}{M})_8 = 1$, where $\pi = \mu\pi_2$ is primary in D_2 and μ is a 16-th root of unity, for details see the proof below. That is why the use of the 8-th power residue and octic reciprocity is not sufficient. Also, it is that single class $-1 \pmod{17}$ that makes necessary the 16-th power residue and bioctic reciprocity, provided $h \not\equiv 0 \pmod{17}$.

Finally, we prove Theorem 3.1 as follows. One may see that we do not need Octic and Bioctic Reciprocity Laws in full generality, rather in the proof of necessity.

Proof of Theorem 3.1. We first show that the generalized Lucasian conditions are necessary for primality of M. Suppose that M is a prime. Since $n \geq 7$, thus $M \neq 17$, and the hypotheses allow $M^* \equiv -1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 7, \pm 8 \pmod{17}$, hence mod π_1 or mod π_2. Since π_1 is primary in D_1, we get $(\frac{\pi_1}{M})_8 = \left(\frac{M^*}{\pi_1}\right)_8$ by applying Octic Reciprocity Law.

(1) Suppose first that $M^* \equiv \pm 4 \pmod{17}$. Then $\left(\frac{M^*}{\pi_1}\right)_8 \equiv (M^*)^{(17-1)/8} \equiv (M^*)^2 \equiv -1 \pmod{\pi_1}$, that is, $\left(\frac{M^*}{\pi_1}\right)_8 = -1$. Applying Lemma 4.1,

$$\alpha_1^{\frac{M^*-1}{8}} \equiv \left(\frac{\pi_1}{M}\right)_8 = \left(\frac{M^*}{\pi_1}\right)_8 = -1 \pmod{M}$$

where $\alpha_1 = (\pi_1/\bar{\pi_1})^{1+3\sigma_3}$. Since $(M^*-1)/8 = (\pm h) \cdot 2^{n-3}$, this gives

$$\alpha_1^{\pm h \cdot 2^{n-3}} \equiv -1 \pmod{M}.$$

We always have $\alpha_1^{h \cdot 2^{n-3}} + \bar{\alpha_1}^{h \cdot 2^{n-3}} \equiv -2 \pmod{M}$ because of $\alpha_1 \bar{\alpha_1} = 1$. Thus we find $\mathrm{Tr}_{K_1/\mathbb{Q}}(\alpha_1^{h \cdot 2^{n-3}} + \bar{\alpha_1}^{h \cdot 2^{n-3}}) \equiv -4 \pmod{M}$ and $\mathrm{Nm}_{K_1/\mathbb{Q}}(\alpha_1^{h \cdot 2^{n-3}} + \bar{\alpha_1}^{h \cdot 2^{n-3}}) \equiv 4 \pmod{M}$. By Proposition 4.3, this is equivalent to $T_{n-3} \equiv -4 \pmod{M}$ and $N_{n-3} \equiv 4 \pmod{M}$.

(2) Suppose that $M^* \equiv \pm 2, \pm 8 \pmod{17}$. Then $\left(\frac{M^*}{\pi_1}\right)_8 \equiv (M^*)^2 \equiv \pm 4 \equiv \pm \zeta_8^2 \pmod{\pi_1}$, that is, $\left(\frac{M^*}{\pi_1}\right)_8 = \pm \zeta_8^2$. Applying Lemma 4.1 again,

$$\alpha_1^{\frac{M^*-1}{8}} \equiv \left(\frac{\pi_1}{M}\right)_8 = \left(\frac{M^*}{\pi_1}\right)_8 = \pm \zeta_8^2 \pmod{M}.$$

That is to say $\alpha_1^{\pm h \cdot 2^{n-3}} \equiv \pm \zeta_8^2 \pmod{M}$ and we have

$$\alpha_1^{h \cdot 2^{n-3}} + \bar{\alpha_1}^{h \cdot 2^{n-3}} \equiv 0 \pmod{M}.$$

Similarly by Proposition 4.3, we find $T_{n-3} \equiv N_{n-3} \equiv 0 \pmod{M}$.

(3) Suppose now that $M^* \equiv \pm 3, \pm 5, \pm 6, \pm 7 \pmod{17}$. Then $\left(\frac{M^*}{\pi_1}\right)_8 \equiv (M^*)^2 \equiv \pm 2, \pm 8 \equiv \pm \zeta_8, \pm \zeta_8^3 \pmod{\pi_1}$, that is, $\left(\frac{M^*}{\pi_1}\right)_8 = \pm \zeta_8, \pm \zeta_8^3$. A final application of Lemma 4.1 yields

$$\alpha_1^{\frac{M^*-1}{8}} \equiv \left(\frac{\pi_1}{M}\right)_8 = \left(\frac{M^*}{\pi_1}\right)_8 = \pm \zeta_8, \pm \zeta_8^3 \pmod{M}.$$

We thus always have

$$\alpha_1^{h \cdot 2^{n-3}} + \bar{\alpha_1}^{h \cdot 2^{n-3}} \equiv \pm(\zeta_8 + \zeta_8^7) \pmod{M}.$$

By Proposition 4.3, we obtain $T_{n-3} \equiv \pm(\zeta_8 + \zeta_8^7 + \zeta_8^3 + \zeta_8^5) = 0 \pmod{M}$, and $N_{n-3} \equiv (\zeta_8 + \zeta_8^7) \cdot (\zeta_8^3 + \zeta_8^5) = -2 \pmod{M}$.

For the last exceptional case (4), let $\pi = \mu\pi_2$ be a primary element in D_2, where μ is a 16-th root of unity. So we can apply Bioctic Reciprocity Law to π and M and obtain $(\frac{\pi}{M})_{16} = \left(\frac{M^*}{\pi}\right)_{16}$. When $M^* \equiv -1 \pmod{17}$,

$$\left(\frac{M^*}{\pi}\right)_{16} \equiv (M^*)^{(17-1)/16} \equiv M^* \equiv -1 \pmod{\pi}$$

i.e. $\left(\frac{M^*}{\pi}\right)_{16} = -1$. The hypotheses imply that 2^7 divides $M^* - 1$, so Corollary 4.8 applies and

$$\alpha_2^{\frac{M^*-1}{16}} \equiv \left(\frac{\pi}{M}\right)_{16} = \left(\frac{M^*}{\pi}\right)_{16} = -1 \pmod{M}$$

where $\alpha_2 = (\pi_2/\bar{\pi}_2)^{1+3\sigma_{-5}+5\sigma_{-3}+7\sigma_7}$. Since $(M^* - 1)/16 = (\pm h) \cdot 2^{n-4}$, this gives

$$\alpha_2^{\pm h \cdot 2^{n-4}} \equiv -1 \pmod{M}.$$

Similarly as above, we have $\alpha_2^{h \cdot 2^{n-4}} + \bar{\alpha}_2^{h \cdot 2^{n-4}} \equiv -2 \pmod{M}$. Let $\eta_{n-4} = \alpha_2^{h \cdot 2^{n-4}} + \bar{\alpha}_2^{h \cdot 2^{n-4}}$, we find $\mathrm{Tr}_{K_2/\mathbb{Q}}(\eta_{n-4}) \equiv -8 \pmod{M}$, $\mathrm{Nm}_{K_2/\mathbb{Q}}(\eta_{n-4}) \equiv 16 \pmod{M}$, $S_2(\eta_{n-4}, \sigma_3(\eta_{n-4}), \sigma_5(\eta_{n-4}), \sigma_7(\eta_{n-4})) \equiv 24 \pmod{M}$, and $S_3(\eta_{n-4}, \sigma_3(\eta_{n-4}), \sigma_5(\eta_{n-4}), \sigma_7(\eta_{n-4})) \equiv -32 \pmod{M}$. By Proposition 4.4, this is equivalent to $X_{n-4} \equiv -8 \pmod{M}$, $W_{n-4} \equiv 16 \pmod{M}$, $Y_{n-4} \equiv 24 \pmod{M}$ and $Z_{n-4} \equiv -32 \pmod{M}$. This completes the proof of necessity.

We now turn to the proof of sufficiency. Let q be an arbitrary prime divisor of M. It suffices to prove that any one of the possible congruences on the generalized Lucasian sequence $\{(T_k, N_k)\}$ or $\{(X_k, Y_k, Z_k, W_k)\}$ could imply that $q > \sqrt{M}$.

Assuming one of the first three hypotheses on the sequence $\{(T_k, N_k)\}$ is satisfied. The hypotheses imply that q is prime to 17, so applying Lemma 4.5 with $\alpha = (\pi_1/\bar{\pi}_1)^{h(1+3\sigma_3)}$, we can obtain $q^2 \equiv 1 \pmod{2^{n-2}}$. If the last hypothesis on the sequence $\{(X_k, Y_k, Z_k, W_k)\}$ is satisfied, then $q \neq 17$, and applying Lemma 4.6 with $\alpha = (\pi_2/\bar{\pi}_2)^{h(1+3\sigma_{-5}+5\sigma_{-3}+7\sigma_7)}$, we would obtain $q^4 \equiv 1 \pmod{2^{n-3}}$. From these congruences we always get $q^4 \equiv 1 \pmod{2^{n-3}}$. By the hypothesis that M is not divisible by any of the solutions of $x^4 \equiv 1 \pmod{2^{n-3}}$ in the range $(1, 2^{n-3})$, it follows easily that in all cases $q \geq 2^{n-3} + 1$, whence $q^2 \geq 2^{2n-6} + 2^{n-2} + 1 = 2^n(2^{n-6} + \frac{1}{4}) + 1 > h \cdot 2^n + 1 \geq M$ because of $h < 2^{n-6}$. Thus $q > \sqrt{M}$ for arbitrary prime divisor q of M, clearly M is prime. This completes the proof of sufficiency, and hence the proof of Theorem 3.1. □

5. Computational complexity

By Theorem 3.1, we obtain a fast deterministic algorithm for testing the primality of numbers $M = h \cdot 2^n \pm 1$, where $0 < h < 2^{n-6}$ is odd, $h \not\equiv 0 \pmod{17}$ and $n \geq 7$. The algorithm can be divided into three steps:

Step 1. We determine if M is divisible by one of the solutions of $x^4 \equiv 1 \pmod{2^{n-3}}$ in the range $1 < x < 2^{n-3}$. Actually, all these solutions are given by $Q_j \equiv 5^{j2^{n-7}} \pmod{2^{n-3}}$, $j = 1, 2, 3$ and $Q_{j+4} \equiv -5^{j2^{n-7}} \pmod{2^{n-3}}$, $j = 0, 1, 2, 3$. Thus complexity of step 1 is that of 3 modular exponentiations of $5^{j2^{n-7}} \pmod{2^{n-3}}$, which is $\tilde{O}(\log^2 M)$ bit operations by applying Schoenhage-Strassen algorithm (see [7]). Note that $n = O(\log M)$ and $\tilde{O}(f)$ stands for $O(f \cdot \mathrm{Poly}(\log f)) \subset O(f^{1+\varepsilon})$ for any function f and any positive real number $\varepsilon > 0$, where $\mathrm{Poly}(\log f)$ indicates some polynomial in $\log f$.

Step 2. If $M^* \not\equiv -1 \pmod{17}$, then we compute the generalized Lucasian sequence $\{(T_k \pmod{M}, N_k \pmod{M})\}$ to see that if one of the first three congruences is satisfied. Complexity of computing the seed $(T_0 \pmod{M}, N_0 \pmod{M})$ is equivalent to that of computing $\alpha_1^h + \bar{\alpha_1}^h \pmod{M}$. Let $\beta_j = \alpha_1^j + \bar{\alpha_1}^j$. Since $\alpha_1 \bar{\alpha_1} = 1$, we easily get the relations $\beta_{i+j} = \beta_i \beta_j - \beta_{i-j}$ for $i \geq j \geq 0$. Thus $\beta_h = \alpha_1^h + \bar{\alpha_1}^h$ can be deduced from $\beta_0 = 2,\ \beta_1 = \alpha_1 + \bar{\alpha_1}$ by two recurrent relations:

$$\beta_{2j} = \beta_j^2 - 2,\ \beta_{2j+1} = \beta_j \beta_{j+1} - \beta_1,$$

where $\alpha_1 = (\pi_1/\bar{\pi_1})^{1+3\sigma_3}$ is the same as in Theorem 3.1. Thus complexity of computing $\beta_h \pmod{M}$ is $\tilde{O}(\log h \log M) = \tilde{O}(\log M)$, since h is fixed in advance. Next, the term $(T_{n-3} \pmod{M}, N_{n-3} \pmod{M})$ can be deduced from $(T_0 \pmod{M}, N_0 \pmod{M})$ by the recurrences (3.1) and (3.2), and the complexity of computing these is $\tilde{O}(\log^2 M)$. Hence the total complexity of step 2 is $\tilde{O}(\log^2 M)$ bit operations.

Step 3. If $M^* \equiv -1 \pmod{17}$, then we compute the generalized Lucasian sequence $\{(X_k \pmod{M}, Y_k \pmod{M}, Z_k \pmod{M}, W_k \pmod{M})\}$, to see that if the last congruence is satisfied. Similarly, complexity of computing the seed $(X_0 \pmod{M}, Y_0 \pmod{M}, Z_0 \pmod{M}, W_0 \pmod{M})$ is equivalent to that of computing $\alpha_2^h + \bar{\alpha_2}^h \pmod{M}$, hence the complexity is $\tilde{O}(\log M)$ as in Step 2, where $\alpha_2 = (\pi_2/\bar{\pi_2})^{1+3\sigma_{-5}+5\sigma_{-3}+7\sigma_7}$ is the same as in Theorem 3.1. And the term $(X_{n-4} \pmod{M}$, $Y_{n-4} \pmod{M}$, $Z_{n-4} \pmod{M}$, $W_{n-4} \pmod{M})$ can be deduced from the seed $(X_0 \pmod{M}$, $Y_0 \pmod{M}$, $Z_0 \pmod{M}$, $W_0 \pmod{M})$ by the recurrences (3.3), (3.4), (3.5) and (3.6). Thereby, the total complexity of step 3 is $\tilde{O}(\log^2 M)$ bit operations.

According to the above analysis, our generalized Lucasian primality test for numbers $M = h \cdot 2^n \pm 1$ (where $h \not\equiv 0 \pmod{17}$) runs in deterministic quasi-quadratic time, that is, the computational complexity of this test is only $\tilde{O}(\log^2 M)$ bit operations.

6. Conclusion and an open problem

Theorem 3.1 together with previous results (given by Bosma, Berrizbeitia and Berry, etc.) have solved the problem of primality testing of numbers $M_{h,n} = h \cdot 2^n \pm 1$ for the cases of $h \not\equiv 0 \pmod 3$, $h \not\equiv 0 \pmod 5$ and $h \not\equiv 0 \pmod{17}$, by means of at most two generalized Lucasian sequences with at most two seeds which depend only on h (not on n). It's natural to ask if such generalized Lucasian primality tests exist for other values of h. Will the Eisenstein's Reciprocity Laws of other order help to obtain the suitable tests for the family of numbers $M_{h,n} = h \cdot 2^n \pm 1$ with n increasing? We propose an opened problem below, which is the question that we expect to solve in the future.

Open Problem. Given arbitrary odd h, for all n large enough, does there exist a generalized Lucasian primality test for the family of numbers $M_{h,n} = h \cdot 2^n \pm 1$ with finitely many seeds which depend only on h (not on n)?

References

[1] B. C. Berndt, R. J. Evans & K. S. Williams, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons, Inc., New York, 1998, A Wiley-Interscience Publication, xii+583 pages.

[2] P. Berrizbeitia & T. G. Berry, "Biquadratic reciprocity and a Lucasian primality test", *Math. Comp.* **73** (2004), no. 247, p. 1559-1564 (electronic).

[3] W. Bosma, "Explicit primality criteria for $h \cdot 2^k \pm 1$", *Math. Comp.* **61** (1993), no. 203, p. 97-109, S7-S9.

[4] K. Ireland & M. Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990, xiv+389 pages.

[5] D. H. Lehmer, "On Lucas's Test for the Primality of Mersenne's Numbers", *J. London Math. Soc.* **10** (1935), no. 3, p. 162-165.

[6] E. Lucas, "Théorie des Fonctions Numériques Simplement Périodiques. [Continued]", *Amer. J. Math.* **1** (1878), no. 2, 3 and 4, p. 184-196, 197-240 and 289-321.

[7] A. Schönhage & V. Strassen, "Schnelle Multiplikation grosser Zahlen", *Computing (Arch. Elektron. Rechnen)* **7** (1971), p. 281-292.

[8] L. C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997, xiv+487 pages.

Yingpu Deng
Key Laboratory of Mathematics Mechanization, NCMIS
Academy of Mathematics and Systems Science
Chinese Academy of Sciences
Beijing 100190, P.R. China
E-mail: dengyp@amss.ac.cn

Dandan Huang
(corresponding author)
Laboratory of Information Security
School of Software Engineering
Jinling Institute of Technology
Nanjing 211169, P.R. China
Key Laboratory of Mathematics Mechanization, NCMIS
Academy of Mathematics and Systems Science
Chinese Academy of Sciences
Beijing 100190, P.R. China
E-mail: huangdd@jit.edu.cn