PRIMALITY PROVING USING ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION BY IMAGINARY QUADRATIC FIELDS OF CLASS NUMBER THREE

HIROSHI ONUKI

Abstract. In 2015, Abatzoglou, Silverberg, Sutherland, and Wong presented a framework for primality proving algorithms for special sequences of integers using an elliptic curve with complex multiplication. They applied their framework to obtain algorithms for elliptic curves with complex multiplication by imaginary quadratic field of class numbers one and two, but, they were not able to obtain primality proving algorithms in cases of higher class number. In this paper, we present a method to apply their framework to imaginary quadratic fields of class number three. In particular, our method provides a more efficient primality proving algorithm for special sequences of integers than the existing algorithms by using an imaginary quadratic field of class number three in which 2 splits. As an application, we give two special sequences of integers derived from $\mathbb{Q}(\sqrt{-23})$ and $\mathbb{Q}(\sqrt{-31})$, which are all the imaginary quadratic fields of class number three in which 2 splits. Finally, we give a computational result for the primality of these sequences.

1. Introduction

Research on algorithms to determine the primality of a given integer has received a lot of interest from computational mathematics and its application to cryptography. There are efficient algorithms for compositeness test, which return the input is composite or undetermined. For example, the Miller-Rabin test [6, Algorithm 3.5.1] has computational complexity $\tilde{O}((\log n)^2)$ with input $n$. However, primality proving algorithms, which determine the primality of the input, are less efficient. The best algorithm currently known is the Agrawal-Kayal-Saxena algorithm [4] improved by Lenstra and Pomerance [9] and has computational complexity $\tilde{O}((\log n)^6)$ with input $n$.

On the other hand, more efficient algorithms are known for an integer $n$ such that a partial factorization of either $n + 1$ or $n - 1$ is known (see §4.1 and 4.2 of [6]). For example, the Lucas-Lehmer test for Mersenne numbers [6, Theorem 4.2.6] and the Pepin test for Fermat numbers [6, Theorem 4.1.2] are such algorithms. The computational complexities of these algorithms are $\tilde{O}((\log n)^2)$ the same as for the Miller-Rabin test. These classical algorithms (we call these the $n \pm 1$ algorithms) use the structure of the multiplicative group of the residue ring modulo $n$.

In 2005, Gross [8] constructed a primality proving algorithm for Mersenne numbers by using an elliptic curve with complex multiplication (CM) by $\mathbb{Q}(\sqrt{-1})$. Its computational complexity is also $\tilde{O}((\log n)^2)$ with input $n$. Similar results for other sequences of integers are obtained by Denomme and Savin [7] for Fermat numbers and integers of the forms $3^{2^l} - 3^{2^{l-1}} + 1$ and $2^{2^l} - 2^{2^{l-1}} + 1$, and by Tsumura [17]
for integers of the form $2^p \pm 2^{(p+1)/2} + 1$. Denomme and Savin used elliptic curves with CM by $\mathbb{Q}(\sqrt{-7})$ and $\mathbb{Q}(\sqrt{-15})$, and Tsunura used an elliptic curve with CM by $\mathbb{Q}(\sqrt{-11})$. However, an integer $N$ to which these algorithms can be applied has the property that $N + 1$ or $N - 1$ is smooth, i.e., the $n \pm 1$ algorithms can also be applied to such $N$.

Based on these studies, Abatzoglou, Silverberg, Sutherland and Wong [2] proposed a primality proving algorithm for sequences of integers to which the $n \pm 1$ algorithms cannot be applied (see also [19]). Their algorithm has the same computational complexity as the above algorithms. The same authors [3] presented a framework for primality proving algorithms using elliptic curves with CM. If one applies their framework to elliptic curves with CM by an imaginary quadratic field in which 2 splits, i.e., 2 splits into two distinct prime ideals, then one can obtain a primality proving algorithm for sequences of integers to which the $n \pm 1$ algorithms cannot be applied. As an application of their framework, they gave a primality proving algorithm for sequences of integers using $\mathbb{Q}(\sqrt{-7})$ and $\mathbb{Q}(\sqrt{-15})$, which are all the imaginary quadratic fields of class number one or two in which 2 splits. A primality proving algorithm using $\mathbb{Q}(\sqrt{-2})$ based on the same framework was also proposed by [11][3]. However, the $n \pm 1$ algorithm can be applied to the sequence of integers to which the algorithm using $\mathbb{Q}(\sqrt{-2})$ can be applied since 2 is ramified in $\mathbb{Q}(\sqrt{-2})$. The algorithm using $\mathbb{Q}(\sqrt{-15})$ is the first algorithm of this type using an imaginary quadratic field of class number two (the previous algorithms use those of class number one). They left as an open problem the construction of a similar primality proving algorithm using an imaginary quadratic field of class number greater than two (see Remark 4.12 in [3]). The main obstacle to use an imaginary quadratic field of class number greater than two is as follows. Let $K$ be an imaginary quadratic field and $H$ the Hilbert class field of $K$. The framework of Abatzoglou et al. uses a sequence $\{p_k\}_k$ of ideals of $\mathcal{O}_H$ such that $N_{H/K}(p_k)$ is principal and a generator $\pi_k$ of $N_{H/K}(p_k)$ satisfying that $\pi_k - 1$ is “highly factored,” i.e., $\pi_k - 1$ is divisible by a smooth $\alpha \in \mathcal{O}_K$ and $N_{K/\mathbb{Q}}(\alpha)$ is approximately greater than $\sqrt{N_{K/\mathbb{Q}}(\pi_k)}$, and they did not know how to systematically find such ideals.

In this paper, we solve this problem in the case that the class number is three. Our method is based on the framework of Abatzoglou et al. and can be applied to any imaginary quadratic field of class number three in which 2 splits. As in the framework of Abatzoglou et al., we can obtain a primality proving algorithm for a special sequence of integers to which the $n \pm 1$ algorithms cannot be applied.

Let $K$ be an imaginary quadratic field of class number three and $H$ the Hilbert class field of $K$. The key idea of this work is using a primitive element $\xi$ of $H/K$ such that $\text{Tr}_{H/K}(\xi) = 0$. In this case, the minimal polynomial of $\xi$ over $K$ is of the form $x^3 + c_1 x + c_0$ for $c_0, c_1 \in \mathcal{O}_K$. We define a sequence $\{p_k\}_k$ of ideals of $\mathcal{O}_H$ as $p_k = (1 - \alpha^k \xi)\mathcal{O}_H$ for a smooth $\alpha \in \mathcal{O}_K$. Then $N_{H/K}(p_k)$ is principal and generated by $\pi_k = 1 + c_1 \alpha^{2k} + c_0 \alpha^k$ and $\pi_k - 1 = \alpha^{2k}(c_1 + c_0 \alpha^k)$ is highly factored.

As an application, we present two sequences of integers and primality proving algorithms for them. These algorithms use $\mathbb{Q}(\sqrt{-23})$ and $\mathbb{Q}(\sqrt{-31})$, respectively, which are all the imaginary quadratic fields of class number three in which 2 splits (see sequence A006203 in [10]).

The organization of this paper is as follows. In §4 we give the notation that we use in this paper. We recall the framework of $\mathbb{Q}$ in §5. Our main contribution is given in §4.1. In particular, we present our idea to solve the open problem in §4.1.
Then, in §4.2 we give the setting of our primality proving. We deal with some technical issues to construct our algorithm in §4.3. Our concrete algorithm is given in §4.4. Finally, in §5 we show the computational result of our primality proving algorithm.

2. Notation

Let $L$ be a number field. We denote the ring of integers of $L$ by $O_L$. The norm and the trace of a finite extension $M/L$ are denoted by $N_{M/L}$ and $\text{Tr}_{M/L}$, respectively. For a place $v$ of $L$, we denote the completion of $L$ at $v$ by $L_v$. For a finite place $\mathfrak{p}$ of $L$ and $a \in L_{\mathfrak{p}}$, we denote the $\mathfrak{p}$-adic valuation of $a$ by $\text{ord}_{\mathfrak{p}}(a)$. For $a, b \in L_v^*$, the quadratic Hilbert symbol $\left( \frac{a, b}{v} \right)$ at $v$ is defined by

$$\left( \frac{a, b}{v} \right) = \begin{cases} 1, & \text{if } ax^2 + by^2 = z^2 \text{ has a solution } (x, y, z) \in L_v^3 \setminus (0, 0, 0), \\ -1, & \text{otherwise}. \end{cases}$$

For a finite place $p$ of $L$ not dividing 2, we define the quadratic residue symbol modulo $p$ as

$$\left( \frac{a}{p} \right) = \begin{cases} \left( \frac{\pi a}{p} \right), & \text{if } \text{ord}_p(a) \text{ is even,} \\ 0, & \text{otherwise}, \end{cases}$$

where $a \in L_p^*$ and $\pi$ is a prime element of $L_p$. Note that this definition does not depend on the choice of $\pi$. If $\text{ord}_p(a) = 0$ then $\left( \frac{a}{p} \right) = 1$ if and only if $a$ is square modulo $p$. For an element $a$ of an imaginary quadratic field, $\bar{a}$ denotes the complex conjugate of $a$.

In this paper, we consider only elliptic curves defined by a short Weierstrass form, i.e., curves defined by a projective equation $Y^2Z = X^3 + AXZ^2 + BZ^3$, where $A$ and $B$ are the coefficients of the curve. For simplicity, we also use the affine model $y^2 = x^3 + Ax + B$ of the same curve. For an elliptic curve $E$, we denote its neutral element by $O_E$, its $j$-invariant by $j(E)$, its discriminant by $\text{disc}(E)$, and its endomorphism ring by $\text{End}(E)$. Note that $O_E$ is the unique point whose $Z$-coordinate is zero. Let $\mathcal{O}$ be an order of an imaginary quadratic field and $E$ an elliptic curve over a number field. When $\text{End}(E)$ is isomorphic to $\mathcal{O}$, we say $E$ is an elliptic curve with complex multiplication (CM) by $\mathcal{O}$. In this case, the normalized isomorphism $\mathcal{O} \to \text{End}(E)$ is denoted by $[\cdot]$ (see [14] Proposition II.1.1) for the definition.

3. Framework for primality proving

In this section, we give an overview of the framework provided in [3]. First, we recall terminology from [3].

Definition 3.1. Let $E$ be an elliptic curve over a number field $M$ and $J$ an ideal of $O_M$ prime to $\text{disc}(E)$. We say that $P \in E(M)$ is strongly nonzero modulo $J$ if one can express $P = (X : Y : Z) \in \mathbb{P}^2(O_M)$ such that $ZO_M + J = O_M$.

Let $K$ be an imaginary quadratic field, $E$ an elliptic curve defined over a number field $M$ containing $K$ with CM by $O_K$. We fix a point $P$ in $E(M)$. Let $\gamma, \alpha_1, \ldots, \alpha_s$ be nonzero elements of $O_K$ and assume that we know the prime ideal factorization of $(\prod_{i=1}^s \alpha_i)O_K$. For $k = (k_1, \ldots, k_s) \in \mathbb{N}^s$, we define

$$\Lambda_k = \gamma \alpha_1^{k_1} \cdots \alpha_s^{k_s}, \quad \pi_k = 1 + \Lambda_k, \quad F_k = N_{K/\mathbb{Q}}(\pi_k),$$

where $N_{K/\mathbb{Q}}$ denotes the norm of $K/\mathbb{Q}$.
and $L_k$ as the positive generator of an ideal $(\Lambda_k/\gamma)\mathcal{O}_K \cap \mathbb{Z}$ of $\mathbb{Z}$. Let $p_k$ be an ideal of $\mathcal{O}_K$ such that $N_{M/\mathbb{Q}}(p_k) = \pi_k\mathcal{O}_K$. When $p_k$ is a prime ideal, we denote the reductions modulo $p_k$ of $E$ and $P$ by $\bar{E}$ and $\bar{P}$. Further, we adopt the assumption described in §3.1 of [3]. In particular, we assume that $k$ is chosen so that the following holds.

**Assumption 3.2.** Whenever $p_k$ is a prime ideal, the following hold:

(i) The Frobenius endomorphism of $\bar{E}$ is $[\pi_k]$,
(ii) $\bar{P} \notin [\lambda]\bar{E}(\mathcal{O}_M/p_k)$ for every prime ideal $\lambda$ of $\mathcal{O}_K$ containing $\prod_{i=1}^{s} \alpha_i$.

In this setting, Abatzoglou et al. showed the following primality theorem.

**Theorem 3.3** (Theorem 3.6 of [3]). With the notation as above, assume Assumption 3.2. Suppose that $\prod_{i=1}^{s} \alpha_i$ is not divisible in $\mathcal{O}_K$ by any rational prime that splits in $K$, and that $F_k > 16N_{K/\mathbb{Q}}(\gamma \prod \lambda)^2$ where $\lambda$ runs over the prime ideals of $\mathcal{O}_K$ that divide $\prod_{i=1}^{s} \alpha_i$ and are ramified in $K/\mathbb{Q}$. Then the following are equivalent:

(a) $p_k$ is a prime ideal,
(b) $[L_k\gamma]P \equiv O_E \pmod{p_k}$, and $\left[\frac{L_k\gamma}{P}\right]P$ is strongly nonzero modulo $p_k$ for every prime divisor $p$ of $N_{K/\mathbb{Q}}(\alpha_1 \cdots \alpha_s)$.

This theorem states that the primality of $p_k$ can be detected by the arithmetic of $P$ modulo $p_k$. The condition $F_k > 16N_{K/\mathbb{Q}}(\gamma \prod \lambda)^2$ means that the unknown part of the factorization of $\pi_k - 1$ is less than about half of the size of $\pi_k$. This and condition (ii) in Assumption 3.2 ensure that $P$ mod $p_k$ has a sufficiently large order to prove the primality of $p_k$. Although $\gamma$ does not depend on $k$ in [3], the proof does not use this fact. Therefore, Theorem 3.3 remains true even if $\gamma$ depends on $k$.

Abatzoglou et al. obtained an algorithm for determining the primality of $p_k$ from this theorem. To make the above theorem a concrete primality proving algorithm, we must choose a setting that satisfies Assumption 3.2.

As in [3], for condition (i), we can use Theorem 5.3 of [12]. Suppose that $E$ is defined by $y^2 = x^3 + Ax + B$ and the discriminant of $K$ is odd. Then the theorem says that the Frobenius map of $E$ is

$$\gamma_3(E) \in H$$

where $\gamma_3(E)$ is the value of a Weber function at a complex number corresponding to $E$ (see §2 in [12] for the definition), and $\epsilon_k$ is $\pm 1$ depending on $\pi_k^3 \pmod{4}$ (see Proposition 6.2 in [12]).

For condition (ii), Abatzoglou et al. showed the following theorem.

**Theorem 3.4** (Theorem 4.4 of [3]). Let $\lambda$ be a prime ideal of $\mathcal{O}_K$ such that $p_k$ does not divide $N_{K/\mathbb{Q}}(\lambda)$, and $\varphi : E \to E'$ an isogeny with kernel $E[\pi]$. Let $P \in E(M)$, $F = M(E'[\lambda])$, and $L = F(\bar{\varphi}^{-1}(P))$, where $\bar{\varphi}$ is the dual isogeny of $\varphi$. If $p_k$ is a prime ideal then the following are equivalent:

(a) $\bar{P} \notin [\lambda]\bar{E}(\mathcal{O}_M/p_k)$,
(b) $p_k$ splits completely in $F$ and $p_k$ does not split completely in $L$.

To determine the condition on $k$ satisfying (b) of this theorem, they restrict their attention to the case $M = F$ and this field is the Hilbert class field of $K$. This
restriction makes \( \lambda \) an ideal above 2 except in the case \( K = \mathbb{Q}(\sqrt{-3}) \). For a detailed discussion, see §4 in [3].

In order to construct a primality proving algorithm for numbers to which the \( n \pm 1 \) algorithms cannot be applied, we need to restrict \( K \) to a field in which 2 splits. Otherwise, \( F_k - 1 \) is highly factored. The imaginary quadratic fields in which 2 splits of class number one or two are \( \mathbb{Q}(\sqrt{-7}) \) and \( \mathbb{Q}(\sqrt{-15}) \). A primality proving algorithm for \( \mathbb{Q}(\sqrt{-7}) \) was given by [2] and one for \( \mathbb{Q}(\sqrt{-15}) \) by [3].

4. Primality Proof for class number three

In this section, we give a method to construct a primality proving algorithm for imaginary quadratic fields of class number three in which 2 splits. In particular, we give a systematic method for constructing \( p_k \) such that \( \pi_k - 1 \) is highly factored.

4.1. Construction of \( p_k \). Let \( K \) be an imaginary quadratic field and \( H \) the Hilbert class field of \( K \). As in the previous section, we let \( p_k \) be an ideal of \( \mathcal{O}_H \), \( \pi_k \) a generator of \( N_{H/K}(p_k) \), and \( F_k = N_{K/Q}(\pi_k) \) for \( k \in \mathbb{N} \). In this setting, “\( \pi_k - 1 \) is highly factored” means that \( \pi_k - 1 \) is of the form \( A\gamma \) satisfying \( A \) is divisible only by a prime ideal of \( \mathcal{O}_K \) above 2, and \( F_k > 16N_{K/Q}(\gamma)^2 \). The latter condition comes from Theorem [3,3].

First, we consider a more general setting. Let \( h \) be the class number of \( K \) and \( \xi \in \mathcal{O}_H \) a primitive element of \( H/K \), i.e., \( H = K(\xi) \). We can write the minimal polynomial \( f(x) \) of \( \xi \) over \( K \) as

\[
f(x) = x^h + c_m x^m + \cdots + c_0, \quad c_0, \ldots, c_m \in \mathcal{O}_K \quad \text{and} \quad m < h.
\]

Let \( \alpha \) be an element in \( \mathcal{O}_K \) such that \( \alpha \) is divisible only by a prime ideal of \( \mathcal{O}_K \) above 2. We define \( p_k \) as an ideal generated by \( 1 - \alpha k \xi \). Then we have

\[
\pi_k = N_{H/K}(1 - \alpha k \xi) = \alpha^{kh} N_{H/Q}(\alpha^{-k} - \xi) = \alpha^{kh} f(\alpha^{-k}) = 1 + c_m \alpha^{(h-m)k} + c_{m-1} \alpha^{(h-(m-1))k} + \cdots + c_0 \alpha^{mk} = 1 + \alpha^{(-m)k}(c_m + c_{m-1} \alpha + \cdots + c_0 \alpha^{mk}).
\]

In this case, if \( m < h/2 \) then the norm condition in Theorem [3,3] holds. More precisely, we have the following lemma.

**Lemma 4.1.** We use the above notation and assume \( m < h/2 \). Let \( \gamma_k = c_m + c_{m-1} \alpha + \cdots + c_0 \alpha^{mk} \). Then we have \( F_k > 16N_{K/Q}(\gamma_k)^2 \) for sufficiently large \( k \).

**Proof.** It suffices to show that \( \lim_{k \to \infty} N_{K/Q}(\gamma_k)^2/F_k = 0 \). Since \( \alpha \) is divisible by a prime ideal above 2, we have \( N_{K/Q}(\alpha) \geq 2 \). Therefore, the limit of a complex number \( \pi_k/\alpha^{hk} = c_0 + c_1 \alpha^{-k} + \cdots + c_m \alpha^{-mk} + \alpha^{-hk} \) as \( k \) approaches infinity equals \( c_0 \). On the other hand, the condition \( m < h/2 \) shows \( \lim_{k \to \infty} \gamma_k/\alpha^{hk/2} = 0 \). Taking the norms of these limits shows that

\[
\lim_{k \to \infty} F_k/N_{K/Q}(\alpha)^{hk} = c_0^2 \quad \text{and} \quad \lim_{k \to \infty} N_{K/Q}(\gamma_k)^2/N_{K/Q}(\alpha)^{hk} = 0.
\]

Since \( c_0 \neq 0 \), we have \( \lim_{k \to \infty} N_{K/Q}(\gamma_k)^2/F_k = 0 \).

As we stated in [3], the framework also works in the case \( \gamma \) depends on \( k \). Therefore, if we find \( \xi \) with \( m < h/2 \) then we can apply the primality proving in [3]. For general class numbers, we do not know how to find such \( \xi \). However, in the
case that the class number of \( K \) is three, we can always find such \( \xi \) by taking a trace-zero element.

**Remark 4.2.** We can construct a primality proving algorithm for a generator of the form \( 1 - \beta \alpha^k \xi \) of \( \mathfrak{p}_k \) with cofactor \( \beta \in \mathcal{O}_K \) in the same way as described in the following sections. In this paper, we describe the case \( \beta = 1 \) to simplify the notation.

4.2. **Settings.** We use the notation in the previous subsection. Suppose that the class number of \( K \) is three and that 2 splits in \( K \). We choose a primitive element \( \xi \) of \( H/K \) so that the trace of \( \xi \) is zero, i.e., the minimal polynomial of \( \xi \) over \( K \) is \( x^3 + c_1 x + c_0 \). Let \( \lambda \) be a prime ideal of \( \mathcal{O}_K \) above 2, and \( \alpha \) a generator of \( \lambda^3 \). For \( k \in \mathbb{N} \), we define \( p_k = 1 - \alpha^k \xi \) and \( \mathfrak{p}_k \) is the ideal of \( \mathcal{O}_H \) generated by \( p_k \). In summary, our setting is

\[
\mathfrak{p}_k = p_k \mathcal{O}_H = (1 - \alpha^k \xi) \mathcal{O}_H, \\
\pi_k = N_{H/K}(p_k) = 1 + c_1 \alpha^{2k} + c_0 \alpha^{3k}, \\
F_k = N_{K/Q}(\pi_k).
\]

Our goal is to construct a primality proving algorithm for \( F_k \) by using an elliptic curve with CM by \( \mathcal{O}_K \). For this, we choose \( \xi \) so that \( F_k \) is a prime number if \( \mathfrak{p}_k \) is a prime ideal since the primality of \( \mathfrak{p}_k \) can be determined by Theorem 3.3. The following lemma gives such a condition on \( \xi \).

**Lemma 4.3.** Let \( t \) be the trace of \( \alpha \). Suppose that \( 1 + c_1 + c_0 \) and \( 1 + c_1 + c_0 t \) are not congruent to \( 1 \) modulo \( \lambda^3 \). Then \( \mathfrak{p}_k \) is a prime ideal if and only if \( F_k \) is a prime number.

**Proof.** First, we show that if \( \mathfrak{p}_k \) is a prime ideal then \( \pi_k \mathcal{O}_K \) is a prime ideal. Let \( \kappa \) be a prime ideal dividing \( \pi_k \mathcal{O}_K \) in \( K \). Because the minimal polynomial \( x^3 + c_1 x + c_0 \) of \( \xi \) has a root \( \alpha^{-k} \) modulo \( \pi_k \mathcal{O}_K \), there exists a prime ideal above \( \kappa \) in \( H \) whose inertia degree over \( \kappa \) is one. From this and the fact that \( H \) is the Hilbert class field of \( K \), it follows that \( \kappa \) splits completely in \( H \). Therefore, if \( \mathfrak{p}_k \) is prime then the inertia degree of \( \mathfrak{p}_k \) over \( K \) is one. This means that \( \pi_k \), the norm of \( \mathfrak{p}_k \) over \( K \), is prime in \( K \).

Next, we show that if \( \pi_k \mathcal{O}_K \) is a prime ideal then \( F_k \) is a prime number. Suppose that \( \pi_k \mathcal{O}_K \) is a prime ideal. We assume that \( F_k \) is not prime. Then \( F_k \) is the square of a rational prime. Therefore, we have \( F_k \equiv 1 \pmod{8} \) or \( F_k \equiv 2^2 \). The latter case occurs only when 2 is inert in \( K \), so \( \alpha \) is divisible by 2. In this case, \( F_k \) must be odd. This contradicts the fact that \( F_k = 2^2 \). Therefore, we conclude that \( F_k \equiv 1 \pmod{8} \). Since \( \pi_k \equiv 1 \pmod{\lambda^3} \), we have \( F_k \equiv \pi_k \pmod{\lambda^3} \). This implies that \( \pi_k \equiv 1 \pmod{\lambda^3} \). On the other hand, we have

\[
\pi_k \equiv 1 + c_1 t^{2k} + c_0 t^{3k} \pmod{\lambda^3}
\]

since \( \alpha \equiv t \pmod{\lambda^3} \). Since \( t \) is odd and \( \lambda^3 \) divides 8, it follows that \( \pi_k \) is congruent to \( 1 + c_1 + c_0 \) or \( 1 + c_1 + c_0 t \) modulo \( \lambda^3 \) depending on whether \( k \) is even or odd. This contradicts our assumption. Therefore, \( F_k \) must be prime.

The other direction is obvious. \( \square \)

From now on, we restrict our attention to \( \xi \) satisfying the assumption in Lemma 4.3. We can find such \( \xi \) for any imaginary quadratic field of class number three in which 2 splits. There are exactly two such quadratic fields, \( \mathbb{Q}(\sqrt{-23}) \) and \( \mathbb{Q}(\sqrt{-31}) \).
We can take $\xi$ as a root of $x^3 - x - 1$ for $\mathbb{Q}(\sqrt{-23})$ and a root of $x^3 + x + 1$ for $\mathbb{Q}(\sqrt{-31})$.

The remaining tasks are to find an elliptic curve and a point on it and to determine the condition on $k$ satisfying Assumption $\star$.

### 4.3. Determining the condition on $k$

We can use the method in $\star$ to determine the condition on $k$, but the authors described methods for searching conditions on $k$ separately for each form of $F_k$. Here, we give a slightly more unified method and explicit algorithms for this.

Let $E$ be an elliptic curve with CM by $O_K$ defined by $y^2 = x^3 + Ax + B$ with $A, B \in O_H$. We can suppose that $B$ is square in $O_H$ since $y^2 = x^3 + Au^2x + Bu^3$ is isomorphic to $E$ for any $u \in H^\times$. We suppose that $B$ is square and let $\beta$ be a square root of $B$. Then $(0, \beta)$ is a point in $E(H)$. We let $P = (0, \beta)$. As in $\star$ when $p_k$ is a prime ideal, we denote the reductions modulo $p_k$ of $E$ and $P$ by $E$ and $P$.

The purpose of this subsection is to give a method to compute sets $T_0$, $T_1$, and $T_2$ satisfying the following conditions:

- $T_0 = \{ k \in \mathbb{N} \mid p_k \text{ does not divide } \text{disc}(E) \}$,
- $k \in T_1$ and $p_k$ is a prime ideal $\implies$ (i) of Assumption $\star$ holds,
- $k \in T_2$ and $p_k$ is a prime ideal $\implies$ (ii) of Assumption $\star$ holds.

We can apply Theorem $\star$ to $k \in T_0 \cap T_1 \cap T_2$ and obtain a primality proving algorithm. In the following, we show that these sets are determined by the condition on $k$ modulo some integer. Determining $T_0$ is trivial, so we focus on $T_1$ and $T_2$ in the following. First, we show that quadratic residue symbols modulo $p_k$ are determined by $k$ modulo some integers. Next, we show that we can define $T_1$ and $T_2$ as sets of integers satisfying conditions on quadratic residue symbols. Finally, we give explicit algorithms to determine $T_1$ and $T_2$.

### 4.3.1. Computing quadratic residue symbols

To determine quadratic residue symbols modulo $p_k$, we use the following theorem.

**Theorem 4.4.** Fix $a \in H^\times$. For a prime ideal $\mathfrak{l}$ of $O_H$, we denote the order of $(O_H/\mathfrak{l})^\times$ by $N_\mathfrak{l}$. Then the quadratic residue symbol $\left( \frac{a}{\mathfrak{l}} \right)$ is determined by $k$ modulo the least common multiple of 2 and $N_\mathfrak{l}$ for the prime ideals $\mathfrak{l}$ of $O_H$ dividing $a$ and not dividing 2.

To prove this theorem, we need the following lemmas.

**Lemma 4.5.** Let $L$ be a number field in which 2 is not ramified, and $\mathfrak{l}$ a prime ideal of $O_L$ above 2. We fix an element $a$ in $L^\times$. Then, for $b \in O_L$ not divisible by $\mathfrak{l}$, the quadratic Hilbert symbol $\left( \frac{a}{\mathfrak{l}} \right)$ is determined by $b$ modulo $\mathfrak{l}^3$.

**Proof.** We may assume that $\text{ord}_\mathfrak{l}(a) = 0$ or 1. Let $O_\mathfrak{l}$ be the valuation ring of $L_\mathfrak{l}$. It suffices to show that $\left( \frac{a}{\mathfrak{l}} \right) = 1$ if and only if $ax^2 + by^2 \equiv z^2 \pmod{\mathfrak{l}^3}$ has a solution $(x, y, z)$ in $O_\mathfrak{l}^\times$ such that at least one of $x, y, z$ is in $O_\mathfrak{l}^\times$.

It is obvious that the former implies the latter. Suppose that the latter holds. Let $(x_0, y_0, z_0)$ be a solution of the equation in the latter. If $\text{ord}_\mathfrak{l}(y_0)$ and $\text{ord}_\mathfrak{l}(z_0)$ are positive then $\text{ord}_\mathfrak{l}(x_0)$ is also positive since $\text{ord}_\mathfrak{l}(a) \leq 1$. Therefore, $y_0$ or $z_0$ is in $O_\mathfrak{l}^\times$. Assume that $y_0 \in O_\mathfrak{l}^\times$. We define a polynomial $f(y) = y^2 + b^{-1}a_0^2x_0^2 - b^{-1}y_0^2$.
Then \( \text{ord}_l(f(y_0)) \geq 3 \) and \( \text{ord}_l(f'(y_0)) = \text{ord}_l(2) = 1 \). Therefore, we can apply Hensel’s lemma [5 Proposition 4.1.37] to \( f(y) \) and obtain a root \( y_1 \in \mathcal{O}_k^\times \) of \( f(y) \).

This means \( \left( \frac{a_k}{p_k} \right) = 1 \). The case \( z_0 \in \mathcal{O}_k^\times \) can be proven by defining \( f \) as \( f(z) = z^2 - ax_0^2 - by_0^2 \).

**Lemma 4.6.** Fix a prime ideal \( \mathfrak{l} \) of \( \mathcal{O}_H \) above 2 and \( a \in H^\times \). The quadratic Hilbert symbol \( \left( \frac{a}{p_k} \right) \) is determined by \( k \mod 2 \).

**Proof.** Recall that \( p_k = 1 - a^k \xi \), where \( \alpha \) is a generator of \( \lambda^3 \) and that \( \lambda \) is a prime ideal of \( \mathcal{O}_K \) above 2.

From Lemma 4.5, the quadratic Hilbert symbol in this lemma is determined by \( p_k \mod \mathfrak{l}^3 \). If \( \mathfrak{l} \) divides \( \lambda \) then \( p_k \equiv 1 \pmod{\mathfrak{l}^3} \) for any \( k \). Otherwise, \( \mathfrak{l} \) divides \( \lambda \), so \( \alpha \equiv \text{Tr}_{K/Q}(\alpha) \pmod{\mathfrak{l}^3} \). Since \( \text{Tr}_{K/Q}(\alpha) \) is an odd integer, \( \alpha^k \mod \mathfrak{l}^3 \) is determined by \( k \mod 2 \). \( \square \)

**Proof of Theorem 4.4.** By the product formula of Hilbert symbols [10 Theorem (8.1)], we have

\[
\left( \frac{a}{p_k} \right) = \prod_{\mathfrak{l} \neq \mathfrak{p}_k} \left( \frac{a, p_k}{\mathfrak{l}} \right) \prod_{\mathfrak{l} \mid \mathcal{O}_H \text{ and } \mathfrak{l} \neq \mathfrak{p}_k} \left( \frac{p_k}{\mathfrak{l}} \right)^{\text{ord}_l(a)}
\]

for \( a \in H^\times \), where \( \mathfrak{l} \) runs over the prime ideals of \( H \) different from \( \mathfrak{p}_k \). From Lemma 4.6 the first product of the right-hand side of (4.2) is determined by \( k \mod 2 \). Since a residue symbol modulo \( \mathfrak{l} \) is determined by \( k \mod N_\mathfrak{l} \), the second product of the right-hand side of (4.2) is determined by \( k \mod \text{least common multiple of } N_\mathfrak{l} \) for the prime ideals \( \mathfrak{l} \) of \( \mathcal{O}_H \) dividing \( a \) and not dividing 2. This completes the proof. \( \square \)

We denote the right-hand side of (4.2) by \( s_k(a) \). Note that \( s_k(a) \) is defined even if \( \mathfrak{p}_k \) is not a prime ideal and equal to \( \left( \frac{a}{\mathfrak{p}_k} \right) \) if \( \mathfrak{p}_k \) is a prime ideal.

4.3.2. Determining \( T_1 \). As mentioned in §3 we can use Theorem 5.3 of [11] for determining \( T_1 \). Since \( B \) is square in \( \mathcal{O}_H \), if \( \mathfrak{p}_k \) is a prime ideal and \( \left( \frac{6\gamma_3(E)}{p_k} \right) \epsilon_k = 1 \) then (i) in Assumption 3.2 holds. Therefore, we can define

\[
T_1 := \{ k \in \mathbb{N} \mid s_k(6\gamma_3(E))\epsilon_k = 1 \}.
\]

In the following, we show how to compute \( \epsilon_k \) and \( \gamma_3(E) \).

First, we show that \( \epsilon_k \) is determined by \( k \mod 2 \). Let \( D \) be the discriminant of \( \mathcal{O}_K \). We fix a square root of \( D \) in \( K \) and denote it by \( \sqrt{D} \). Proposition 6.2 of [11] says that, in our case,

\[
\epsilon_k = \begin{cases} 
1 & \text{if } \pi_k^2 \equiv 1 \pmod{4} \text{ or } -\sqrt{D} \pmod{4}, \\
-1 & \text{otherwise}.
\end{cases}
\]

Since 2 splits in \( K \), we have \( (\mathcal{O}_K/4\mathcal{O}_K)^\times \cong (\mathbb{Z}/4\mathbb{Z})^\times \oplus (\mathbb{Z}/4\mathbb{Z})^\times \). Therefore, \( \pi_k \) mod 4 is determined by \( k \mod 2 \), so \( \epsilon_k \) is also determined by \( k \mod 2 \).

Next, we show how to compute \( \gamma_3(E) \). We have \( \gamma_3(E) \in H \) (Lemma 3.4 of [11]) and

\[
\gamma_3(E)^2 = j(E) - 1728.
\]
This equation determines $\gamma_3(E)$ up to sign. The sign can be determined as follows. Let $p$ be a rational prime congruent to 3 modulo 4, splitting in $O_K$, and not dividing the discriminant of $E$. Let $\pi$ be a prime of $O_K$ above $p$ and let $p$ be a a prime ideal of $O_H$ above $\pi$. We denote the reduction of $E$ modulo $p$ by $\tilde{E}$. Theorem 5.3 of [11] says that the Frobenius endomorphism of $\tilde{E}$ is $\left(\frac{6\gamma_3(E)}{p}\right)\epsilon(\pi)[\pi]$, where $\epsilon(\pi)$ is defined in the same way as in (4.4). Since $p \equiv 3 \pmod{4}$ and $p$ splits in $O_K$, we have $\left(\frac{-1}{p}\right) = -1$. Therefore, we can determine the sign of $\gamma_3(E)$ by checking whether

$$\left(\frac{6\gamma_3(E)}{p}\right)\epsilon(\pi)[\pi]Q = Q$$

for $Q \in \tilde{E}(O_H/p)$ such that $[2]Q \neq O_E$. More precisely, the sign of $\gamma_3(E)$ can be determined as follows.

1. Compute a square root $t$ of $j(E) - 1728$.
2. Determine $\epsilon(\pi)$ by (4.4).
3. Take $Q \in \tilde{E}(O_H/p)$ such that $[2]Q \neq O_E$.
4. If $\left[\left(\frac{6}{p}\right)\epsilon(\pi)p\right]Q = Q$ then $\gamma_3(E) = t$, otherwise $\gamma_3(E) = -t$.

We can take $p = 59$ in the case $K = \mathbb{Q}(\sqrt{-23})$ and $p = 47$ in the case $K = \mathbb{Q}(\sqrt{-31})$.

4.3.3. Determining $T_2$. We use Theorem 3.4 to determine $T_2$. In particular, we show the following theorem.

**Theorem 4.7.** There exists a polynomial $f$ with coefficients in $O_H$ of degree 2 such that when $p_k$ is a prime ideal, the following are equivalent:

(a) $\tilde{P} \not\in [\lambda]\tilde{E}(O_H/p_k)$,

(b) $f \mod p_k$ has a multiple root or does not have a root in $O_H/p_k$.

**Proof.** Let $\varphi$ be an isogeny from $E$ with kernel $E[\lambda]$ and $E': y^2 = x^3 + A'x + B'$ its codomain. The theory of complex multiplication shows that $E'$ has also CM by $O_K$. Therefore, we can assume that $A'$ and $B'$ are in $O_H$.

From Lemma 4.6 of [3], we have $E'[\lambda] \subset E'(H)$. Therefore, the field $F$ in Theorem 3.3 is equal to $H$ in our case. Consequently, when $p_k$ is a prime ideal, (a) holds if and only if $p_k$ does not split completely in $H(\tilde{\varphi}^{-1}(P))$.

Let $x_0$ be the $x$-coordinate of the generator of $E'[\lambda]$. Since $\lambda$ divides 2, we have $x_0$ a root of $x^3 + A'x + B'$. Therefore, we have $x_0 \in O_H$.

By Vélu’s formula [13], the image of an affine point $(x, y) \in E'$ under $\tilde{\varphi}$ is given by

$$\tilde{\varphi}(x, y) = \left(\frac{f(x)}{x - x_0}, \frac{g(x)}{(x - x_0)^2}y\right),$$

where and $f, g$ are univariate polynomials over $H$ of degree 2. From the explicit form of Vélu’s formula, we can show that the coefficients of $f$ and $g$ are in $\mathbb{Z}[A', B', x_0]$. Therefore, the coefficients of $f$ and $g$ are in $O_H$.

Let $H_f$ be the splitting field of $f$ over $H$. Then $H_f$ is a subfield of $H(\tilde{\varphi}^{-1}(P))$. Note that the degrees of these fields over $H$ are at most 2 and that $H_f \subseteq H(\tilde{\varphi}^{-1}(P))$. Therefore, we have $H_f = H(\tilde{\varphi}^{-1}(P))$ if $H_f \neq H$.

Assume that $H_f = H$. Let $Q$ be a point in $\tilde{\varphi}^{-1}(P)$. The $x$-coordinate of $Q$ is a root of $f$, so it is in $H$. Then $Q^\sigma = \pm Q$ for any $\sigma$ in the Galois group of
$H(\tilde{\tau}^{-1}(P))/H$. If there exists $\sigma$ such that $Q^\sigma = -Q$ then we have $-P = \tilde{\tau}(-Q) = \tilde{\tau}(Q^\sigma) = (\tilde{\tau}(Q))^\sigma = P^\sigma = P$. This means that $P \in E[2]$. This contradicts $P = (0, \beta)$ with $\beta \neq 0$. Note that $B \neq 0$ since $E$ does not have CM by the Gauss integer ring. Therefore, we have $Q \in E'(H)$. This means that $H(\tilde{\tau}^{-1}(P)) = H$.

Therefore, we have $H_f = H(\tilde{\tau}^{-1}(P))$ in any case. This means that when $p_k$ is a prime ideal, it follows that $p_k$ does not split completely in $H(\tilde{\tau}^{-1}(P))$ if and only if (b) holds. \hfill \qed

Let $f$ be the same as in the proof of Theorem 4.7 and denote the discriminant of $f$ by $\text{disc}(f)$. Then we can define

$$T_2 := \{ k \in \mathbb{N} \mid s_k(\text{disc}(f)) \neq 1 \}. \quad (4.8)$$

Remark 4.8. For computing the isogeny $\varphi$ with kernel $E[\lambda]$, we need to compute the action of $\lambda$ on $E$. It suffices for this to obtain $[\tau]$ as a rational map, where $\tau$ is an element of $O_K$ such that $O_K = \mathbb{Z} + \mathbb{Z}\tau$. In our case, the norm of $\tau$ is small (6 or 8 in the case $K = \mathbb{Q}(\sqrt{-23})$ or $\mathbb{Q}(\sqrt{-31})$, respectively). Therefore, the rational map of $[\tau]$ consists of polynomials of degree at most 8. We can find the rational map of $[\tau]$ by computing all the cyclic isogenies from $E$ of degree $N_{K/Q}(\tau)$ by Vélu’s formula. There are exactly two such isogenies from $E$ to $E$, which correspond to $[\tau]$ and $[\tilde{\tau}]$. We can determine the desired $[\tau]$ by computing these invariant differentials.

4.3.4. Algorithm. The remaining task for determining $T_1$ and $T_2$ explicitly is to determine the condition on $k$ to satisfy $s_k(a) \in S$ for given $a \in O_H$ and $S \subset \{-1, 0, 1\}$. Theorem 4.3 shows that there exist a positive integer $M$ and a subset $T_{a,S}$ of $\mathbb{Z}/M\mathbb{Z}$ such that $s_k(a) \in S$ if and only if $k \mod M \in T_{a,S}$.

We can determine $M$ and a subset $T_{a,S}$ by the following algorithm.

Algorithm 4.9. For $a \in O_H$ and $S \subset \{-1, 0, 1\}$, return a positive integer $M$ and a subset $T_{a,S}$ of $\mathbb{Z}/M\mathbb{Z}$ such that $s_k(a) \in S$ if and only if $k \mod M \in T_{a,S}$.

1. Set $N$ be the least common multiple of 2 and $N_t$ for the prime ideals $t$ of $O_H$ dividing $a$ and not dividing 2.
2. Set $T = \emptyset$.
3. For $k \in \{1, \ldots, N\}$, if $s_k(a) \in S$ then append $k$ to $T$.
4. Set $M = \min\{t \in \mathbb{N} \mid t \text{ divides } N \text{ and } k \in T \Rightarrow k + t \in T \forall k \in \{1, \ldots, N - t\}\}$.
5. Return $M$ and $\{k \in T \mid k \leq M\}$.

For $T_1$, we use Algorithm 4.9 with input $6\gamma_2(E)$ and $\{1\}$ replacing $s_k(a) \in S$ in Step 3 with $s_k(a) \in k$. For $T_2$, the input is $\text{disc}(f)$ and $\{-1, 0\}$.

4.4. Primality proving. Now, we describe our primality proving algorithm. In our algorithm, we need to compute a square root of $D$ modulo $F_k$. For this, we use Algorithm 2.3.8 in [3]. This algorithm terminates in deterministic polynomial time in $k$ in our case since $F_k \equiv 1 \pmod 8$. We note that this algorithm can be defined even if $F_k$ is not prime. In this case, the output is not necessarily a square of $D$ modulo $F_k$. Therefore, if the output is not a square of $D$ modulo $F_k$ then we can determine that $F_k$ is not prime.

Let $C_k$ be the odd part of $N_{K/Q}(c_1 + c_0a^k)$. We assume that $2^{6k+1}$ does not divide $N_{K/Q}(c_1 + c_0a^k)$. Then we can construct a primality proving by replacing $\gamma$ in Theorem 4.4 with $C_k$. In particular, we obtain the following primality proving algorithm.
Algorithm 4.10. For \( k \in T_0 \cap T_1 \cap T_2 \) such that \( F_k > 16N_{K/Q}(c_1 + c_0\alpha)^2 \) and \( 2^{6k+1} \) does not divide \( N_{K/Q}(c_1 + c_0\alpha)^2 \), this algorithm returns whether \( F_k \) is prime.

1. Compute \( r \) by Algorithm 2.3.8 in [3] with input \( F_k \) and \( D \).
2. If \( r^2 \not\equiv D \pmod{F_k} \) then return \( \text{False} \).
3. Let \( a \) be an integer modulo \( F_k \) by replacing \( \sqrt{D} \) in \( \alpha \) with \( r \).
4. Let \( t \) be \( a^{-k} \mod F_k \).
5. Compute \( t^3 + c_1t + c_0 \mod F_k \), where \( \sqrt{D} \) in \( c_0 \) and \( c_1 \) is replaced with \( r \).
   If it is not congruent to zero then replace \( r \) with \( -r \) and go to Step 2.
6. Define an elliptic curve \( E' \) over \( \mathbb{Z}/F_k\mathbb{Z} \) and its point \( P' \) by replacing \( \sqrt{D} \) with \( r \) and \( \xi \) with \( t \) in \( E \) and \( P \).
7. Compute \( Q = \left[2^{6k-1}C_k\right]P' \).
8. If \( Q \) is not strongly nonzero modulo \( F_k \) then return \( \text{False} \).
9. Return whether \( \left[2\right]Q \equiv O_{E'} \pmod{F_k} \).

This algorithm is analogous to Algorithm 6.3 in [3], which is a primality proving algorithm for an integer sequence obtained from \( Q(\sqrt{-15}) \). As in Algorithm 6.3 in [3], the complexity of this algorithm is \( O(k^2 \log k \log \log k) \). We show the correctness of Algorithm 4.10 by [3]. The proof is similar to that of Theorem 6.3 by [3]. For the proof, we recall a lemma from [3].

Lemma 4.11 (Lemma 2.5 of [3]). If \( C, F \in \mathbb{R}, C \geq 1 \), and \( F > 16C^2 \), then \( C(F^{1/4} + 1)^2 < \left(\sqrt{F} - 1\right)^2 \).

Theorem 4.12. Algorithm 4.10 returns \( \text{True} \) if and only if \( F_k \) is prime.

Proof. Assume that \( F_k \) is prime. Then \( p_k \) is a prime ideal and we can define the reduction \( \tilde{E} \) and \( \tilde{P} \). From Lemma 4.3, we have \( \mathbb{Z}/F_k\mathbb{Z} \cong \mathcal{O}_H/p_k \). Therefore, there exists a square root of \( D \) modulo \( F_k \) and the condition in Step 2 holds. In Step 5, \( r \) and \( t \) satisfy that

\[ r \equiv \sqrt{D} \quad \text{and} \quad t \equiv \xi \pmod{p_k}. \]

Therefore, through the isomorphism \( \mathcal{O}_H/p_k \cong \mathbb{Z}/F_k\mathbb{Z} \), we can identify \( E' \) with \( \tilde{E} \) and \( P' \) with \( \tilde{P} \).

Since the Frobenius endomorphism on \( \tilde{E} \) is \( \left[\pi_k\right] \), we have

\[
\tilde{E}(\mathcal{O}_H/p_k) \cong \mathcal{O}_K/(\pi_k - 1)\mathcal{O}_K
\cong \mathcal{O}_K/(\alpha^{2k}(c_1 + c_0\alpha^k))\mathcal{O}_K
\cong \mathbb{Z}/2^{6k}Z \oplus \mathcal{O}_K/(c_1 + c_0\alpha^k)\mathcal{O}_K.
\]

From this and the assumption that \( 2^{6k+1} \) does not divide \( N_{K/Q}(c_1 + c_0\alpha^k) \), we have \( \left[2^{6k}C_k\right]P = O_{\tilde{E}} \). In addition, \( \left[2^{6k-1}C_k\right]P \neq O_{\tilde{E}} \) since \( \tilde{P} \not\equiv \left[2\right]E(\mathcal{O}_H/p_k) \). This means that the condition in Step 8 does not hold and that the congruence in Step 9 holds.

Conversely, assume that Algorithm 4.10 returns \( \text{True} \). This means that, for any prime factor \( p \) of \( F_k \), there exists a point in \( E' \mod p \) of order at least \( 2^{6k} \).

Assume that \( F_k \) is not prime. Let \( p \) be the smallest prime factor of \( F_k \). Then \( \sqrt{F_k} \geq p \). By the Hasse’s theorem [15] Theorem V.1.1], the order of \( (E' \mod
$p)(\mathbb{Z}/p\mathbb{Z})$ is at most $(\sqrt{p} + 1)^2$. Therefore, we have

$$(F_k^{1/4} + 1)^2 \geq (\sqrt{p} + 1)^2 \geq 2^{6k} = N_{K/Q}\left(\frac{\pi_k - 1}{c_1 + c_0a^k}\right)$$

$$= \frac{(\pi_k - 1)(\pi_k - 1)}{N_{K/Q}(c_1 + c_0a^k)} = \frac{F_k - \text{Tr}_{K/Q}(\pi_k) + 1}{N_{K/Q}(c_1 + c_0a^k)}$$

$$\geq \frac{F_k - 2\sqrt{F_k} + 1}{N_{K/Q}(c_1 + c_0a^k)} = \frac{(\sqrt{F_k} - 1)^2}{N_{K/Q}(c_1 + c_0a^k)}.$$  

The final inequality comes from the fact that $\text{Tr}_{K/Q}(\beta)^2 \leq 4N_{K/Q}(\beta)$ for any $\beta \in K$. From the above inequality, we have

$$N_{K/Q}(c_1 + c_0a^k)(F_k^{1/4} + 1)^2 \geq (\sqrt{F_k} - 1)^2.$$  

This contradicts Lemma 4.11 with $C = N_{K/Q}(c_1 + c_0a^k)$ and $F = F_k$. Therefore, $F_k$ must be prime. □

5. Examples

As mentioned above, our algorithm can be applied to the following two cases.

(1) $K = \mathbb{Q}(\sqrt{-23})$ and $\xi$ is a root of $x^4 - x - 1$,

(2) $K = \mathbb{Q}(\sqrt{-31})$ and $\xi$ is a root of $x^4 + x + 1$.

In these cases, the sequences $\{F_k\}$ determined the primality are

(1) $F_k = N_{\mathbb{Q}(\sqrt{-23})/\mathbb{Q}}\left(1 - \left(\frac{3 + \sqrt{-23}}{2}\right)2^k - \left(\frac{3 - \sqrt{-23}}{2}\right)3^k\right)$,

(2) $F_k = N_{\mathbb{Q}(\sqrt{-31})/\mathbb{Q}}\left(1 + \left(\frac{1 + \sqrt{-31}}{2}\right)2^k + \left(\frac{1 - \sqrt{-31}}{2}\right)3^k\right)$.

In these cases, the conditions on $k$ in Algorithm 4.10 hold for $k \geq 2$. In particular, we have the following lemmas.

**Lemma 5.1.** Let $k \geq 2$ be an integer and $F_k$ one of the two integers defined above. We define

- $c_0 = c_1 = -1$ and $\alpha = \frac{3 + \sqrt{-23}}{2}$ if $F_k$ is the sequence defined by (1),

- $c_0 = c_1 = 1$ and $\alpha = \frac{1 + \sqrt{-31}}{2}$ if $F_k$ is the sequence defined by (2).

Then we have

$$(5.1) \quad F_k > 16N_{K/Q}(c_1 + c_0a^k)^2.$$  

**Proof.** Let $K$ be $\mathbb{Q}(\sqrt{-23})$ in the case (1) or $\mathbb{Q}(\sqrt{-31})$ in the case (2). Note that we have $F_k = N_{K/Q}(1 + c_1\alpha^{2k} + c_0a^{3k})$ in the both cases.

For any $\beta \in K$, we have $\text{Tr}_{K/Q}(\beta)^2 \leq 4N_{K/Q}(\beta)$. Since $c_0, c_1 \in \{\pm 1\}$ and $N_{K/Q}(\alpha) = 8$, we have

$$F_k = 8^{3k} + 8^{2k} + 1 + c_1\text{Tr}_{K/Q}(\alpha^{2k}) + c_0\text{Tr}_{K/Q}(\alpha^{3k}) + c_0c_18^{2k}\text{Tr}_{K/Q}(\alpha^k) \geq 8^{3k} + 8^{2k} + 1 - 4(8^k + 8^{1.5k} + 8^{2.5k})$$

$$> 8^{3k} - 8 \cdot 8^{2.5k}.$$  

On the other hand,

$$N_{K/Q}(c_1 + c_0a^k) = N_{K/Q}(1 + a^k) = 8^k + 1 + \text{Tr}_{K/Q}(a^k) < 2 \cdot 8^k.$$
Lemma 5.2. Let $K$ be an imaginary quadratic field, $k$ be a positive integer, $c_0, c_1 \in \{\pm 1\}$. Let $\alpha \in O_K$ such that $N_{K/Q}(\alpha) = 8$. Then $2^{6k}$ does not divide $N_{K/Q}(c_0 + c_1 \alpha^k)$.

Proof. It suffices to show $N_{K/Q}(c_0 + c_1 \alpha^k) < 2^{6k}$. As in the proof of Lemma 5.1, we have $\Tr_{K/Q}(\alpha^k) \leq 2 \sqrt{N_{K/Q}(\alpha^k)} = 2 \cdot 2^{1.5k}$. Therefore,

$$N_{K/Q}(c_0 + c_1 \alpha^k) = 1 + 2^{3k} \pm \Tr_{K/Q}(\alpha^k) \leq (1 + 2^{1.5k})^2 < (2 \cdot 2^{1.5k})^2 < 2^{6k}.$$

We implemented the primality proving algorithm in this paper for these sequences. We used SageMath [13] for implementation and our code is available at https://github.com/hiroshi-onuki/ecpp_cm_h3

As in [13] we can determine the sets $T_0$, $T_1$, and $T_2$ explicitly. In particular, $T_0$ is determined by the discriminant of the elliptic curve $E$, and $T_1$ and $T_2$ are determined by Algorithm 4.9. The set $T_0 \cap T_1 \cap T_2$ is determined modulo 1320 in case (1), and 7920 in case (2) for $E$’s that we used (see n23_def_symbols.sage and n31_def_symbols.sage of our code for the explicit construction).

We ran our primality proving algorithm for $k$ in $[2, 20000] \cap T_0 \cap T_1 \cap T_2$. Our computation showed the following fact.

Theorem 5.3. Let $k \in [2, 20000] \cap T_0 \cap T_1 \cap T_2$.

- $F_k$ defined by (1) is prime if and only if $k = 100, 120, and 313$,
- $F_k$ defined by (2) is prime if and only if $k = 23, 191, 1350, and 2071$.

The computations were performed on a single core of an Apple M1 CPU and took about one week in both cases.

Acknowledgements. The author would like to thank the anonymous reviewers for their useful feedback. This research was in part conducted under a contract of “Research and development on new generation cryptography for secure wireless communication services” among “Research and Development for Expansion of Radio Wave Resources (JPJ000254)”, which was supported by the Ministry of Internal Affairs and Communications, Japan.

References

1. A. Abatzoglou, A CM elliptic curve framework for deterministic primality proving on numbers of special form, University of California at Irvine PhD thesis (2014).
2. A. Abatzoglou, A. Silverberg, A. V. Sutherland, and A. Wong, Deterministic elliptic curve primality proving for a special sequence of numbers, The Open Book Series 1 (2013), no. 1, 1–20.
3. , A framework for deterministic primality proving using elliptic curves with complex multiplication, Mathematics of Computation 85 (2015), no. 299, 1461–1483.
4. M. Agrawal, N. Kayal, and N. Saxena, PRIMES is in P, Annals of Mathematics 160 (2005), 781–793.
5. H. Cohen, Number Theory Volume I: Tools and Diophantine Equations, Graduate Texts in Mathematics, Springer New York, NY, 2007.
6. R. Crandall and C. B. Pomerance, Prime numbers: A computational perspective, second ed., Springer New York, 2005.
7. R. Denomme and G. Savin, Elliptic curve primality tests for Fermat and related primes, Journal of Number Theory 128 (2008), no. 8, 2398–2412.

8. B. H. Gross, An elliptic curve test for Mersenne primes, Journal of Number Theory 110 (2005), no. 1, 114–119, Arnold Ross Memorial Issue.

9. H. W. Lenstra jr. and C. Pomerance, Primality testing with Gaussian periods, Journal of European Mathematical Society 21 (2019), no. 4, 1229–1269.

10. J. Neukirch, Algebraic number theory, Grundlehren der mathematischen Wissenschaften, Springer Berlin Heidelberg, 2013.

11. Alexander Rostovtsev and Anton Stolbunov, Public-key cryptosystem based on isogenies, Cryptology ePrint Archive, Report 2006/145, 2006, https://eprint.iacr.org/2006/145

12. K. Rubin and A. Silverberg, Point counting on reductions of CM elliptic curves, Journal of Number Theory 129 (2009), no. 12, 2903–2923.

13. The Sage Developers, Sagemath, the Sage Mathematics Software System (Version 9.8), 2023, https://www.sagemath.org

14. J. H. Silverman, Advanced topics in the arithmetic of elliptic curves, Graduate texts in mathematics, Springer-Verlag, 1994.

15. Joseph H. Silverman, The arithmetic of elliptic curves, 2nd ed., Graduate Texts in Mathematics, Springer New York, 2009.

16. N. J. A. Sloane et al., The on-line encyclopedia of integer sequences, published electronically at http://oeis.org

17. Y. Tsumura, Primality tests for $2^p \pm 2^{(p+1)/2} + 1$ using elliptic curves, Proceedings of the American Mathematical Society 139 (2011), no. 8, 2697–2703.

18. J. Vélu, Isogénies entre courbes elliptiques, Comptes-Rendues de l’Académie des Sciences 273 (1971), 238–241.

19. A. Wong, Primality test using elliptic curves with complex multiplication by $\mathbb{Q}(\sqrt{-7})$, University of California at Irvine PhD thesis (2013).