CHOOSING THE CORRECT ELLIPTIC CURVE IN THE CM METHOD

K. RUBIN AND A. SILVERBERG

ABSTRACT. We give easy ways to distinguish between the twists of an ordinary elliptic curve E over $\mathbb{F}_p$ in order to identify one with $p+1-2U$ points, when $p = U^2 + dV^2$ with $2U, 2V \in \mathbb{Z}$ and E is constructed using the CM method. This is useful for finding elliptic curves with a prescribed number of points, and is a new, faster, and easier way to implement the last step of the CM method. Our algorithms are completely elementary, in most cases consisting of merely reading off simple congruence conditions on U and V modulo 4, whereas current algorithms rely on elliptic curve arithmetic and computing square roots.

1. INTRODUCTION

For various purposes, including elliptic curve primality proving and finding suitable elliptic curves for elliptic curve cryptography or for pairing-based cryptography, one wants to find an elliptic curve E over $\mathbb{F}_p$ with a given number N of points. The standard way of doing this is the "CM method", a version of which proceeds as follows.

(1) Find U, V, and d such that $p := U^2+dV^2$ is prime and $N = p+1-2U$, with d a squarefree positive integer, and U and V integers if $d \equiv 1$ or $2 \pmod 4$ and half-integers if $d \equiv 3 \pmod 4$. (For now, assume for simplicity that $d \neq 1, 3$.)
(2) Compute the minimal polynomial of $j(z_d)$ (or some other suitable class invariant) over $\mathbb{Q}$, where z_d is in the complex upper half-plane and $\mathbb{Z}+\mathbb{Z}z_d$ is the ring of integers of $\mathbb{Q}(\sqrt{-d})$, and find a root j of this polynomial in $\mathbb{F}_p$.
(3) Write down an elliptic curve E over $\mathbb{F}_p$ with $j(E) = j$. Then $|E(\mathbb{F}_p)| = p+1-2\varepsilon U$ with $\varepsilon \in \{\pm 1\}$. If $\varepsilon = 1$, then E is the desired curve. If $\varepsilon = -1$, the twist of E is the desired curve.

The sign ε determines whether the desired curve (with N points over $\mathbb{F}_p$) is E or its quadratic twist. A number of *ad hoc* methods have been used to compute ε. One method is to use a point counting algorithm, such as Schoof's, to compute $|E(\mathbb{F}_p)|$, and thus ε. In A.14.4.2 of IEEE 1363-2000: Standard Specifications For Public Key Cryptography [10] (see also the implementation [24]), the method for distinguishing between the two twists is to take one of them, choose a random point

2000 *Mathematics Subject Classification.* 11Y40, 11G20, 11T71, 11G15.
Key words and phrases. elliptic curves, CM method, point-counting.
Rubin was supported by NSF grant DMS-0457481 and Silverberg was supported by NSA grants H98230-05-1-0044 and H98230-07-1-0039.

P on it, and compute NP. If $NP = O$ (and $(4U)P \neq O$), then $|E(\mathbb{F}_p)| = N$ as desired; if $NP \neq O$, then the twist of E has N points.

In this paper we give an easy way to read off ε, i.e., to determine whether the desired curve is E or its twist. In most cases our algorithm is a simple test of congruence conditions on U and V modulo 4. Our algorithms are elementary, whereas the current algorithms require elliptic curve arithmetic.

See [1], Chapter VIII of [4], or IX.15 of [7] for the CM method. We emphasize that our results do not speed up the difficult part of the CM method, which is computing the minimal polynomial in step (2). However, if one precomputes a table of these minimal polynomials for a desired range of d, then our algorithms give a significant improvement. Precomputation of class polynomials is standard, and tables are even available online. If the class polynomials are precomputed, then the difficult steps are finding a representation $p = U^2 + dV^2$ such that $p + 1 - 2U = N$ and d is small, and computing a root of the class polynomial modulo p. While our algorithms do not improve the major bottlenecks in the CM method, they do provide elementary and fast ways to do the last step, and we believe they should be considered for practical use.

The cases $d = 1$ and 3 date back to Gauss. Other individual values of d were dealt with by a number of authors; see p. 349 of [19] for some of the relevant references. The case where d is prime and $d \equiv 3 \pmod 4$ was dealt with by Gross [9, 8]. The case where $d \equiv 3 \pmod 4$ and $3 \nmid d$ (i.e., $d \equiv 7$ or $11 \pmod{12}$) was dealt with by Stark [27]. In [16, 17] a simple method is given for distinguishing the two twists that is applicable in the case where $d \equiv 3 \pmod 8$ and $U, V \notin \mathbb{Z}$. See [15, 12] for other recent work on this question. Atkin and Morain discussed the case when the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ has class number one (i.e., the cases dealt with by Gross in [8] and $d = 1, 2, 3$) in [1] (see also [14]). They left the case where $d \equiv 3 \pmod 4$ and the class number of $\mathbb{Q}(\sqrt{-d})$ is two as an open problem (see Conjecture 8.1 of [1]).

Our contribution settles the problem in full generality. In particular, we settle the conjecture of Atkin and Morain, and our results apply to all squarefree d, and all class numbers. Even in those cases where the methods of Gross or Stark apply, our method is faster because we only need to check congruences on U and $V \pmod 4$, while they need to compute a Jacobi symbol modulo d.

The fact that the sign can be read off easily in certain cases was often overlooked, even in the cases $d = 1$ and 3 where the result occurs in popular textbooks [11, 26]. In §2 of [2], Barreto and Naehrig have $p = U^2 + 3V^2$, and suggest doing a search for the smallest b such that $b + 1$ is a square modulo p and such that the point $P = (1, \sqrt{b+1} \pmod p)$ on $E_b : y^2 = x^3 + b$ over $\mathbb{F}_p$ satisfies $NP = O$ with $N = p + 1 - 2U$, as "a simplification of the technique described in" A.14.4 of [10]. Similarly, for $d = 3$ and N prime, p. 13 of [13] recommends choosing arbitrary $b \in \mathbb{F}_p$ until $E_b(\mathbb{F}_p)$ has a non-zero point P that satisfies $NP = O$. However, when $d = 3$ there is an easier way to choose among the 6 possible b's (modulo sixth powers), going back to work of Gauss (see Algorithm 3.5 below).

Our algorithms are easy to implement. When $d \equiv 3$ or $2 \pmod 4$, determining ε (once a curve has been obtained by the CM method above) consists of checking some congruences modulo 4, using our Algorithms 3.1 or 3.2. (Alternatively, if $d \equiv 3$ or $2 \pmod 4$, in Algorithms 3.1′ or 3.2′ one computes a Jacobi symbol modulo d or $d/2$.) When $d \equiv 1 \pmod 4$, a small amount of additional computation is needed, in

Algorithm 3.3. These computations are clearly simpler than the current methods, which require computing a Jacobi symbol and a square root modulo the large prime p, in order to find a point P on the curve, and also involve computing NP.

We have posted PARI/GP [18] implementations of the algorithms at [21].

Outline of the paper: In §2 we give notation needed for our algorithms. We state the algorithms in §3. Given a squarefree positive integer d, a prime $p \geq 5$, and half-integers U and V such that $p = U^2 + dV^2$, our algorithms output an elliptic curve E over $\mathbb{F}_p$ such that $|E(\mathbb{F}_p)| = p + 1 - 2U$. While the algorithms have simple formulations and can be implemented in a straightforward way, without any deep knowledge, they rely on our results in [20], which in turn are based on deep results from the theory of complex multiplication, including Shimura's Reciprocity Law and work of Rumely [22]. In §4 we state the results we need from [20] on counting points on reductions of CM elliptic curves, and sketch their proofs. In §5 we explain how the correctness of our algorithms follows from the results stated in §4, and we give examples in §6. We have tried to write the paper in a style accessible to both number theorists and cryptographers.

2. Notation

Throughout the paper we suppose d is a squarefree positive integer.

Let $\mathfrak{H}$ denote the complex upper half-plane. Let $\sqrt{-d}$ be the square root of $-d$ in $\mathfrak{H}$. Define $z_d \in \mathfrak{H}$ by the following table, depending on $d \pmod 8$:

$d \pmod 8$:	$1, 2$ or 5	3	6	7
z_d :	$\sqrt{-d}$	$\frac{3+\sqrt{-d}}{2}$	$3 + \sqrt{-d}$	$\frac{-3+\sqrt{-d}}{2}$

For $z \in \mathfrak{H}$, let $L_z := \mathbb{Z} + \mathbb{Z}z$,

$$g_2(z) := 60 \sum_{0 \neq \omega \in L_z} \omega^{-4} \qquad \text{and} \qquad g_3(z) = 140 \sum_{0 \neq \omega \in L_z} \omega^{-6}.$$

Let η denote the Dedekind eta function $\eta(z) = e^{2\pi i z/24} \prod_{n=1}^{\infty}(1 - e^{2\pi i n z})$ on $\mathfrak{H}$, and define the Weber functions

$$\gamma_2(z) := 12 \frac{g_2(z)}{(2\pi i)^4 \eta(z)^8} \qquad \text{and} \qquad \gamma_3(z) := -6^3 \frac{g_3(z)}{(2\pi i)^6 \eta(z)^{12}}.$$

Let $j(z)$ be the usual j-function. By Weber ([28]; see for example p. 326 of [23]),

$$j(z) = \gamma_2(z)^3 = 1728 + \gamma_3(z)^2. \tag{1}$$

Recall that if $E : y^2 = x^3 + ax + b$ is an elliptic curve over $\mathbb{F}_p$, then its quadratic twist, which we will denote by $E^{(c)}$, is $y^2 = x^3 + ac^2x + bc^3$ for any non-square $c \in \mathbb{F}_p^{\times}$.

3. Algorithms

Throughout this section, the inputs are

- a prime number $p \geq 5$,
- a squarefree positive integer $d \neq p$, and
- $U, V \in \frac{1}{2}\mathbb{Z}$ such that $p = U^2 + dV^2$. (If $d \equiv 1$ or $2 \pmod 4$, then necessarily $U, V \in \mathbb{Z}$.)

The algorithms output an elliptic curve E over $\mathbb{F}_p$ such that $|E(\mathbb{F}_p)| = p+1-2U$.

Algorithms 3.1, 3.2, and 3.3 below cover the cases $d \equiv 3, 2, 1 \pmod 4$, respectively (excluding $d = 1$ and 3, which are treated separately in Algorithms 3.4 and 3.5). In each case the first step is the hard part of the CM method, namely, computing a Hilbert class polynomial, and the second step is choosing a root mod p; these are standard steps in the CM method. The new part is Step 3 (and Step 4 for Algorithm 3.3). Here, rather than finding a point on the curve and checking its order, our algorithms for the most part use only elementary congruences.

Algorithms 3.1′ and 3.2′ are variants of Algorithms 3.1 and 3.2, replacing the congruence conditions on U and $V \pmod 4$ by a Jacobi symbol.

Algorithms 3.9 and 3.10 compute minimal polynomials of the appropriate class invariants, which are used in Step 1 of each of the previous algorithms. We thank the referee for suggesting we include this.

In §6 we give examples to illustrate the use of the algorithms.

Algorithm 3.1. Suppose $d \equiv 3 \pmod 4$ and $d \neq 3$.

Step 1. Compute the minimal polynomial $f(w) \in \mathbb{Z}[w]$ for $\gamma_3(z_d)\sqrt{-d}$, using Algorithm 3.9 below.

Step 2. Compute a root $\beta \in \mathbb{F}_p$ of $f(w) \pmod p$, compute $\alpha := -\beta V/U \in \mathbb{F}_p^\times$, compute $\delta := 1728 + \alpha^2 \in \mathbb{F}_p^\times$, and let E be the elliptic curve over $\mathbb{F}_p$:

$$E : y^2 = x^3 - 27\delta^3 x + 54\alpha\delta^4.$$

Step 3. If either:

(a) $d \equiv 7 \pmod 8$ and $U - V \equiv 1 \pmod 4$, or

(b) $d \equiv 3 \pmod 8$ and

(b_1) $p \equiv U + V \pmod 4$ and $2U \equiv 0 \pmod 2$, or

(b_2) $p \equiv 1 \pmod 4$ and $2U \equiv 3 \pmod 4$, or

(b_3) $p \equiv 3 \pmod 4$ and $2V \equiv 1 \pmod 4$,

then output E and terminate.

Step 4. Otherwise, find a non-square $\nu \in \mathbb{F}_p^\times$, and output $E^{(\nu)}$.

Note that $U \in \mathbb{Z} \iff 2U \equiv 0 \pmod 2 \iff 2V \equiv 0 \pmod 2$.

Recall the Jacobi symbol $\left(\frac{a}{d}\right) \in \{\pm 1\}$.

Algorithm 3.1′. Suppose $d \equiv 3 \pmod 4$ and $d \neq 3$.

Step 1. Compute the minimal polynomial $f(w) \in \mathbb{Z}[w]$ for $\gamma_3(z_d)\sqrt{-d}$, using Algorithm 3.9 below.

Step 2. Compute a root $\beta \in \mathbb{F}_p$ of $f(w) \pmod p$, compute $\delta := 1728 - \beta^2/d \in \mathbb{F}_p^\times$, and let E be the elliptic curve over $\mathbb{F}_p$:

$$E : y^2 = x^3 + 27\delta^3 dx - 54\beta\delta^4 d.$$

Step 3. If $\left(\frac{4U}{d}\right) = 1$, then output E and terminate.

Step 4. Otherwise, find a non-square $\nu \in \mathbb{F}_p^\times$ and output $E^{(\nu)}$.

Algorithm 3.2. Suppose $d \equiv 2 \pmod 4$.

Step 1. Compute the minimal polynomial $f(w) \in \mathbb{Z}[w]$ for $\gamma_3(z_d)\sqrt{d}$, using Algorithm 3.9 below.

Step 2. Compute a root $\beta \in \mathbb{F}_p$ of $f(w) \pmod p$, compute $\alpha := \beta V/U \in \mathbb{F}_p^\times$, compute $\delta := 1728 - \alpha^2 \in \mathbb{F}_p^\times$, and let E be the elliptic curve over $\mathbb{F}_p$:

$$E : y^2 = x^3 + 27\delta^3 x - 54\alpha\delta^4.$$

Step 3. If $V \equiv 1$ or $U - 1 \pmod 4$ then output E and terminate.
Step 4. Otherwise, find a non-square $\nu \in \mathbb{F}_p^\times$ and output $E^{(\nu)}$.

Algorithm 3.2′. Suppose $d \equiv 2 \pmod 4$.

Step 1. Compute the minimal polynomial $f(w) \in \mathbb{Z}[w]$ for $\gamma_3(z_d)\sqrt{d}$, using Algorithm 3.9 below.
Step 2. Compute a root $\beta \in \mathbb{F}_p$ of $f(w) \pmod p$, compute $\delta := 1728 + \beta^2/d \in \mathbb{F}_p^\times$, and let E be the elliptic curve over $\mathbb{F}_p$:

$$E : y^2 = x^3 - 27\delta^3 dx - 54\beta\delta^4 d.$$

Step 3. Let $d' = d/2$. If either:
(a) $d \equiv 2 \pmod 8$ and $\left(\frac{U}{d'}\right) = (-1)^{(U-1)/2}(-1)^{(p-1)(p+d+3)/16}$, or
(b) $d \equiv 6 \pmod 8$ and $\left(\frac{U}{d'}\right) = (-1)^{(p-1)(p+d+11)/16}$
then output E and terminate.
Step 4. Otherwise, find a non-square $\nu \in \mathbb{F}_p^\times$ and output $E^{(\nu)}$.

Algorithm 3.3. Suppose $d \equiv 1 \pmod 4$ and $d \neq 1$.

Step 1. Compute the minimal polynomial $f_1(w) + f_2(w)\sqrt{d}$ for $j(z_d)$ over $\mathbb{Q}(\sqrt{d})$, with $2f_1, 2f_2 \in \mathbb{Z}[w]$, using Algorithm 3.10 below.
Step 2. Compute:
a square root δ of d in $\mathbb{F}_p$,
a root $\beta \in \mathbb{F}_p$ of $f_1(w) + \delta f_2(w) \pmod p$,
$\alpha := \beta - 1728 \in \mathbb{F}_p^\times$,
$\eta := \alpha^{(p-1)/4} \in \mathbb{F}_p^\times$,
and let E be the elliptic curve over $\mathbb{F}_p$:

$$E : y^2 = x^3 - 27\beta^3\alpha x + 54\beta^4\alpha^2.$$

Step 3. If V is even, let $\varepsilon \in \{\pm 1\}$ be such that $\varepsilon \equiv \eta \pmod p$. Then:
Step 3a. If $U \equiv \varepsilon \pmod 4$, then output E and terminate.
Step 3b. Otherwise, find a non-square $\nu \in \mathbb{F}_p^\times$, output $E^{(\nu)}$, and terminate.
Step 4. If V is odd, compute $\iota := \delta V/U \in \mathbb{F}_p^\times$.
Step 4a. If either:
(i) $\eta = \iota$ and $V \equiv 3 \pmod 4$, or
(ii) $\eta \neq \iota$ and $V \equiv 1 \pmod 4$,
then output E and terminate.
Step 4b. Otherwise, find a non-square $\nu \in \mathbb{F}_p^\times$ and output $E^{(\nu)}$.

For completeness we include the cases $d = 1$ and 3 below.

Algorithm 3.4. Suppose $d = 1$. For $a \in \mathbb{F}_p^\times$, let E_a be $y^2 = x^3 - ax$.

Step 1. If U is odd and $U - 1 \equiv V \pmod 4$, output E_1 and terminate.
Step 2. If U is odd and $U - 1 \not\equiv V \pmod 4$, output E_a where $a \in \mathbb{F}_p$ is any square that is not a fourth power (i.e., $a^{(p-1)/4} = -1$ in $\mathbb{F}_p$), and terminate.
Step 3. If U is even, replace V by $-V$ if necessary to ensure that $V - 1 \equiv U \pmod 4$. Output E_a, for any $a \in \mathbb{F}_p$ satisfying $a^{(p-1)/4} \equiv U/V \pmod p$.

Algorithm 3.5. Suppose $d = 3$. For $b \in \mathbb{F}_p^\times$, let $E_{(b)}$ be $y^2 = x^3 + b$.

Step 1. If $2V \equiv 0 \pmod 3$ and $2U \equiv 2 \pmod 3$, output $E_{(16)}$ and terminate.
Step 2. If $2V \equiv 0 \pmod 3$ and $2U \equiv 1 \pmod 3$, output $E_{(16b)}$ where $b \in \mathbb{F}_p^\times$ is any cube that is not a square (i.e., $b^{(p-1)/6} = -1$ in $\mathbb{F}_p$), and terminate.

Step 3. If $2V \not\equiv 0 \pmod 3$, replace V by $-V$ if necessary to ensure that $2V \equiv 1 \pmod 3$. If $2U \equiv 2 \pmod 3$ output $E_{(16b)}$ for any $b \in \mathbb{F}_p$ satisfying $b^{(p-1)/6} \equiv 2U/(3V-U) \pmod p$, and terminate.

Step 4. Otherwise, output $E_{(16b)}$ for any $b \in \mathbb{F}_p$ satisfying $b^{(p-1)/6} \equiv 2U/(3V+U) \pmod p$.

Remark 3.6. While the CM method always has versions of Steps 1 and 2 of the algorithms above, the curves we define in Step 2 are different from those considered by others; this choice is one reason we are able to cover all (squarefree) d.

Remark 3.7. In Algorithms 3.1 and 3.2, determining the sign $\varepsilon \in \{\pm 1\}$ such that $|E(\mathbb{F}_p)| = p + 1 - 2\varepsilon U$ is a simple matter of checking the congruence classes of U and $V \pmod 4$. This easy check replaces the elliptic curve point multiplication or point counting that would otherwise be used to determine ε. In Algorithm 3.3, a small amount of additional computation is required.

Remark 3.8. In Algorithms 3.1′ and 3.2′ we replace the congruence conditions on U and $V \pmod 4$ by a Jacobi symbol modulo d or $d/2$. This seems less efficient than Algorithms 3.1 and 3.2, but still better than point counting or elliptic curve multiplication. The algorithms in [27] and [1] are special cases of Algorithm 3.1′.

The following two algorithms compute the minimal polynomial of the appropriate class invariant in Algorithms 3.1 through 3.3. These are modifications of standard algorithms (see [1]).

Algorithm 3.9. The input is a squarefree positive integer $d \equiv 2$ or $3 \pmod 4$. The output is the monic irreducible polynomial $f(w) \in \mathbb{Z}[w]$ that has $\gamma_3(z_d)\sqrt{-d}$ or $\gamma_3(z_d)\sqrt{d}$, respectively, as a root, when $d \equiv 3$ or $2 \pmod 4$, respectively.

Step 1. Define integers D, B, N depending on $d \pmod 8$, by the following table:

$d \pmod 8$	2	3	6	7
D	$-4d$	$-d$	$-4d$	$-d$
B	0	-3	-6	3
N	4	2	4	2

and use Algorithm 5.3.5 of [5] to compute a list $Q_1, Q_2, \ldots, Q_h$ of all reduced binary quadratic forms of discriminant D.

Step 2. For $1 \le k \le h$, modify the quadratic form $Q_k = A_k X^2 + B_k XY + C_k Y^2$ sequentially as follows.

Step 2a. If A_k is even and $B_k C_k$ is odd, replace (A_k, B_k, C_k) by $(A_k, B_k + 2A_k, C_k + B_k + A_k)$.

Step 2b. If A_k is even, replace the triple (A_k, B_k, C_k) by $(A_k + B_k + C_k, B_k + 2C_k, C_k)$.

Step 2c. Let μ be the remainder of (the integer) $A_k(B - B_k)/2$ on division by N, and replace the triple (A_k, B_k, C_k) by $(A_k, B_k + 2\mu A_k, C_k + \mu B_k + \mu^2 A_k)$.

Step 3. With the modified triple (A_k, B_k, C_k), let τ_k be the unique root of $A_k X^2 + B_k X + C_k$ in $\mathfrak{H}$, and let

$$f(w) = \begin{cases} \prod_{k=1}^{h} \bigl(w - \gamma_3(\tau_k)\sqrt{-d}\bigr) & \text{if } d \equiv 3 \pmod 4 \\ \prod_{k=1}^{h} \bigl(w - (-1)^{(A_k-1)/2}\gamma_3(\tau_k)\sqrt{d}\bigr) & \text{if } d \equiv 2 \pmod 4. \end{cases}$$

Algorithm 3.10. The input is a squarefree positive integer $d \equiv 1 \pmod 4$ such that $d \neq 1$. The output is $f_1, f_2 \in \frac{1}{2}\mathbb{Z}[w]$ such that $f_1(w) + f_2(w)\sqrt{d}$ is the monic irreducible polynomial in $\mathbb{Q}(\sqrt{d})[w]$ that has $j(z_d)$ as a root.

Step 1. Let $D = -4d$. Use Algorithm 5.3.5 of [5] to compute a list $Q_1, Q_2, \ldots, Q_h$ of all reduced binary quadratic forms of discriminant D.

Step 2. For $1 \leq k \leq h$, modify the quadratic form $Q_k = A_kX^2 + B_kXY + C_kY^2$ sequentially as follows.

Step 2a. If A_k is even and B_kC_k is odd, replace (A_k, B_k, C_k) by $(A_k, B_k + 2A_k, C_k + B_k + A_k)$.

Step 2b. Choose $\mu \in \mathbb{Z}$ so that $A_k + \mu B_k + \mu^2 C_k$ is relatively prime to D, and replace the triple (A_k, B_k, C_k) by $(A_k + \mu B_k + \mu^2 C_k, B_k + 2\mu C_k, C_k)$.

Step 3. With the modified (A_k, B_k, C_k), let τ_k be the unique root of $A_kX^2 + B_kX + C_k$ in $\mathfrak{H}$, let

$$g_1(w) = \prod_{\left(\frac{d}{A_k}\right) = 1} \big(w - j(\tau_k)\big) \quad \text{and} \quad g_2(w) = \prod_{\left(\frac{d}{A_k}\right) = -1} \big(w - j(\tau_k)\big),$$

where $\left(\frac{d}{A_k}\right)$ is the Jacobi symbol, and let $f_1 = (g_1 + g_2)/2$ and $f_2 = (g_1 - g_2)/(2\sqrt{d})$.

4. Counting points on CM elliptic curves

Next we state the results we need from [20], in the special cases in which we use them.

Throughout this section, suppose d is a squarefree positive integer and $d \neq 1, 3$. Let $K = \mathbb{Q}(\sqrt{-d})$ and let H be its Hilbert class field. If F is a number field, let $\mathcal{O}_F$ denote its ring of integers. Note that $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}z_d$; further, $\mathcal{O}_K^\times = \{\pm 1\}$ since $d \neq 1, 3$. Since $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}z_d$, we have $H = K(j(z_d))$ (see Theorem 5.7(iv) of [25]).

In the next result, (i) follows from (1) and the well-known fact that $j(z_d) \in \mathbb{R}$, (ii) and (iii) are Theorems 2 and 3 of [23], (iv) and (v) follow from the end of §6 of [3], and i is the square root of -1 in $\mathfrak{H}$.

Lemma 4.1. (i) $\gamma_2(z_d)^3, \gamma_3(z_d)^2 \in \mathbb{Q}(j(z_d)) = H \cap \mathbb{R}$.

(ii) *If* $3 \nmid d$, *then* $\gamma_2(z_d) \in \mathbb{Q}(j(z_d)) \subset H$.

(iii) *If* $d \equiv 3 \pmod 4$, *then* $\mathbb{Q}(\gamma_3(z_d)\sqrt{-d}) = \mathbb{Q}(j(z_d))$ *and* $\gamma_3(z_d) \in H$.

(iv) *If* $d \equiv 2 \pmod 4$, *then* $\mathbb{Q}(\gamma_3(z_d)\sqrt{d}) = \mathbb{Q}(j(z_d)) \subset H$ *and* $i\gamma_3(z_d) \in H$.

(v) *If* $d \equiv 1 \pmod 4$, *then* $i \in \mathcal{O}_H$.

Let $\boldsymbol{\mu}_4$ denote the set of fourth roots of unity in $\mathbb{C}$.

Definition 4.2. Define a function $\epsilon_d : (\mathcal{O}_K/4\mathcal{O}_K)^\times \to \boldsymbol{\mu}_4$ by the following tables.

If $d \equiv 3 \pmod 4$:

$\lambda^3 \pmod 4$:	$1, -\sqrt{-d}$	$-1, \sqrt{-d}$
$\epsilon_d(\lambda)$:	1	-1

If $d \equiv 2 \pmod 4$:

$\lambda \pmod 4$:	$1, -1 + 2\sqrt{-d}, \pm 1 + \sqrt{-d}$	$-1, 1 + 2\sqrt{-d}, \pm 1 - \sqrt{-d}$
$\epsilon_d(\lambda)$:	1	-1

If $d \equiv 1 \pmod 4$:

$\lambda \pmod 4$:	$1, 1+2\sqrt{-d}$	$2+\sqrt{-d}, \sqrt{-d}$	$-1, -1+2\sqrt{-d}$	$2-\sqrt{-d}, -\sqrt{-d}$
$\epsilon_d(\lambda)$:	1	i	-1	$-i$

Definition 4.3. Suppose $\mathfrak{P}$ is a prime ideal of H not dividing 2, and $a \in \mathcal{O}_H$ is prime to $\mathfrak{P}$. Let $q = \mathbf{N}_{H/\mathbb{Q}}(\mathfrak{P})$. Define $\left(\frac{a}{\mathfrak{P}}\right)_2$ to be the unique element of $\{\pm 1\}$ such that $\left(\frac{a}{\mathfrak{P}}\right)_2 \equiv a^{(q-1)/2} \pmod{\mathfrak{P}}$. If $i \in H$, define $\left(\frac{a}{\mathfrak{P}}\right)_4$ to be the unique element of $\boldsymbol{\mu}_4$ such that $\left(\frac{a}{\mathfrak{P}}\right)_4 \equiv a^{(q-1)/4} \pmod{\mathfrak{P}}$.

If $\mathfrak{P}$ is a prime ideal of H, let $\mathrm{Fr}_{\mathfrak{P}} \in \mathrm{Gal}(\bar{\mathbb{Q}}/H)$ denote a Frobenius of $\mathfrak{P}$, i.e., a Galois automorphism such that for some prime $\bar{\mathfrak{P}}$ of $\bar{\mathbb{Q}}$ above $\mathfrak{P}$, $\alpha^{\mathrm{Fr}_{\mathfrak{P}}} \equiv \alpha^q \pmod{\bar{\mathfrak{P}}}$ for every algebraic integer $\alpha \in \bar{\mathbb{Q}}$. If E is an elliptic curve over $\mathbb{C}$ and $N \in \mathbb{Z}^+$, let $E[N] \subset E(\mathbb{C})$ denote the subgroup of points of order dividing N.

Definition 4.4. Suppose E is an elliptic curve over H with complex multiplication by $\mathcal{O}_K$. Let B be the set of primes of H where E has bad reduction, and let $I(B)$ be the group of fractional ideals of H supported outside of B. If $\omega \in \mathcal{O}_K$, let $[\omega] \in \mathrm{End}(E)$ denote the image of $\omega \in \mathcal{O}_K$ under the embedding $\mathcal{O}_K \hookrightarrow \mathrm{End}(E)$. The *Hecke character* of E over H is the unique character $\psi : I(B) \to K^\times$ such that for every prime $\mathfrak{P}$ of H where E has good reduction:

(i) $\psi(\mathfrak{P})\mathcal{O}_K = \mathbf{N}_{H/K}(\mathfrak{P})$,
(ii) $|E(\mathcal{O}_H/\mathfrak{P})| = \mathbf{N}_{H/\mathbb{Q}}(\mathfrak{P}) + 1 - \mathrm{Tr}_{K/\mathbb{Q}}(\psi(\mathfrak{P}))$, *and*
(iii) if $N \in \mathbb{Z}^+$, $\mathfrak{P} \nmid N$, and $t \in E[N]$, then $t^{\mathrm{Fr}_{\mathfrak{P}}} = [\psi(\mathfrak{P})]t$.

For basic properties of the Hecke character, see for example Chapter II of [26].

Thus to count points on E over the finite field $\mathcal{O}_H/\mathfrak{P}$ we need only evaluate the Hecke character ψ at $\mathfrak{P}$. The next theorem, on counting points on reductions of elliptic curves with complex multiplication, is in Corollary 5.3 of [20]. In [20] we dealt with elliptic curves with CM by any order in an imaginary quadratic field; here we care only about maximal orders. (Note that $D(\tau)$ of [20] is $-d$ of this paper when $D(\tau)$ is odd and is $-4d$ otherwise.)

Theorem 4.5. *Suppose $c \in \mathcal{O}_H$, and suppose $\mathfrak{P}$ is a prime ideal of H not dividing $6cj(z_d)(j(z_d)-1728)$. Let $\lambda \in \mathcal{O}_K$ be a generator of the principal ideal $N_{H/K}(\mathfrak{P})$, and let $q = \mathbf{N}_{H/\mathbb{Q}}(\mathfrak{P})$.*

(i) *If $d \equiv 3 \pmod 4$ then*

$$E : y^2 = x^3 - c^2\frac{j(z_d)^3}{48}x + c^3\frac{\gamma_3(z_d)j(z_d)^4}{864}$$

is an elliptic curve over H, $j(E) = j(z_d)$, and

$$|E(\mathcal{O}_H/\mathfrak{P})| = q + 1 - \left(\tfrac{c}{\mathfrak{P}}\right)_2 \epsilon_d(\lambda)\mathrm{Tr}_{K/\mathbb{Q}}(\lambda).$$

(ii) *If $d \equiv 2 \pmod 4$ then*

$$E : y^2 = x^3 + c^2\frac{j(z_d)^3}{48}x - c^3\frac{i\gamma_3(z_d)j(z_d)^4}{864}$$

is an elliptic curve over H, $j(E) = j(z_d)$, and

$$|E(\mathcal{O}_H/\mathfrak{P})| = q + 1 - \left(\tfrac{c}{\mathfrak{P}}\right)_2 \epsilon_d(\lambda)\mathrm{Tr}_{K/\mathbb{Q}}(\lambda).$$

(iii) *If* $d \equiv 1 \pmod 4$ *then*

$$E : y^2 = x^3 - c^2 \frac{j(z_d)^3(j(z_d)-1728)}{48}x + c^3 \frac{j(z_d)^4(j(z_d)-1728)^2}{864}$$

is an elliptic curve over H, $j(E) = j(z_d)$, *and*

$$|E(\mathcal{O}_H/\mathfrak{P})| = q + 1 - \left(\tfrac{c^2(j(z_d)-1728)}{\mathfrak{P}}\right)_4 \epsilon_d(\lambda)\mathrm{Tr}_{K/\mathbb{Q}}(\lambda).$$

Sketch of the proof. By Lemma 4.1, E is defined over H. The fact that $j(E) = j(z_d)$ follows directly from the definition of $j(E)$. In particular it follows that E is an elliptic curve with complex multiplication by $\mathcal{O}_K$.

Let ψ be the Hecke character of E over H. By Definition 4.4(ii), it suffices to compute $\psi(\mathfrak{P})$. For this computation we use a method of Rumely [22], which in turn relies on Shimura's Reciprocity Law (Theorem 6.31 of [25]). By Definition 4.4(iii), it suffices to compute the action of $\mathrm{Fr}_{\mathfrak{P}}$ on torsion points of E. We need to make Theorem 1 of [22] explicit in the case of interest to us.

Let A be the following elliptic curve over $\mathbb{C}$:

$$A : y^2 = x^3 - \tfrac{1}{4}g_2(z_d)x - \tfrac{1}{4}g_3(z_d).$$

Classical formulas show that $j(A) = j(z_d)$, and for every $N \in \mathbb{Z}^+$,

$$A[N] = \{(\wp(az_d + b; z_d), \tfrac{1}{2}\wp'(az_d + b; z_d)) : a, b \in N^{-1}\mathbb{Z}/\mathbb{Z}\} \tag{2}$$

where $\wp(u; z_d)$ is the Weierstrass $\wp$-function for the lattice $L_{z_d} = \mathbb{Z} + \mathbb{Z}z_d$. Using (1) we can show that the curve E in the statement of the theorem is the twist of A by $\alpha(2\pi i)^{-2}\eta(z_d)^{-4}$, where

$$\alpha := \begin{cases} c\gamma_2(z_d)^4 & \text{if } d \equiv 3 \pmod 4, \\ ci\gamma_2(z_d)^4 & \text{if } d \equiv 2 \pmod 4, \\ c\gamma_2(z_d)^4\gamma_3(z_d) & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Let

$$x_{a,b}(z) = \frac{\wp(az + b; z)}{(2\pi i)^2\eta(z)^4}, \qquad y_{a,b}(z) = \frac{\wp'(az + b; z)}{2(2\pi i)^3\eta(z)^6},$$

and $t_{a,b} = (\alpha x_{a,b}(z_d), \alpha^{3/2} y_{a,b}(z_d))$. it follows from (2) that

$$E[N] = \{t_{a,b} : a, b \in N^{-1}\mathbb{Z}/\mathbb{Z}\}.$$

Again using classical formulas (see §2.2 of [25]), for each fixed pair $a, b \in N^{-1}\mathbb{Z}/\mathbb{Z}$, the functions $x_{a,b}(z)$ and $y_{a,b}(z)$ are modular functions with Fourier coefficients in $\mathbb{Q}(e^{2\pi i/N})$. Therefore we can use Shimura's Reciprocity Law (Theorem 6.31 of [25]) to compute $x_{a,b}(z_d)^{\mathrm{Fr}_{\mathfrak{P}}}$ and $y_{a,b}(z_d)^{\mathrm{Fr}_{\mathfrak{P}}}$, i.e., to compute the action of $\mathrm{Fr}_{\mathfrak{P}}$ on the x and y coordinates of torsion points of E. Explicitly, following p. 392 of [22] we can show that

$$t_{a,b}^{\mathrm{Fr}_{\mathfrak{P}}} = [(\alpha^{9/2})^{(\mathrm{Fr}_{\mathfrak{P}}-1)}\tilde{\epsilon}_d(\lambda)\lambda]t_{a,b},$$

where

$$\tilde{\epsilon}_d(\lambda) = \begin{cases} \epsilon_d(\lambda) & \text{if } d \equiv 1 \text{ or } 3 \pmod 4, \\ i^{3(q-1)/2}\epsilon_d(\lambda) & \text{if } d \equiv 2 \pmod 4. \end{cases}$$

Since this holds for all a, b as above, and $t_{a,b}^{\mathrm{Fr}_{\mathfrak{P}}} = [\psi(\mathfrak{P})]t_{a,b}$ by Definition 4.4(iii), it follows that

$$\psi(\mathfrak{P}) = (\alpha^{9/2})^{(\mathrm{Fr}_{\mathfrak{P}}-1)}\tilde{\epsilon}_d(\lambda)\lambda.$$

Finally, one checks using Lemma 4.1 that

$$(\alpha^{9/2})^{(\mathrm{Fr}_{\mathfrak{P}}-1)} = \begin{cases} \left(\frac{c}{\mathfrak{P}}\right)_2 & \text{if } d \equiv 3 \pmod 4, \\ \left(\frac{c}{\mathfrak{P}}\right)_2 i^{(q-1)/2} & \text{if } d \equiv 2 \pmod 4, \\ \left(\frac{c^2(j(z_d)-1728)}{\mathfrak{P}}\right)_4 & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

as desired. This completes a sketch of the proof. See [20] for details. □

5. Justifications for the algorithms

Next we prove that our algorithms give the correct result. As in §3, suppose p is a prime ≥ 5, d is a squarefree positive integer, $U, V \in \frac{1}{2}\mathbb{Z}$, $p = U^2 + dV^2$, and $d \neq p$. Let $K = \mathbb{Q}(\sqrt{-d})$, let H be its Hilbert class field, let $\lambda = U + V\sqrt{-d}$, and let $\mathfrak{p} = \lambda\mathcal{O}_K$, a prime ideal of $\mathcal{O}_K$ above p. Since $\mathfrak{p}$ is a principal ideal, it splits completely in the Hilbert class field $H = K(j(z_d))$. Since $p = U^2 + dV^2$, we have $-d = U^2/V^2$ in $\mathbb{F}_p$.

Justification for Algorithms 3.1 and 3.1′. Suppose $d \equiv 3 \pmod 4$. Let $f(w)$ be the minimal polynomial of $\gamma_3(z_d)\sqrt{-d}$ over $\mathbb{Q}$. By Lemma 4.1(iii), $\mathbb{Q}(\gamma_3(z_d)\sqrt{-d}) \subset H$. Since p splits completely in H, it splits completely in $\mathbb{Q}(\gamma_3(z_d)\sqrt{-d}) \cong \mathbb{Q}[w]/(f(w))$, so $f(w) \in \mathbb{Z}[w]$ factors into linear factors mod p, and we can fix a root $\beta \in \mathbb{F}_p$ of f.

Let $\rho : \mathcal{O}_H \to \mathbb{F}_p$ be the ring homomorphism that sends $\gamma_3(z_d)\sqrt{-d}$ to β and $\sqrt{-d}$ to $-U/V \pmod p$ (note that $\gamma_3(z_d)\sqrt{-d}$ and $\sqrt{-d}$ generate disjoint fields). Then $\rho(\gamma_3(z_d)) = -\beta V/U$ and $\rho(j(z_d)) = 1728 + \rho(\gamma_3(z_d)^2) = 1728 - \beta^2/d$. Let $\mathfrak{P} = \ker(\rho)$. Then $\lambda \in \mathfrak{P}$, so $\mathfrak{P}$ is a prime ideal of $\mathcal{O}_H$ above $\mathfrak{p}$, and ρ is the reduction map $\mathcal{O}_H \to \mathcal{O}_H/\mathfrak{P} \cong \mathbb{F}_p$.

It follows that the curve E of Step 2 of Algorithm 3.1 is the reduction mod $\mathfrak{P}$ of the curve of Theorem 4.5(i) with $c = 36$ (to clear denominators). By Theorem 4.5(i),

$$|E(\mathbb{F}_p)| = p + 1 - \epsilon_d(\lambda)\mathrm{Tr}_{K/\mathbb{Q}}(\lambda) = p + 1 - \epsilon_d(\lambda)2U.$$

The conditions on U and V in Step 3 of Algorithm 3.1 are precisely the conditions under which $\epsilon_d(\lambda) = 1$. Thus Theorem 4.5(i) shows that Algorithm 3.1 is correct.

Similarly, the E of Step 2 of Algorithm 3.1′ is the reduction mod $\mathfrak{P}$ of the curve of Theorem 4.5(i) with $c = (-1)^{(d-3)/4}\sqrt{-d}$. The correctness of Algorithm 3.1′ follows from Theorem 4.5(i) using that

$$\left(\tfrac{c}{\mathfrak{P}}\right)_2 \epsilon_d(\lambda) = \left(\tfrac{4U}{d}\right)$$

which can be shown using class field theory (see the proof of Theorem 7.4 of [20]). □

Justification for Algorithms 3.2 and 3.2′. This is similar to the justification for Algorithms 3.1 and 3.1′ above. Note that for Algorithm 3.2′, since $p = U^2 + dV^2 \geq 5$ and $d \equiv 2 \pmod 4$ it follows that $p \equiv 1$ or $d + 1 \pmod 8$ and the exponents in Step 3 are integers. □

Justification for Algorithm 3.3. Suppose $d \equiv 1 \pmod 4$. Note that since $p = U^2 + dV^2$, we have $p \equiv 1 \pmod 4$. By Lemma 4.1(i,v) we have $i, \sqrt{-d} \in H$ so $\sqrt{d} \in H \cap \mathbb{R} = \mathbb{Q}(j(z_d))$. Let $f(w) = f_1(w) + f_2(w)\sqrt{d}$ be the minimal polynomial of $j(z_d)$ over $\mathbb{Q}(\sqrt{d})$, with $2f_1, 2f_2 \in \mathbb{Z}[w]$ (since $j(z_d)$ is an algebraic integer). Since $\mathfrak{p}$ splits completely in $H = K(j(z_d)) \supset \mathbb{Q}(j(z_d))$, we can fix a square root $\delta \in \mathbb{F}_p$ of d and a root $\beta \in \mathbb{F}_p$ of $f_1(w) + \delta f_2(w)$.

Let $\rho : \mathcal{O}_H \to \mathbb{F}_p$ be a homomorphism that sends $\sqrt{d}$ to δ, $j(z_d)$ to β, and $\sqrt{-d}$ to $-U/V \pmod p$. Let $\mathfrak{P} = \ker(\rho)$. Then $\lambda \in \mathfrak{P}$, so $\mathfrak{P}$ is a prime ideal of $\mathcal{O}_H$ above $\mathfrak{p}$, and ρ is the reduction map $\mathcal{O}_H \to \mathcal{O}_H/\mathfrak{P} \cong \mathbb{F}_p$.

It follows that the E of Step 2 of Algorithm 3.3 is the reduction mod $\mathfrak{P}$ of the curve of Theorem 4.5(iii) with $c = 36$. Thus by Theorem 4.5(iii),

$$|E(\mathbb{F}_p)| = p + 1 - \left(\tfrac{j(z_d)-1728}{\mathfrak{P}}\right)_4 \epsilon_d(\lambda) 2U.$$

Since $\rho(j(z_d) - 1728) = \alpha$, we have

$$\left(\tfrac{j(z_d)-1728}{\mathfrak{P}}\right)_4 \equiv (j(z_d) - 1728)^{(p-1)/4} \equiv \eta \pmod{\mathfrak{P}}.$$

First suppose V is even. Then by the definition of ϵ_d, we have $\epsilon_d(\lambda) \in \{\pm 1\}$. It follows that $\left(\tfrac{j(z_d)-1728}{\mathfrak{P}}\right)_4 \in \{\pm 1\}$ and $\varepsilon = \left(\tfrac{j(z_d)-1728}{\mathfrak{P}}\right)_4$. The condition on U in Step 3a of Algorithm 3.3 is precisely the condition under which $\varepsilon \cdot \epsilon_d(\lambda) = 1$.

Now suppose V is odd. Note that $\rho(i) = \rho(-\sqrt{d}/\sqrt{-d}) = \delta V/U = \iota$. By the definition of ϵ_d, we have $\epsilon_d(\lambda) \in \{\pm i\}$, so $\left(\tfrac{j(z_d)-1728}{\mathfrak{P}}\right)_4 = \pm\epsilon_d(\lambda) \in \{\pm i\}$. Define $s \in \{1, 3\}$ by $\left(\tfrac{j(z_d)-1728}{\mathfrak{P}}\right)_4 = i^s$, and define $r \in \{0, 1, 2, 3\}$ by $\eta = \iota^r$. Then

$$\iota^s \equiv i^s = \left(\tfrac{j(z_d)-1728}{\mathfrak{P}}\right)_4 \equiv \eta = \iota^r \pmod{\mathfrak{P}}.$$

Since ι has order 4, we have $r = s$, so $\left(\tfrac{j(z_d)-1728}{\mathfrak{P}}\right)_4 \epsilon_d(\lambda) = i^r \epsilon_d(\lambda)$. The conditions on V and η in Step 4a of the algorithm are precisely the conditions under which $\epsilon_d(\lambda) = i^{-r}$. It follows that Algorithm 3.3 is correct. □

Algorithms 3.4 and 3.5 can be easily shown to follow from Theorems 5 and 4 on pp. 305–307 of [11] (see also Exercise 2.33 on p. 185 and Example 10.6 on p. 177 of [26] or p. 318 of [6]).

Justification for Algorithm 3.9. Step 3 of the algorithm is the method described in the proof of Proposition 3 of [23] for replacing each quadratic form Q_k, $1 \le k \le h$, by an equivalent (in the sense of Definition 5.2.3 of [5]) form $A_kX^2 + B_kXY + C_kY^2$ such that A_k is odd and $B_k \equiv B \pmod{2N}$. The choice of B in Step 1 allows us to take

$$Q_1 = \begin{cases} X^2 + dY^2 & \text{if } d \equiv 2 \pmod 8 \\ X^2 + 3XY + \frac{d+9}{4}Y^2 & \text{if } d \equiv 3 \pmod 8 \\ X^2 - 6XY + (d+9)Y^2 & \text{if } d \equiv 6 \pmod 8 \\ X^2 - 3XY + \frac{d+9}{4}Y^2 & \text{if } d \equiv 7 \pmod 8 \end{cases}$$

at the end of Step 3, and then $\tau_1 = z_d$. Note that $B - B_k$ is even since $B_k^2 - 4A_kC_k = D = B^2 - 4A_1C_1$, so μ in Step 3c makes sense. Define a function $g : \mathfrak{H} \to \mathbb{C}$ by

$$g(z) = \begin{cases} \gamma_3(z) & \text{if } d \equiv 3 \pmod 4 \\ i\gamma_3(z) & \text{if } d \equiv 2 \pmod 4. \end{cases}$$

Then g is a modular function of level N, with Fourier coefficients in $\mathbb{Q}(e^{2\pi i/N})$, with $N = 2$ or 4 as in the table in Step 1. The set $\{\tau_1, \ldots, \tau_h\}$ of Step 3 is an "N-system mod 1" as in the Definition on p. 329 of [23]. Now apply Theorem 7 of [23], with g as above and with the N-system $\{\tau_1, \ldots, \tau_h\}$.

Case 1: $d \equiv 3 \pmod 4$. In this case Theorem 7 of [23] shows that

$$F(w) := \prod_{k=1}^{h} \big(w - \gamma_3(\tau_k)\big) \in K[w].$$

Then $f(w) := (\sqrt{-d})^h F(w/\sqrt{-d}) \in K[w]$ as well, $f(w)$ is monic, and

$$f(\gamma_3(z_d)\sqrt{-d}) = (\sqrt{-d})^h F(\gamma_3(\tau_1)) = 0.$$

Using Lemma 4.1(i,iii),

$$[K(\gamma_3(z_d)\sqrt{-d}) : K] = [\mathbb{Q}(\gamma_3(z_d)\sqrt{-d}) : \mathbb{Q}] = [\mathbb{Q}(j(z_d)) : \mathbb{Q}] = h = \deg(f),$$

so f must be the monic irreducible polynomial for $\gamma_3(z_d)\sqrt{-d}$ in $\mathbb{Q}[w]$. Since $\gamma_3(z_d)\sqrt{-d}$ is an algebraic integer, $f(w) \in \mathbb{Z}[w]$.

Case 2: $d \equiv 2 \pmod 4$. In this case, since the Fourier coefficients of $i\gamma_3$ lie in $i\mathbb{Q}$, Theorem 7 of [23] shows that

$$F(w) := \prod_{k=1}^{h} \big(w - (-1)^{(A_k-1)/2} i\gamma_3(\tau_k)\big) \in K[w].$$

Then $f(w) := (-\sqrt{-d})^h F(-w/\sqrt{-d}) \in K[w]$ as well, $f(w)$ is monic, and

$$f(\gamma_3(z_d)\sqrt{d}) = (-\sqrt{-d})^h F(i\gamma_3(\tau_1)) = 0.$$

Using Lemma 4.1(i,iv),

$$[K(\gamma_3(z_d)\sqrt{d}) : K] = [\mathbb{Q}(\gamma_3(z_d)\sqrt{d}) : \mathbb{Q}] = [\mathbb{Q}(j(z_d)) : \mathbb{Q}] = h = \deg(f),$$

so f must be the monic irreducible polynomial for $\gamma_3(z_d)\sqrt{d}$ in $\mathbb{Q}[w]$. Since $\gamma_3(z_d)\sqrt{d}$ is an algebraic integer, $f(w) \in \mathbb{Z}[w]$. □

Justification for Algorithm 3.10. Step 2 of the algorithm (similar to the method described in the proof of Proposition 3 of [23]) replaces each quadratic form Q_k, $1 \le k \le h$, by an equivalent form $A_kX^2 + B_kXY + C_kY^2$ such that A_k is prime to D. We may assume that $Q_1 = X^2 + dY^2$, so $\tau_1 = \sqrt{-d} = z_d$.

For $1 \le k \le h$, let $\mathfrak{a}_k$ be the ideal of K corresponding to Q_k, i.e., $\mathfrak{a}_k = \phi_{FI}(Q_k)$ in the notation on p. 221 of [5], and let $\sigma_k \in \mathrm{Gal}(H/K)$ be the Galois automorphism corresponding to the class of $\mathfrak{a}_k$ by class field theory. Then $\mathrm{Gal}(H/K) = \{\sigma_1, \dots, \sigma_h\}$, and $j(\tau_k) = j(\tau_1)^{\sigma_k}$. By the definition of $\mathfrak{a}_k$ (see p. 221 of [5]), the absolute norm of $\mathfrak{a}_k$ is A_k. By class field theory it follows that σ_k restricts to the identity on $\mathbb{Q}(\sqrt{d})$ if and only if the Jacobi symbol $\left(\frac{d}{A_k}\right) = 1$. It follows that the sets $\{j(\tau_k) : \left(\frac{d}{A_k}\right) = 1\}$ and $\{j(\tau_k) : \left(\frac{d}{A_k}\right) = -1\}$ are each stable under the action of $\mathrm{Gal}(H/K(\sqrt{d}))$, so the polynomials $g_1(w), g_2(w)$ of Step 3 of the algorithm have coefficients in $K(\sqrt{d})$. Since

$$[K(j(z_d)) : K(\sqrt{d})] = [\mathbb{Q}(j(z_d)) : \mathbb{Q}(\sqrt{d})] = \frac{h}{2} = \deg(g_1) = \deg(g_2),$$

we have $g_1, g_2 \in \mathbb{Q}(\sqrt{d})[w]$. Since each $j(\tau_k)$ is an algebraic integer, $g_1, g_2 \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}][w]$. If γ is the nontrivial automorphism of $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, then $g_1^\gamma = g_2$. If $f_1 = (g_1 + g_2)/2$ and $f_2 = (g_1 - g_2)/(2\sqrt{d})$, it follows that $f_1, f_2 \in \frac{1}{2}\mathbb{Z}[w]$, and $f_1(w) + f_2(w)\sqrt{d} = g_1(w)$ has $j(z_d)$ as a root. □

6. Examples

Since the class number one case is the simplest to state, we begin with such an example, that already follows from the work of Gross (see Theorem 12.2.1 and §24 of [8]; see also Theorem 1 of [27]).

Example 6.1. Suppose $d \in \{7, 11, 19, 43, 67, 163\}$, p is a prime, $p \neq d$, and $p = U^2 + dV^2$ with $2U, 2V \in \mathbb{Z}$. If $4U$ is a square modulo d, then the elliptic curve E_d in Table 1 has $p + 1 - 2U$ points over $\mathbb{F}_p$. Otherwise, its twist does.

Table 1.

d	curve name	E_d
7	$49a1$	$y^2 + xy = x^3 - x^2 - 2x - 1$
11	$121b1$	$y^2 + y = x^3 - x^2 - 7x + 10$
19	$361a1$	$y^2 + y = x^3 - 38x + 90$
43	$1849a1$	$y^2 + y = x^3 - 860x + 9707$
67	$4489a1$	$y^2 + y = x^3 - 7370x + 243528$
163	$26569a1$	$y^2 + y = x^3 - 2174420x + 1234136692$

To deduce this from Algorithm 3.1′, note that in these cases $j(z_d) \in \mathbb{Q}$, so $\gamma_3(z_d)\sqrt{-d} \in \mathbb{Q}$ by Lemma 4.1(iii). The curve E_d is a minimal model of

$$y^2 = x^3 + 27j(z_d)^3 dx - (-1)^{(d-3)/4} 54 j(z_d)^4 \gamma_3(z_d)\sqrt{-d} d.$$

Reducing this curve mod p gives the curve in Algorithm 3.1′, since the reductions of $\gamma_3(z_d)\sqrt{-d}$ and $j(z_d)$ are β and δ, respectively. By Algorithm 3.1′, this curve has the desired number of points.

The following examples illustrate Algorithms 3.1, 3.1′, 3.2, 3.2′, and 3.3.

Example 6.2. Let $d = 339$, so $d \equiv 3 \pmod 4$. The class number of $\mathbb{Q}(\sqrt{-339})$ is 6. Let $U = 31415926$, $V = 54331845$, $p = 1001697800600701951 = U^2 + 339V^2$.

Step 1. Using Algorithm 3.9, the minimal polynomial of $\gamma_3(\frac{3+\sqrt{-339}}{2})\sqrt{-339}$ over $\mathbb{Q}$ is

$$\begin{aligned} f(w) = w^6 &+ 66913885985328w^5 - 18537374891907279936w^4 \\ &- 11143657311764756187340 8w^3 - 860994151195427800704552960w^2 \\ &- 167334410660170709596432741 1712w \\ &- 104070235053073794929864764843 6224. \end{aligned}$$

Step 2. Factoring f in $\mathbb{F}_p[w]$ gives a root $\beta = 570246892109169272 \in \mathbb{F}_p$, and then

$$\alpha = -\beta V/U = 913345758273409607,$$
$$\delta = 1728 + \alpha^2 = 820523299493064878 \in \mathbb{F}_p.$$

(Note that $1728 + \alpha^2 = 1728 - \beta^2/d$.) Proceeding as in Algorithm 3.1:

Step 3. We have $339 \equiv 3 \pmod 8$, $U \in \mathbb{Z}$, and $U + V \equiv p \equiv 3 \pmod 4$, so

$$E : y^2 = x^3 + 647953552270601199x + 991648387830183931$$

has $p + 1 - 2U = 1001697800537870100$ points over $\mathbb{F}_p$.

Alternatively, proceeding as in Algorithm 3.1′:

Step 3′. $\left(\frac{4U}{339}\right) = -1$.

Step 4′. Since $\left(\frac{3}{p}\right) = -1$, twist $E : y^2 = x^3 + 27\delta^3 dx - (-1)^{(d-3)/4}54\beta\delta^4 d$ by 3 to conclude that

$$E^{(3)} : y^2 = x^3 + 445170408181393125x + 757904404913672579$$

has $p + 1 - 2U$ points over $\mathbb{F}_p$.

Example 6.3. Let $d = 142$, so $d \equiv 14 \pmod{16}$. The class number of $\mathbb{Q}(\sqrt{-142})$ is 4. Let $U = 27182845$, $V = 5433082$, $p = 4930517024952833 = U^2 + 142V^2$.

Step 1. Using Algorithm 3.9, the minimal polynomial of $\gamma_3(\sqrt{-142})\sqrt{142}$ is

$$f(w) = w^4 + 216055258840008000w^3 + 346672526005250366831626752w^2 + 104075428173999337606699008000w + 17082811813568501666080780517376.$$

Step 2. Factoring f in $\mathbb{F}_p[w]$ gives a root $\beta = 4347457965648780 \in \mathbb{F}_p$, and then

$$\alpha = \beta V/U = 286811067969178, \quad \delta = 1728 - \alpha^2 = 1038464359088172 \in \mathbb{F}_p.$$

(Note that $1728 - \alpha^2 = 1728 + \beta^2/d$.) Proceeding as in Algorithm 3.2:

Step 3. We have $V \equiv 2 \pmod 4$, $U \equiv 1 \pmod 4$.

Step 4. Since $\left(\frac{3}{p}\right) = -1$, twist $E : y^2 = x^3 + 27\delta^3 x - 54\alpha\delta^4$ by 3 to conclude that

$$E^{(3)} : y^2 = x^3 + 3313493192956667x + 778757513038160$$

has $p + 1 - 2U = 4930516970587144$ points over $\mathbb{F}_p$.

Alternatively, proceeding as in Algorithm 3.2′:

Step 3′. $d \equiv 6 \pmod 8$, $d/2 = 71$, $\left(\frac{U}{71}\right) = -1 \neq (-1)^{(p-1)(p+d+11)/16} = 1$.

Step 4′. Since $\left(\frac{3}{p}\right) = -1$, twist $E : y^2 = x^3 - 27\delta^3 dx - 54\beta\delta^4 d$ by 3 to conclude that

$$E^{(3)} : y^2 = x^3 + 2813600995625254x + 3658823747837768$$

has $p + 1 - 2U$ points over $\mathbb{F}_p$.

Example 6.4. Let $d = 33$, so $d \equiv 1 \pmod 4$. The class number of $\mathbb{Q}(\sqrt{-33})$ is 4. Let $U = 31415926$, $V = 6951499$, $p = 2581630571888509 = U^2 + 33V^2$. We apply Algorithm 3.3.

Step 1. The minimal polynomial of $j(\sqrt{-33})$ over $\mathbb{Q}(\sqrt{33})$ given by Algorithm 3.10 is $f_1(w) + f_2(w)\sqrt{33}$, where

$$f_1(w) = w^2 - 2368431749232000w - 163005261895650240000000,$$

$$f_2(w) = -412291047168000w - 28375573899239424000000.$$

Step 2. We compute that $\delta = 906667748366218$ satisfies $\delta^2 \equiv 33 \pmod p$, and $\beta = 1230386087224503$ is a root in $\mathbb{F}_p$ of $f_1(w) + \delta f_2(w)$. Then $\alpha = \beta - 1728 = 1230386087222775 \in \mathbb{F}_p$, and $\eta = \alpha^{(p-1)/4} = 1415502600194918 \in \mathbb{F}_p$.

Step 4. Since V is odd, we are in Step 4. We compute

$$\iota = \delta V/U = 1166127971693591 \in \mathbb{F}_p^\times.$$

Since $\eta = -\iota \neq \iota$, and $V \equiv 3 \pmod 4$, we are in Step 4b. Since $\left(\frac{2}{p}\right) = -1$, twist $E : y^2 = x^3 - 27\beta^3\alpha x + 54\beta^4\alpha^2$ by 2 to conclude that

$$E^{(2)} : y^2 = x^3 + 765794649689631x + 1999640137701174$$

has $p + 1 - 2U = 2581630509056658$ points over $\mathbb{F}_p$.

References

[1] A. O. L. Atkin, F. Morain, *Elliptic curves and primality proving*, Math. Comp. **61** (1993), 29–68.

[2] P. Barreto, M. Naehrig, *Pairing-Friendly Elliptic Curves of Prime Order*, Selected Areas in Cryptography – SAC 2005, Lect. Notes in Comp. Sci. **3897**, Springer, Berlin, 2006, 319–331.

[3] B. J. Birch, *Weber's class invariants*, Mathematika **16** (1969), 283–294.

[4] I. Blake, G. Seroussi, N. Smart, Elliptic Curves in Cryptography, London Math. Society Lecture Note Series **265**, Cambridge University Press, Cambridge, 1999.

[5] H. Cohen, A course in computational algebraic number theory, *Graduate Texts in Mathematics* **138**, Springer, New York, 1993.

[6] D. A. Cox, Primes of the form $x^2 + ny^2$, John Wiley & Sons, New York, 1989.

[7] S. Galbraith, *Pairings*, Chapter IX of Advances in Elliptic Curve Cryptography, I. F. Blake, G. Seroussi, N. P. Smart, eds., London Math. Society Lecture Note Series **317**, Cambridge University Press, Cambridge, 2005, 183–213.

[8] B. H. Gross, Arithmetic on elliptic curves with complex multiplication, Lect. Notes in Math. **776**, Springer, Berlin, 1980.

[9] B. H. Gross, *Minimal models for elliptic curves with complex multiplication*, Compositio Math. **45** (1982), 155–164.

[10] *IEEE 1363-2000: Standard Specifications For Public Key Cryptography, Annex A. Number-Theoretic Background*, `http://grouper.ieee.org/groups/1363/private/P1363-A-11-12-99.pdf`

[11] K. Ireland, M. Rosen, A classical introduction to modern number theory, Second Edition, Grad. Texts **84**, Springer, New York, 1990.

[12] N. Ishii, *Trace of Frobenius endomorphism of an elliptic curve with complex multiplication*, Bull. Austral. Math. Soc. **70** (2004), 125–142.

[13] A. Menezes, *An introduction to pairing-based cryptography*, notes from lectures given in Santander, Spain, 2005, 18 pp., `http://www.cacr.math.uwaterloo.ca/~ajmeneze/publications/pairings.pdf`

[14] F. Morain, *Primality proving using elliptic curves: an update*, in Algorithmic number theory (Portland, OR, 1998), Lect. Notes in Comp. Sci. **1423**, Springer, Berlin, 1998, 111–127.

[15] F. Morain, *Computing the cardinality of CM elliptic curves using torsion points*, to appear in J. Théor. Nombres Bordeaux, `http://www.lix.polytechnique.fr/~morain/Articles/articles.english.html`

[16] Y. Nogami, Y. Morikawa, *A Method for Distinguishing the Two Candidate Elliptic Curves in CM Method*, in Information Security and Cryptology — ICISC 2004, Lect. Notes in Comp. Sci. **3506**, Springer, Berlin, 2005, 249–260.

[17] Y. Nogami, M. Obara, Y. Morikawa, *A Method for Distinguishing the Two Candidate Elliptic Curves in the Complex Multiplication Method*, ETRI Journal **28**, (2006) 745–760.

[18] PARI/GP, version `2.4.0 (alpha)`, Bordeaux (2005), `http://pari.math.u-bordeaux.fr`

[19] A. R. Rajwade, J. C. Parnami, *A new cubic character sum*, Acta Arith. **40** (1981/82), 347–356.

[20] K. Rubin, A. Silverberg, *Point counting on reductions of CM elliptic curves*, preprint, `http://math.uci.edu/~asilverb/bibliography/RubinSilverbergCM.pdf`

[21] K. Rubin, A. Silverberg, `http://math.uci.edu/~asilverb/bibliography/CMmethod.html`

[22] R. S. Rumely, *A formula for the grössencharacter of a parametrized elliptic curve*, J. Number Theory **17** (1983), 389–402.

[23] R. Schertz, *Weber's class invariants revisited*, J. Théor. Nombres Bordeaux **14** (2002), 325–343.

[24] M. Scott, *A C++ Implementation of the Complex Multiplication (CM) Elliptic Curve Generation Algorithm from Annex A*, in Implementations of portions of the IEEE P1363 draft, `http://grouper.ieee.org/groups/1363/P1363/implementations.html`

[25] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Reprint of the 1971 original, Publications of the Mathematical Society of Japan **11**, Princeton University Press, Princeton, NJ, 1994.

[26] J. Silverman, Advanced topics in the arithmetic of elliptic curves, *Graduate Texts in Mathematics* **151**, Springer, New York, 1994.
[27] H. M. Stark, *Counting points on CM elliptic curves*, Rocky Mountain J. Math. **26** (1996), 1115–1138.
[28] H. Weber, Lehrbuch der Algebra, Braunschweig, 1908 (reprinted by Chelsea Publ. Co., New York, Third Reprinted Edition, 1979).

Mathematics Department, University of California, Irvine, CA 92697-3875, USA
E-mail address: krubin@uci.edu
E-mail address: asilverb@uci.edu