Contemporary Mathematics

Group Order Formulas for Reductions of CM Elliptic Curves

A. Silverberg

Abstract. We give an overview of joint work with Karl Rubin on computing the number of points on reductions of elliptic curves with complex multiplication, including some of the history of the problem.

1. Introduction

In this paper we try to give a readable survey of joint work with Karl Rubin on computing the number of points on reductions of CM elliptic curves. Proofs and details appear in [**31, 32**].

In §2, we give some of the history of the problem. Notation is given in §3. In §§4–6, we state the main results of [**31**], which give formulas for the group orders of reductions of CM elliptic curves. We give applications (also joint with Rubin) to $\mathbb{Q}$-curves in §7, and to a simple way to do the last step of the CM method of Oliver Atkin and François Morain in §8. Brief sketches of proofs are given in §9 and §8.1.

An extensive study of the mathematics surrounding such questions can be found in the books of David Cox [**5**] and Franz Lemmermeyer [**17**].

Acknowledgments. I thank the organizers of GeoCrypt 2009 for the invitation, Harold Stark for informing me about Wendy Miller's thesis, and Yuri Zarhin, Karl Rubin, Nick Alexander, and the referees for helpful comments on the paper.

2. Some history

If p is an odd prime number and $p \equiv 2 \pmod 3$, then $(a^{(2p-1)/3})^3 \equiv a \pmod p$, so the map $x \mapsto x^3$ defines an onto (and thus one-to-one) map from the finite field $\mathbb{F}_p$ to itself. It follows that if $p \nmid B \in \mathbb{Z}$, then the elliptic curve $y^2 = x^3 + B$ has $p+1$ points mod p, including the point at infinity (since half the values $x^3 + B$ are squares, and each such has two square roots).

This leads to the question of how many points the elliptic curve $y^2 = x^3 + B$ has modulo primes $p \equiv 1 \pmod 3$ (i.e., when the curve has ordinary reduction at p, rather than supersingular). The answer is part of a long story that goes back to Carl Friedrich Gauss.

2010 *Mathematics Subject Classification.* 11G15, 11G05, 11G20.

This material is based upon work supported by the National Science Foundation under grant CNS-0831004 and the National Security Agency under grant H98230-07-1-0039.

According to p. 86 (see (4.24)) of Cox's book [**5**], the following result can be wrested from §358 of Gauss's *Disquisitiones Arithmeticae* [**7**].

THEOREM 2.1 (Gauss, *Disquisitiones Arithmeticae*, 1801). *If p is a prime and $p \equiv 1 \pmod 3$, then $x^3 - y^3 \equiv 1 \pmod p$ has $p - 2 + a$ solutions, where $4p = a^2 + 27b^2$ with $a, b \in \mathbb{Z}$ and $a \equiv 1 \pmod 3$.*

If one rephrases the above statement in modern language, it says the following (see §14C of [**5**]).

THEOREM 2.2 (Gauss). *If p is a prime, $p \equiv 1 \pmod 3$, and E is the elliptic curve $y^2 = x^3 - 432$, then*

$$\#E(\mathbb{F}_p) = p + 1 - (\pi + \bar{\pi})$$

where $p = \pi\bar{\pi}$ in $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ and π is chosen to be normalized so that $\pi \equiv 1 \pmod 3$.

In 1814, in his last diary entry [**8**], Gauss stated a similar result for a different curve (see also p. 86 of [**5**] or §5 of Chapter 11 of [**14**]). As pointed out by Lemmermeyer in [**17**], Gauss's statement was based on numerical evidence, and the first published proof was given by Gustav Herglotz [**12**] in 1921 (see p. 317 and p. 342 of [**17**] for more on the history). One formulation of Gauss's statement is the following.

THEOREM 2.3 (Gauss, Herglotz). *Suppose p is a prime and $p \equiv 1 \pmod 4$. Write p in the form $a^2 + b^2$ with integers a and b, normalized so that $a + bi \equiv 1 \pmod{2 + 2i}$. Then $x^2 + y^2 + x^2y^2 \equiv 1 \pmod p$ has $p - 3 - 2a = (a-1)^2 + b^2 - 4$ solutions.*

Rephrasing this in modern language gives:

THEOREM 2.4 (Gauss, Herglotz). *If p is a prime, $p \equiv 1 \pmod 4$, and E is the elliptic curve $y^2 = x^3 + 4x$, then*

$$\#E(\mathbb{F}_p) = p + 1 - (\pi + \bar{\pi})$$

where $p = \pi\bar{\pi}$ in $\mathbb{Z}[i]$ with $\pi \equiv 1 \pmod{2 + 2i}$.

Theorems 2.2 and 2.4 can easily be generalized to deal with the families of sextic, respectively, quartic, twists of the given curve, as follows.

THEOREM 2.5 (Gauss and others). *If p is a prime, $p \equiv 1 \pmod 3$, $p \nmid B \in \mathbb{Z}$, and E is $y^2 = x^3 + B$, then*

$$\#E(\mathbb{F}_p) = p + 1 - \left(\frac{4B}{\pi}\right)_6^{-1} \pi - \left(\frac{4B}{\pi}\right)_6 \bar{\pi}$$

where $p = \pi\bar{\pi}$ in $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ with $\pi \equiv 1 \pmod 3$, and where $\left(\frac{4B}{\pi}\right)_6$ is the unique sixth root of unity congruent to $(4B)^{(p-1)/6} \pmod \pi$.

See Theorem 4 on p. 305 of Ireland and Rosen [**14**] for (an equivalent statement to) the previous result, and Theorem 5 on p. 307 of [**14**] for the following result. Related references include a well-known paper of Harold Davenport and Helmut Hasse [**6**] and a paper of A. R. Rajwade [**26**].

THEOREM 2.6 (Gauss, Herglotz, and others). *If p is a prime, $p \equiv 1 \pmod 4$, $p \nmid A \in \mathbb{Z}$, and E is $y^2 = x^3 - Ax$, then*

$$\#E(\mathbb{F}_p) = p + 1 - \left(\frac{A}{\pi}\right)_4^{-1} \pi - \left(\frac{A}{\pi}\right)_4 \bar{\pi}$$

where $p = \pi\bar{\pi}$ in $\mathbb{Z}[i]$ with $\pi \equiv 1 \pmod{2+2i}$, and where $\left(\frac{A}{\pi}\right)_4$ is the unique fourth root of unity congruent to $A^{(p-1)/4} \pmod \pi$.

Nowadays, the above results are viewed as part of the theory of complex multiplication. The previous two results deal with all elliptic curves with complex multiplication (CM) by $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ and $\mathbb{Z}[i]$, respectively. In a series of papers beginning in the late 1960's and continuing into the 1980's, Rajwade and co-authors (see for example [**25, 26, 27, 28, 29**]) dealt with elliptic curves over $\mathbb{Q}$ with complex multiplication by the ring of integers in $\mathbb{Q}(\sqrt{-d})$ for some small values of d, including $d = 1, 2, 3, 7, 11, 19$, using cyclotomy and the theory of complex multiplication.

For example, the next result, which appears in a paper of Rajwade [**25**], deals with all the elliptic curves with CM by $\mathbb{Z}[\sqrt{-2}]$. Related work that uses the theory of cyclotomy includes papers by B. W. Brewer, A. L. Whiteman, and others.

As usual, we use $(\frac{a}{m})$ to denote the Jacobi (or Legendre) symbol.

THEOREM 2.7 (Rajwade [**25**]). *If p is a prime, $p \equiv 1$ or $3 \pmod 8$, and E is the elliptic curve $y^2 = x(x^2 - 4ax + 2a^2)$ with $p \nmid a$, then*

$$\#E(\mathbb{F}_p) = p + 1 - \left(\frac{a}{p}\right)(\pi + \bar{\pi})$$

where $p = \pi\bar{\pi}$ in $\mathbb{Z}[\sqrt{-2}]$ and π (and $\bar{\pi}$) is congruent modulo $4\sqrt{-2}$ to an element of

$$\{1, 3, 1 \pm \sqrt{-2}, 3 \pm \sqrt{-2}, 5 + 2\sqrt{-2}, 7 + 2\sqrt{-2}\}.$$

See the introductions to [**28**] and [**29**] for more on the history; they state that Emma Lehmer and Ronald J. Evans conjectured that there would be an answer similar to the ones above for the elliptic curves over $\mathbb{Q}$ with complex multiplication by the ring of integers in the remaining fields $\mathbb{Q}(\sqrt{-d})$ of class number one.

From now on, we assume that d is square-free.

In addition to $d = 1, 2, 3$ given above, the remaining d's for which the ring of integers $\mathcal{O}_K$ of $K = \mathbb{Q}(\sqrt{-d})$ has class number one are $d \in \{7, 11, 19, 43, 67, 163\}$. The elliptic curves with CM by these $\mathcal{O}_K$ are the curves $A(d)$ (in the notation of Dick Gross's thesis [**9**]) in Table 1 below and their quadratic twists (see [**11**] or §24 of [**9**]). For these d, if p is a prime $\neq d$, and $p = u^2 + dv^2$ with $u, v \in \frac{1}{2}\mathbb{Z}$, then

$$\#(A(d)(\mathbb{F}_p)) = p + 1 - \left(\tfrac{4u}{d}\right)2u. \tag{2.1}$$

Here $\pi = u + v\sqrt{-d}$, so $\pi + \bar{\pi} = 2u$.

To show (2.1), one can combine §11.2, Theorem 12.2.1, and §24 of Gross's thesis [**9**], which computes the Hecke characters for these elliptic curves using the theory of complex multiplication.

In the same way, with Proposition 3.5 of Gross's 1982 paper [**10**] in place of §24 of Gross's thesis [**9**], one can obtain a similar formula, corresponding to similar models of elliptic curves with CM by the ring of integers in $\mathbb{Q}(\sqrt{-d})$, for all *prime* $d \equiv 3 \pmod 4$. When the class number of $\mathbb{Q}(\sqrt{-d})$ is greater than one, the elliptic curves are no longer defined over $\mathbb{Q}$.

TABLE 1. Curves with CM by $\mathcal{O}_K$ of class number one

d	curve	$A(d)$
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	$26569a1$	$y^2 + y = x^3 - 2174420x + 1234136692$

For (2.1), see also [**41**], the work of Rajwade et al., and/or [**24, 16, 18**]; the latter two employ ideas of Rajwade and Harold Stark.

Can this be generalized to elliptic curves with CM by orders in imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$ for arbitrary d?

Let $\mathcal{O}_F$ denote the ring of integers in a number field F. The theory of complex multiplication shows that if

- E is an elliptic curve over a number field F,
- E has CM by $K \subseteq F$ with $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$,
- $\mathfrak{P}$ is a prime of F where E has good reduction,
- $\pi \in K$ is a generator of the principal ideal $N_{F/K}(\mathfrak{P})$,
- $q := \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{P})$ $(= \#(\mathcal{O}_F/\mathfrak{P}))$,

then

$$\#E(\mathcal{O}_F/\mathfrak{P}) = q + 1 - \epsilon(\pi)(\pi + \bar{\pi}) \quad \text{with } \epsilon(\pi) \in \{\pm 1\}. \tag{2.2}$$

To make this explicit in the way that Gauss and others did above, one needs to either choose a suitably normalized π so that the sign $\epsilon(\pi)$ in equation (2.2) is 1 (as in Theorems 2.2 and 2.4 above), or else find an explicit formula for the sign $\epsilon(\pi)$ (as in (2.1) above).

Stark [**41**] generalized (2.1) to all the elliptic curves with CM by the ring of integers in $\mathbb{Q}(\sqrt{-d})$, when $d \equiv 7$ or $11 \pmod{12}$ (i.e., when both $d \equiv 3 \pmod 4$ and $3 \nmid d$ hold), using the theory of complex multiplication and Goro Shimura's Reciprocity Law [**38**]. More precisely, Stark showed:

THEOREM 2.8 (Stark, Theorem 1 of [**41**]). *Suppose d is a (square-free) positive integer and $d \equiv 7$ or $11 \pmod{12}$. If (π) is a prime ideal of $\mathbb{Q}(\sqrt{-d})$ of norm p with $(p, 6d) = 1$, $\pi = u + v\sqrt{-d}$ with $u, v \in \frac{1}{2}\mathbb{Z}$, $\mathfrak{P}$ is a prime ideal of the Hilbert class field H of $\mathbb{Q}(\sqrt{-d})$ above π, $a \in H^\times$, and $\mathrm{ord}_{\mathfrak{P}}(a) = 0$, then the reduction mod $\mathfrak{P}$ of the elliptic curve (defined over H and with CM by $\mathbb{Q}(\sqrt{-d})$)*

$$E : y^2 = x^3 + \frac{a^2 d \gamma_2(\tau)}{48} x - \frac{a^3 d \sqrt{-d} \gamma_3(\tau)}{864}$$

has

$$p + 1 - \left(\frac{(-1)^{\frac{d+1}{4}} a}{\mathfrak{P}}\right)_{2,H} \left(\frac{4u}{d}\right) 2u$$

points, where $\tau = \frac{-3+\sqrt{-d}}{2}$, γ_2 *and* γ_3 *are the Weber functions (see §3 below), and the quadratic residue symbol* $\left(\frac{\alpha}{\mathfrak{P}}\right)_{2,H}$ *is defined in Definition 3.2 below.*

Wendy Miller generalized Stark's theorem to the case of elliptic curves with CM by the ring of integers in an imaginary quadratic field whose discriminant is even and not divisible by 3, in her 1998 UCSD PhD thesis [**19**].

In [**31**], Rubin and I generalized the above results to elliptic curves with CM by arbitrary imaginary quadratic fields K (and arbitrary orders $\mathcal{O}$ in $\mathcal{O}_K$). In particular, we give an explicit formula for $\#E(\mathcal{O}_F/\mathfrak{P})$, whenever

- E is an elliptic curve over a number field F with CM by an order $\mathcal{O}$ in an imaginary quadratic field $K \subseteq F$, and
- $\mathfrak{P} \nmid 2$ is a prime ideal of $\mathcal{O}_F$ where E has good reduction.

As an application (see §8 below), in [**32**] we give a faster method for the last step of the Atkin-Morain "CM method" for finding an elliptic curve over a finite field with a specified number of points (also jointly with Rubin). This answers an open question of Atkin and Morain (Conjecture 8.1 of [**2**]). As Morain points out in the introduction to [**20**], for implementing the Atkin-Morain Elliptic Curve Primality Proving algorithm [**2, 21**] and for cryptographic applications, it is important to do this step rapidly, and preferably deterministically.

There are many impediments, both theoretical and computational, to generalizing the elliptic curve results to higher dimensional abelian varieties. Nick Alexander is making progress in the two-dimensional case [**1**], utilizing work of Robert Rumely [**35, 33**].

3. Weber's Zoo and Additional Notation

For z in the complex upper half plane $\mathfrak{H}$, let $L_z = \mathbb{Z} + \mathbb{Z}z$,

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

Recall the Dedekind η-function:

$$\eta(z) = e^{\pi i z/12} \prod_{n=1}^{\infty} (1 - e^{2\pi i n z})$$

and the Weber functions:

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

which satisfy

$$j(z) = \gamma_2(z)^3 = 1728 + \gamma_3(z)^2.$$

Bryan Birch [**4**] has referred to these and other Weber functions as "Weber's zoo". Our proofs make use of results of Heinrich Weber [**42**], Bryan Birch [**3**], and Reinhard Schertz [**36**] on the Weber functions.

From now on, $\mathcal{O}$ is an order in an imaginary quadratic field K and D is the discriminant of $\mathcal{O}$. Define $d \in \mathbb{Z}^+$ by

$$d = \begin{cases} -D & \text{if } D \text{ is odd} \\ -D/4 & \text{if } D \text{ is even.} \end{cases}$$

Then $K = \mathbb{Q}(\sqrt{-d}) = \mathbb{Q}(\sqrt{D})$.

DEFINITION 3.1. With $\mathcal{O}$, D, and d as above, define τ_D by

D :	1 (mod 8)	5 (mod 8)	4 or 8 (mod 32)	otherwise
τ_D :	$\frac{-3+\sqrt{-d}}{2}$	$\frac{3+\sqrt{-d}}{2}$	$3+\sqrt{-d}$	$\sqrt{-d}$

By abuse of notation, denote $j(\tau_D)$ by j and for $i = 1, 2$ denote $\gamma_i(\tau_D)$ by γ_i.

Then $\mathcal{O} = \mathbb{Z}+\mathbb{Z}\tau_D$, $H := K(j)$ is the ring class field of $\mathcal{O}$, and $j = j(\mathcal{O})$ (where $j(\mathcal{O})$ is the j-invariant of any elliptic curve isomorphic to $\mathbb{C}/\mathcal{O}$).

DEFINITION 3.2. Suppose F is a number field containing the n-th roots of unity $\boldsymbol{\mu}_n \subset \mathbb{C}$, $\mathfrak{P}$ is a prime of F not dividing n, and $a \in F^\times$ is such that $n \mid \mathrm{ord}_{\mathfrak{P}}(a)$. Letting b be any n-th root of a and letting $\mathrm{Fr}_{\mathfrak{P}} \in \mathrm{Gal}(F(b)/F)$ denote the Frobenius automorphism associated to $\mathfrak{P}$, define the *n-th power symbol*

$$\left(\tfrac{a}{\mathfrak{P}}\right)_{n,F} := \frac{b^{\mathrm{Fr}_{\mathfrak{P}}}}{b} \in \boldsymbol{\mu}_n \subset F.$$

REMARK 3.3. Note that if $a \in \mathcal{O}_F - \mathfrak{P}$, then $\left(\frac{a}{\mathfrak{P}}\right)_{n,F}$ can be characterized as the unique n-th root of unity that is congruent mod $\mathfrak{P}$ to $a^{(\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{P})-1)/n}$. When $n = 2$ it is the quadratic residue symbol. When $n = 6$ and $F = \mathbb{Q}(\sqrt{-3})$ it is the symbol $\left(\frac{a}{\pi}\right)_6$ in Theorem 2.5, and when $n = 4$ and $F = \mathbb{Q}(i)$ it is the symbol $\left(\frac{a}{\pi}\right)_4$ in Theorem 2.6, where π is a generator of $\mathfrak{P}$.

If E is $y^2 = x^3+ax+b$, let $E^{(c)}$ denote the quadratic twist $y^2 = x^3+ac^2x+bc^3$. If E is defined over $\mathbb{C}$, we say E has CM by $\mathcal{O}$ if $\mathrm{End}(E) \cong \mathcal{O}$.

For $x, y \in \mathbb{Q}$, by $x \equiv y \pmod{2^m}$ we mean $\mathrm{ord}_2(x-y) \geq m$.

4. Main Result, Version I

In this section and the next we formulate two versions of our main result.

THEOREM 4.1 (Corollary 5.4 of [**31**]). *Suppose $\mathcal{O}$ is an order of discriminant D in an imaginary quadratic field K, F is a finite extension of the ring class field H of $\mathcal{O}$, $c \in F^\times$, and (for simplicity) $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$. With j as in Definition 3.2, let E be as in Table 2. Suppose $\mathfrak{P} \nmid 2$ is a prime of F where E has good reduction, π is a generator of $N_{F/K}(\mathfrak{P})$, and $q = \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{P})$. Then:*

(i) *E is defined over F,*
(ii) $\mathrm{End}(E) = \mathcal{O}$,
(iii) *$j(E) = j$, and*
(iv) (a) *if $D \equiv 0$ or $12 \pmod{16}$ then:*

$$\#E(\mathcal{O}_F/\mathfrak{P}) = q + 1 - \left(\tfrac{c^2(j-1728)}{\mathfrak{P}}\right)_{4,F}\epsilon_D(\pi)(\pi+\bar{\pi})$$

(b) *otherwise:*

$$\#E(\mathcal{O}_F/\mathfrak{P}) = q + 1 - \left(\tfrac{c}{\mathfrak{P}}\right)_{2,F}\epsilon_D(\pi)(\pi+\bar{\pi})$$

where $\epsilon_D(\pi) \in \boldsymbol{\mu}_4$ will be given in Table 3 below.

Note that every elliptic curve E over F such that $\mathrm{End}(E) = \mathcal{O}$ and $j(E) = j$ occurs in Table 2 for some c.

TABLE 2.

D	E
odd	$y^2 = x^3 - \frac{c^2 j^3}{48}x + \frac{c^3 \gamma_3 j^4}{864}$
4 *or* 8 (mod 16)	$y^2 = x^3 + \frac{c^2 j^3}{48}x - \frac{c^3 i \gamma_3 j^4}{864}$
0 *or* 12 (mod 16)	$y^2 = x^3 - \frac{c^2 j^3 (j-1728)}{48}x + \frac{c^3 j^4 (j-1728)^2}{864}$

5. Main Result, Version II

The following lemma allows us to choose a good normalization of τ in the upper half plane such that $j(\tau) = j(E)$.

LEMMA 5.1 (Lemma 6.4(i) of [**31**]). *If E is an elliptic curve over $\mathbb{C}$ and $\mathrm{End}(E)$ is isomorphic to an order $\mathcal{O}$ of discriminant D in an imaginary quadratic field $K \subset \mathbb{C}$, then there are $\tau \in \mathfrak{H} \cap K$ and $r, s \in \mathbb{Q}$ so that*

(i) $j(\tau) = j(E)$,
(ii) $\tau = r\tau_D + s$,
(iii) $r \equiv 1 \pmod 2$, *and*
(iv) $s \equiv 0 \pmod 4$.

THEOREM 5.2 (Theorem 5.3 of [**31**]). *If:*

- $E : y^2 = x^3 + ax + b$ *is an elliptic curve over a number field $F \subset \mathbb{C}$,*
- *the ring* $\mathrm{End}(E)$ *is isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field $K \subseteq F$ and (for simplicity) $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$,*
- $\mathfrak{P} \nmid 2$ *is a prime of F where E has good reduction,*
- π *is a generator of the principal ideal $N_{F/K}(\mathfrak{P})$,*
- $q := \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{P})$,
- D *is the discriminant of $\mathcal{O}$, and*
- τ *is as in Lemma 5.1,*

then:

- *if D is odd, then*
$$\#E(\mathcal{O}_F/\mathfrak{P}) = q + 1 - \left(\tfrac{6b\gamma_3(\tau)}{\mathfrak{P}}\right)_{2,F} \epsilon_\tau(\pi)(\pi + \bar{\pi})$$
- *if $D \equiv 4$ or $8 \pmod{16}$, then*
$$\#E(\mathcal{O}_F/\mathfrak{P}) = q + 1 - \left(\tfrac{-6bi\gamma_3(\tau)}{\mathfrak{P}}\right)_{2,F} \epsilon_\tau(\pi)(\pi + \bar{\pi})$$
- *if $D \equiv 0$ or $12 \pmod{16}$, then*
$$\#E(\mathcal{O}_F/\mathfrak{P}) = q + 1 - \left(\tfrac{6^2 b^2 (j(E)-1728)}{\mathfrak{P}}\right)_{4,F} \epsilon_\tau(\pi)(\pi + \bar{\pi})$$

where we give an algorithm for computing $\epsilon_\tau(\pi) \in \boldsymbol{\mu}_4$ in §6.

6. The functions ϵ_D and ϵ_τ

We now define the functions ϵ_D and ϵ_τ used above. Let $\mathcal{O}_2 = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_2$.

When $j(E) = j(\mathcal{O})$, we can take $\tau = \tau_D$ in Theorem 5.2, and then $\epsilon_\tau(\pi) = \epsilon_D(\pi)$ can be read off from Table 3. Note that π is not necessarily in $\mathcal{O}$ (see Remark

9.1 below). However, since $\mathfrak{P} \nmid 2$ and $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$, it follows (see Lemma 2.6(iii) and Remark 2.7 of [**31**]) that $\pi \in \mathcal{O}_2^\times$.

TABLE 3. $\epsilon_D : \mathcal{O}_2^\times \to \boldsymbol{\mu}_4$

If D is odd:

$\pi^3 \pmod 4$	$1, -\sqrt{-d}$	$-1, \sqrt{-d}$
$\epsilon_D(\pi)$	1	-1

If $D \equiv 4 \pmod{16}$:

$\pi \pmod 4$	$1, \sqrt{-d}, -1+2\sqrt{-d}, 2-\sqrt{-d}$	otherwise
$\epsilon_D(\pi)$	1	-1

If $D \equiv 8 \pmod{16}$:

$\pi \pmod 4$	$1, -1+2\sqrt{-d}, \pm 1+\sqrt{-d}$	otherwise
$\epsilon_D(\pi)$	1	-1

If $D \equiv 12 \pmod{16}$:

$\pi \pmod 4$	$1, 1+2\sqrt{-d}$	$2+\sqrt{-d}, \sqrt{-d}$	$-1, -1+2\sqrt{-d}$	$2-\sqrt{-d}, -\sqrt{-d}$
$\epsilon_D(\pi)$	1	i	-1	$-i$

If $D \equiv 0 \pmod{16}$:

$\pi \pmod 4$	$1, -1+2\sqrt{-d}$	$\pm 1-\sqrt{-d}$	$-1, 1+2\sqrt{-d}$	$\pm 1+\sqrt{-d}$
$\epsilon_D(\pi)$	1	i	-1	$-i$

In general, take τ, r, and s as in Lemma 5.1 (for E). With ϵ_D defined in Table 3, then

$$\epsilon_\tau(\pi) = \begin{cases} \epsilon_D(\pi) & \text{if } r \equiv 1 \pmod 4, \\ \epsilon_D(\pi)(-1)^{(\mathrm{N}_{K/\mathbb{Q}}(\pi)-1)/2} & \text{if } r \equiv -1 \pmod 4 \text{ and } D \equiv 4, 8 \pmod{16}, \\ \overline{\epsilon_D(\pi)} & \text{if } r \equiv -1 \pmod 4 \text{ and } D \not\equiv 4, 8 \pmod{16}. \end{cases}$$

REMARK 6.1. In our results the sign $\epsilon_\tau(\pi)$ is in terms of π modulo 4, while in the results of Gross and Stark the corresponding sign is in terms of π modulo d — recall the $\left(\frac{4u}{d}\right)$ in Theorem 2.8 and in (2.1). When their results apply, quadratic reciprocity allows one to go back and forth between their results and ours.

7. $\mathbb{Q}$-curves

Recall that K is an imaginary quadratic field, and let H_K denote the Hilbert class field of K.

DEFINITION 7.1 (§11.1 of [**9**]). An elliptic curve E over H_K is a $\mathbb{Q}$-*curve* if E is isogenous over H_K to E^σ for all $\sigma \in \mathrm{Gal}(H_K/\mathbb{Q})$.

With $K = \mathbb{Q}(\sqrt{-d})$, in [**10**] Gross produced a model of a $\mathbb{Q}$-curve with CM by $\mathcal{O}_K$, for all prime $d \equiv 3 \pmod 4$. We produce a model of a $\mathbb{Q}$-curve with CM by $\mathcal{O}_K$ whenever $d \equiv 2$ or $3 \pmod 4$ (with d square-free).

There are no $\mathbb{Q}$-curves with CM by $\mathcal{O}_K$ when $d > 1$ is a product of primes congruent to $1 \pmod 4$. (See Example 3 on p. 527 of [**37**] and §11.3 of [**9**].)

In the next result, we assume we have a square-free positive integer $d \equiv 2$ or $3 \pmod 4$. Let $D = -d$ if $d \equiv 3 \pmod 4$ and let $D = -4d$ if $d \equiv 2 \pmod 4$, so D is the discriminant of the ring of integers of $K := \mathbb{Q}(\sqrt{-d})$. Let j denote $j(\tau_D)$ and let γ_3 denote $\gamma_3(\tau_D)$.

THEOREM 7.2 (Theorem 7.4 of [**31**]). *The following elliptic curve E is a $\mathbb{Q}$-curve defined over $\mathbb{Q}(j)$ with CM by $\mathbb{Q}(\sqrt{-d})$:*

$$\begin{cases} y^2 = x^3 + \frac{dj^3}{48}x - \frac{d\sqrt{-d}\gamma_3 j^4}{864} & \text{if } d \equiv 3 \pmod 4, \\ y^2 = x^3 - \frac{dj^3}{48}x - \frac{d\sqrt{d}\gamma_3 j^4}{864} & \text{if } d \equiv 2 \pmod 4. \end{cases}$$

If $d \neq 3$, $\mathfrak{P} \nmid 2$ is a prime of H_K where E has good reduction, $\pi = u + v\sqrt{-d} \in \mathcal{O}_K$ is a generator of $\mathrm{N}_{H_K/K}(\mathfrak{P})$ with $u, v \in \frac{1}{2}\mathbb{Z}$, and $q = \mathrm{N}_{H_K/\mathbb{Q}}(\mathfrak{P}) = u^2 + dv^2$, then

$$\#E(\mathcal{O}_F/\mathfrak{P}) = q + 1 - f(u, d, q)(\pi + \overline{\pi})$$

where

$$f(u,d,q) = \begin{cases} \left(\frac{4u}{d}\right) & \text{if } d \equiv 3 \pmod 4, \\ (-1)^{(q-1)(q+d+11)/16}\left(\frac{u}{d/2}\right) & \text{if } d \equiv 6 \pmod 8, \\ (-1)^{(u-1)/2}(-1)^{(q-1)(q+d+3)/16}\left(\frac{u}{d/2}\right) & \text{if } d \equiv 2 \pmod 8. \end{cases}$$

8. Application to Last Step of CM Method

In 1993, Atkin and Morain [**2**] published an algorithm, now known as the CM method, which has the following inputs and output:

Input:

- prime $p \geq 5$,
- (square-free) $d \in \mathbb{Z}^+$, $d \neq p$,
- $U, V \in \frac{1}{2}\mathbb{Z}$ such that $p = U^2 + dV^2$ ($U, V \in \mathbb{Z}$ if $d \equiv 1$ or $2 \pmod 4$).

Output: an elliptic curve E over $\mathbb{F}_p$ such that

$$\#E(\mathbb{F}_p) = p + 1 - 2U.$$

A version of the CM method is the following. For the CM method, see [**2**], or A.14 of [**13**]; Step (3) below is A.14.4.2 of [**13**]. Assume for simplicity that $d \neq 1, 3$.

(1) Compute the minimal polynomial of $j(\sqrt{-d})$ over $\mathbb{Q}$, and find a root j of this polynomial in $\mathbb{F}_p$.
(2) Write down an elliptic curve E over $\mathbb{F}_p$ with $j(E) = j$. Then $\#E(\mathbb{F}_p) = p + 1 \pm 2U$.
(3) To determine whether to output E or its twist, let $N = p + 1 - 2U$, choose a random point $P \in E(\mathbb{F}_p)$, and compute NP. If $NP = O$ (and $4UP \neq O$), then $\#E(\mathbb{F}_p) = N$ as desired; if $NP \neq O$, then the twist of E has N points.

In [**32**], we give algorithms that replace Step (3) (the "last step" of the CM method) with a simpler step (at the possible expense of replacing the class invariant in Step (1) with a different one, though Morain states in §9 of [**20**] that while "it is easier to use invariants of small height," his article shows that "we might as well favor those invariants that give us a fast way of computing the right equation instead").

We emphasize that our results do not speed up the major bottleneck in the CM method, which is computing class polynomials in Step (1) (note that Step (2) is easy). However, precomputation of minimal polynomials for a desired range of d is standard, and tables are available online. We posted PARI/GP implementations of our algorithms at [**30**]. See §6 of [**32**] for some examples. Related work appears in [**20, 15, 22, 23**]. Morain, Andreas Enge, and others have done much work on improving the CM method and finding the best class polynomials. We leave open the problems of modifying and improving our algorithms by using class invariants of smaller height, and of computing the complexity of optimized algorithms.

As an example, we next state the algorithm for the case $d \equiv 2 \pmod 4$ (this is Algorithm 3.2 of [**32**]). The first two steps are standard steps in the CM method. The remaining step is new.

As above, input a square-free positive integer $d \equiv 2 \pmod 4$, a prime $p \geq 5$, and integers U and V such that $p = U^2 + dV^2$. The algorithm outputs an elliptic curve E over $\mathbb{F}_p$ such that $\#E(\mathbb{F}_p) = p + 1 - 2U$.

(1) Let $z_d = \sqrt{-d}$ if $d \equiv 2 \pmod 8$ and let $z_d = 3 + \sqrt{-d}$ if if $d \equiv 6 \pmod 8$. (Pre)compute the minimal polynomial $f(w) \in \mathbb{Z}[w]$ for $\gamma_3(z_d)\sqrt{d}$.
(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:
$$E : y^2 = x^3 + 27\delta^3 x - 54\alpha\delta^4.$$
(3) If $V \equiv 1$ or $U - 1 \pmod 4$ then output E and terminate. Otherwise, find a non-square $\nu \in \mathbb{F}_p^\times$ and output $E^{(\nu)}$.

For a concrete example to illustrate the simplicity of the algorithm, consider the case $d = 2$ (the case considered by Rajwade in [**25**] — see Theorem 2.7 above). Then $\gamma_3(\sqrt{-2})\sqrt{2} = 112$, so $f(w) = w - 112$. The algorithm can be restated as follows (simplifying the model slightly). If $V \equiv 1 \pmod 4$ or $V \equiv U - 1 \pmod 4$, output $y^2 = x^3 + 135x + 756VU^{-1} \pmod p$. Otherwise, find a non-square $\nu \in \mathbb{F}_p^\times$ and output $y^2 = x^3 + 135\nu^2 x + 756\nu^3 VU^{-1} \pmod p$.

See [**32**] for algorithms when $d \equiv 1, 3 \pmod 4$ (Algorithm 3.1 and 3.3 of [**32**]; see also Algorithm 3.4 and 3.5 of [**32**]). When $d \equiv 2$ or $3 \pmod 4$, our algorithms for the last step consist of reading off congruences modulo 4. When $d \equiv 1 \pmod 4$, a square root of $d \pmod p$ also needs to be computed.

Remark 8.1. Algorithm 3.3′ of [**32**] gives an alternative algorithm when $d \equiv 3 \pmod 4$ that is closer to the formulations of Stark and Atkin-Morain and requires computation of the Jacobi symbol $\left(\frac{4U}{d}\right)$. An alternative algorithm when $d \equiv 2 \pmod 4$ (Algorithm 3.2′ of [**32**]), that requires the computation of a Jacobi symbol modulo $d/2$, is the following. Compute $f(w)$ and β as above. Compute $\delta := 1728 + \beta^2/d \in \mathbb{F}_p^\times$, and let E be: $y^2 = x^3 - 27\delta^3 dx - 54\beta\delta^4 d$. Let $d' = d/2$. If either:

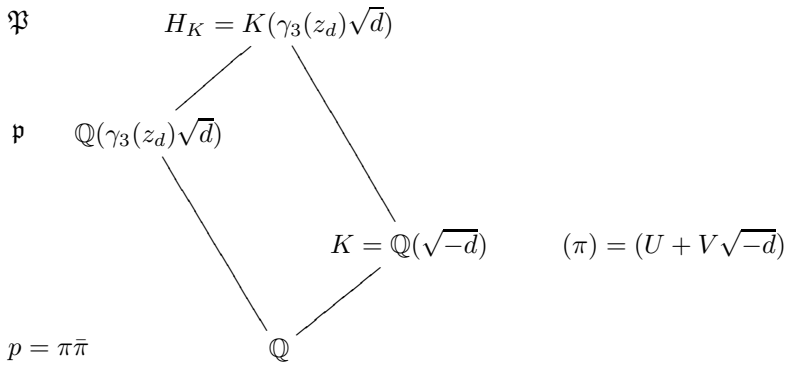
(i) $d \equiv 2 \pmod 8$ and $\left(\frac{U}{d'}\right) = (-1)^{(U-1)/2}(-1)^{(p-1)(p+d+3)/16}$, or

(ii) $d \equiv 6 \pmod 8$ and $\left(\frac{U}{d'}\right) = (-1)^{(p-1)(p+d+11)/16}$

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

8.1. Obtaining the Algorithms from the Main Result. We give a sketch of a proof that the above algorithm for $d \equiv 2 \pmod 4$ works. In the notation of the algorithm, the root β of f uniquely determines a prime $\mathfrak{p}$ of $\mathbb{Q}(\gamma_3(z_d)\sqrt{d})$ above p. Let $\mathfrak{P}$ be the prime of the Hilbert class field H_K above $\mathfrak{p}$ and (π) (as in Figure 1).

FIGURE 1. Prime ideals



Reduction mod $\mathfrak{P}$ sends:

$$\begin{aligned} \sqrt{-d} &\mapsto -U/V \text{ (since } \pi = U + V\sqrt{-d}) \\ \gamma_3(z_d)\sqrt{d} &\mapsto \beta \\ i\gamma_3(z_d) &\mapsto \beta V/U = \alpha \\ j(z_d) = 1728 + \gamma_3(z_d)^2 &\mapsto 1728 - \alpha^2 = \delta. \end{aligned}$$

It follows that E is the reduction mod $\mathfrak{P}$ of the elliptic curve over $H = H_K$ in Theorem 4.1 above, for which we have a formula of the form:

$$\#E(\mathcal{O}_H/\mathfrak{P}) = \#E(\mathbb{F}_p) = p + 1 - \tilde{\epsilon}(\pi) \cdot 2U$$

with an explicit $\tilde{\epsilon}(\pi) \in \boldsymbol{\mu}_2$. One can check that the congruence conditions in the last step of the algorithm hold if and only if $1 = \tilde{\epsilon}(\pi)$.

9. Ideas of Proof of Main Result

The method of proof in [**31**] is similar to the method of Stark [**41**], which follows an approach used by Rumely in his thesis [**33**] and in [**34**]. As did Stark (and Miller), we use the theory of complex multiplication ([**38**]) and Shimura's Reciprocity Law (Theorem 6.31(i) of [**38**]).

Suppose that E is an elliptic curve over a number field F, and E has CM by an order $\mathcal{O}$ in an imaginary quadratic field $K \subseteq F$. Identify $\mathcal{O}$ with $\mathrm{End}(E)$ via an isomorphism $\theta : \mathcal{O} \xrightarrow{\sim} \mathrm{End}(E)$ that is normalized so that $\omega \circ \theta(\alpha) = \alpha\omega$ for all $\alpha \in \mathcal{O}$ and holomorphic differential forms ω on E.

Let $\mathcal{I}$ denote the group of fractional ideals of F supported on the primes of F where E has good reduction. We recall that the *Hecke character* $\psi : \mathcal{I} \to K^\times$ is characterized by the property that for every prime $\mathfrak{P}$ of F where E has good reduction, writing $\tilde{E}$ for the reduction of E modulo $\mathfrak{P}$, then the image of $\psi(\mathfrak{P})$ under

$$K = \mathcal{O} \otimes \mathbb{Q} = \mathrm{End}(E) \otimes \mathbb{Q} \hookrightarrow \mathrm{End}(\tilde{E}) \otimes \mathbb{Q}$$

is the Frobenius endomorphism of $\tilde{E}$. One then has:

- $\psi(\mathfrak{P}) \in \mathcal{O}_K$,
- $\psi(\mathfrak{P})\mathcal{O}_K = \mathrm{N}_{F/K}(\mathfrak{P})$,
- $\#E(\mathcal{O}_F/\mathfrak{P}) = \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{P}) + 1 - \mathrm{Tr}_{K/\mathbb{Q}}(\psi(\mathfrak{P}))$.

In other words, finding π in (2.2) so that the sign $\epsilon(\pi)$ is 1 corresponds to finding the generator $\psi(\mathfrak{P})$ of the ideal $\mathrm{N}_{F/K}(\mathfrak{P})$ of $\mathcal{O}_K$ that reduces modulo $\mathfrak{P}$ to the Frobenius endomorphism of $\tilde{E}$.

Rumely and Stark considered the family of elliptic curves

$$E_z : y^2 = x^3 - \frac{\gamma_2(z)}{48}x + \frac{\gamma_3(z)}{864}.$$

When $d \equiv 3 \pmod 4$ and $3 \nmid d$ (as considered by Stark) then E_{z_d} is defined over the Hilbert class field H_K of $K := \mathbb{Q}(\sqrt{-d})$ and has CM by $\mathcal{O}_K$, and then Stark computed the Hecke character for E_{z_d} over H_K, and thus the number of points on the reductions of E_{z_d}.

If either $3 \mid d$ or $d \not\equiv 3 \pmod 4$, then z can be chosen so that E_z has CM by $\mathcal{O}$, but now E_z is defined over a nontrivial extension of H. However, E_z has quadratic twists defined over H. We used the action (as defined by Shimura; [**39**] or §A5 of [**40**]; see also §6.6 of [**38**] or §1 of [**34**]) of $\mathrm{GL}_2^+(\mathbb{A}_\mathbb{Q})$ on the space of arithmetic modular forms, and Shimura's Reciprocity Law, to compute the Hecke characters for these twists. (This is where the most work is.) From that, we computed the Hecke characters, and thus the number of points on the reductions, for *all* elliptic curves over H with CM by $\mathcal{O}$.

Remark 9.1. If ψ is the Hecke character associated to an elliptic curve with CM by an order $\mathcal{O}$, then $\psi(\mathfrak{P})$ is in the maximal order $\mathcal{O}_K$. When $\mathfrak{P}$ does not divide the conductor of the order $\mathcal{O}$, then $\psi(\mathfrak{P})$ lies in the order $\mathcal{O}$. However, when $\mathfrak{P}$ divides the conductor of $\mathcal{O}$, then $\psi(\mathfrak{P})$ is not necessarily in $\mathcal{O}$ (contrary to a popular belief). We give a "typical" example of this phenomenon in Example 4.3 of [**31**], which will hopefully help to dispel the myth that $\psi(\mathfrak{P})$ always lies in $\mathcal{O}$.

References

[1] N. C. Alexander, *Point counting on reductions of CM abelian surfaces*, UC Irvine PhD Thesis, in preparation.

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

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

[4] B. J. Birch, *Heegner's friends, the modular functions*, Park City Mathematics Institute Lecture, July 3, 2009.

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

[6] H. Davenport, H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. **172** (1934), 151–182.

[7] C. F. Gauss, Disquisitiones arithmeticae (English translation from Latin), Yale University Press, New Haven, Conn.–London 1966.

[8] C. F. Gauss, Mathematisches Tagebuch, 1796–1814, (German translation from Latin), Fifth edition, Ostwalds Klassiker der Exakten Wissenschaften **256**, Verlag Harri Deutsch, Frankfurt am Main, 2005.

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

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

[11] T. Hadano, *Conductor of elliptic curves with complex multiplication and elliptic curves of prime conductor*, Proc. Japan Acad. **51** (1975), 92–95.

[12] G. Herglotz, *Zur letzten Eintragung im Gaussschen Tagebuch*, Ber. Verh. Sächs. Akad. Wiss. Leipzig Math.-Nat. Kl. **73** (1921), 271–276; Ges. Werke 415–420.

[13] *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`

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

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

[16] A. Joux, F. Morain, *Sur les sommes de caractères liées aux courbes elliptiques à multiplication complexe*, J. Number Theory **55** (1995), 108–128.

[17] F. Lemmermeyer, Reciprocity laws: from Euler to Eisenstein, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.

[18] F. Leprévost, F. Morain, *Revêtements de courbes elliptiques à multiplication complexe par des courbes hyperelliptiques et sommes de caractères*, J. Number Theory **64** (1997), 165–182.

[19] W. Miller, *Counting points on certain CM elliptic curves modulo primes*, UCSD PhD thesis, 1998.

[20] F. Morain, *Computing the cardinality of CM elliptic curves using torsion points*, J. Théor. Nombres Bordeaux **19** (2007), 663–681.

[21] F. Morain, *Implementing the asymptotically fast version of the elliptic curve primality proving algorithm*, Math. Comp. **76** (2007), 493–505.

[22] 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.

[23] 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.

[24] R. Padma, S. Venkataraman, *Elliptic curves with complex multiplication and a character sum*, J. Number Theory **61** (1996), 274–282.

[25] A. R. Rajwade, *Arithmetic on curves with complex multiplication by* $\sqrt{-2}$, Proc. Cambridge Philos. Soc. **64** (1968), 659–672.

[26] A. R. Rajwade, *A note on the number of solutions* N_p *of the congruence* $y^2 \equiv x^3 - Dx \pmod{p}$, Proc. Cambridge Philos. Soc. **67** (1970), 603–605.

[27] A. R. Rajwade, *The Diophantine equation* $y^2 = x(x^2+21Dx+112D^2)$ *and the conjectures of Birch and Swinnerton-Dyer*, J. Austral. Math. Soc. Ser. A **24** (1977), 286–295.

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

[29] D. B. Rishi, J. C. Parnami, A. R. Rajwade, *Evaluation of a cubic character sum using the* $\sqrt{-19}$ *division points of the curve* $Y^2 = X^3 - 2^3 \cdot 19X + 2 \cdot 19^2$, J. Number Theory **19** (1984), 184–194.

[30] K. Rubin, A. Silverberg, web posting of algorithms and pre-computed polynomials,
`http://math.uci.edu/~asilverb/bibliography/CMmethod.html`

[31] K. Rubin, A. Silverberg, *Point counting on reductions of CM elliptic curves*, J. Number Theory **129** (2009), 2903–2923.

[32] K. Rubin, A. Silverberg, *Choosing the correct elliptic curve in the CM method*, Math. Comp. **79** (2010), 545–561.

[33] R. S. Rumely, *An explicit formula for the grössencharacter of an abelian variety with complex multiplication*, Princeton University PhD Thesis, 1978.

[34] R. S. Rumely, *A formula for the grössencharacter of a parametrized elliptic curve*, J. Number Theory **17** (1983), 389–402.
[35] R. S. Rumely, *On the grössencharacter of an abelian variety in a parametrized family*, Trans. Amer. Math. Soc. **276** (1983), 213–233.
[36] R. Schertz, *Weber's class invariants revisited*, J. Théor. Nombres Bordeaux **14** (2002), 325–343.
[37] G. Shimura, *On the zeta-function of an abelian variety with complex multiplication*, Ann. of Math. **94** (1971), 504–533.
[38] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Reprint of the 1971 original, Publications of the Mathematical Society of Japan **11**, Princeton Univ. Press, Princeton, NJ, 1994.
[39] G. Shimura, *On certain reciprocity-laws for theta functions and modular forms*, Acta Math. **141** (1978), 35–71.
[40] G. Shimura, Elementary Dirichlet series and modular forms, Springer, New York, 2007.
[41] H. M. Stark, *Counting points on CM elliptic curves*, Rocky Mountain J. Math. **26** (1996), 1115–1138.
[42] H. Weber, Lehrbuch der Algebra III, Braunschweig, 1908.

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