ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 26, Number 3, Summer 1996

# COUNTING POINTS ON $CM$ ELLIPTIC CURVES

H.M. STARK

*To Wolfgang Schmidt on the occasion of his 60th birthday*

**1. Introduction.** Let $E$ be an elliptic curve in Weierstrass normal form,

$$E : y^2 = 4x^3 - g_2x - g_3 \tag{1}$$

where $g_2$ and $g_3$ are in a number field $K$. If $\mathfrak{P}$ is a first degree prime of $K$ of norm $p$, and $g_2$ and $g_3$ are integral at $\mathfrak{P}$, we can reduce the curve (mod $\mathfrak{P}$) to a curve over the field $\mathbf{F}_p$ of $p$ elements

$$\overline{E} : y^2 = 4x^3 - \bar{g}_2x - \bar{g}_3$$

and we can then ask how many points are there on $\overline{E}$? It suffices to know the Frobenius automorphism of $\overline{E}$ which sends the point $(x, y)$ on $\overline{E}$ to the point $(x^p, y^p)$ in order to answer this question. In the case of curves with complex multiplication by an order in a complex quadratic field $k = \mathbf{Q}(\sqrt{D})$ of discriminant $D$, we will show how this can be done.

Since $k$ is always a subfield of $K(\sqrt{D})$, it will be convenient for much of the paper to assume that $k$ is a subfield of $K$. To avoid excess terminology, it will also be convenient to restrict ourselves to the case where $E$ has complex multiplication by the full ring of integers of $k$. Let $H$ be the Hilbert class field of $k$ and $H^+$ the real subfield of $H$. The degree $[H : k]$ is $h(k)$, the class-number of $k$. A curve with complex multiplication by the full ring of integers of $k$ may be rescaled so as to be defined over $H$. With correct rescalings, there are $h(k)$ such curves, all conjugate under automorphisms of the Galois group $G(H/k)$.

In this paper we consider the case that $(D, 6) = 1$ as this includes the interesting class-number one fields that were the original motivation for this paper. It is convenient to set

$$\theta = \frac{-3 + \sqrt{D}}{2},$$

Received by the editors on August 4, 1995, and in revised form on December 18, 1995.

and let

$$\gamma_2 = \gamma_2(\theta), \qquad \gamma_3 = \gamma_3(\theta)$$

be the values of the classical modular functions $\gamma_2(z)$ and $\gamma_3(z)$ at $z = \theta$. For $(D, 6) = 1$, these values reside in $H$ and, indeed, both $\gamma_2$ and $\gamma_3\sqrt{D}$ are in $H^+$. One of the $h(k)$ classes of curves (the one with $j$-invariant equal to $j(\theta)$) may be rescaled to the curve

$$E_1 : y^2 = 4x^3 - D\frac{\gamma_2}{12}x + D\frac{\gamma_3\sqrt{D}}{216}, \tag{2}$$

defined over $H^+$.

Let $\mathfrak{P}$ be a first degree prime of $H$ of norm $p$, and let $\mathfrak{p} = \mathbf{N}_{H/k}(\mathfrak{P})$. The hypothesis that $\mathfrak{P}$ is a first degree prime of $H$ implies that $\mathfrak{p}$ is a principal first degree prime of $k$. To completely determine the Frobenius automorphism of $E_1$ reduced modulo any $\mathfrak{P}$ above $\mathfrak{p}$ is tantamount via Galois theory to finding the Frobenius automorphism for any of the $h(k)$ classes of curves. This fact, together with the fact that there is only one class of curves when $h(k) = 1$, motivates our further restriction in this paper to dealing with a rescaling of $E_1$. Conversely, let $\mathfrak{p} = (\pi)$ be a principal first degree prime ideal of norm $p$ in $k$. The ideal $(\pi)$ splits completely in the Hilbert class field of $k$. Let $\mathfrak{P}$ be any of the first degree prime ideals in $H$ above $(\pi)$. It then makes sense to reduce the curve (2) $(\mathrm{mod}\,\mathfrak{P})$. It has long been known that complex multiplication by one of $\pm\pi$ when reduced $(\mathrm{mod}\,\mathfrak{P})$ takes $(x, y)$ to $(x^p, y^p)$. Since this fact is a by-product of our analysis, we will re-prove it in the course of this paper. Thus, one of $\pm\pi$ serves as the Frobenius automorphism of the reduced curve.

The whole problem of determining the number of points on $\overline{E}_1$ reduces to deciding which of $\pm\pi$ is the Frobenius automorphism. We will answer this question by applying the general reciprocity law of complex multiplication due to Shimura [**8, 9**] (see also Lang [**3**] and Stark [**12**]) which allows us to explicitly calculate what the number field Frobenius automorphism does to division points of $E_1$. The version of the reciprocity law which we will use applies equally well in the case of nonmaximal orders, but we will avoid the extra terminology in this paper. The reciprocity law applies to modular functions in the field of functions of level $N$. These are modular functions that are not only invariant under the principal congruence subgroup $\Gamma(N)$ of the modular

group, but whose Fourier coefficients in their expansion at every cusp also lie in the cyclotomic field of $N$th roots of unity. In Section 2 we will verify that the relevant functions are in the field of functions of level $N$, and in Section 3 we will apply the reciprocity law to appropriate values of these functions. "Appropriate values" turn out to be values at any division point other than two-division points, although there are some advantages in not considering any particular division point exclusively.

Our main result is the following

**Theorem 1.** *Suppose that $D$ is the discriminant of a complex quadratic field $k$ and that $(D, 6) = 1$. Suppose that*

$$\pi = \frac{u + v\sqrt{D}}{2}$$

*and that $(\pi)$ is a principal first degree prime ideal in $k$ of norm $p$ where $(p, 6D) = 1$. Let $\mathfrak{P}$ be a prime ideal of $H$ above $(\pi)$. Let also $a$ be any nonzero number of $H^+$ whose numerator and denominator are relatively prime to $\mathfrak{P}$. Then the curve*

$$E_a : y^2 = 4x^3 - a^2 D\frac{\gamma_2}{12}x + a^3 D\frac{\gamma_3\sqrt{D}}{216},$$

*with coefficients in $H^+$ reduces $\pmod{\mathfrak{P}}$ to a curve $\overline{E}_a$ defined over $\mathbf{F}_p$ with*

$$p + 1 - \begin{cases} \left(\frac{a}{\mathfrak{P}}\right)\left(\frac{2u}{|D|}\right)u & \text{if } D \equiv 1 \pmod 8 \\ \left(\frac{-a}{\mathfrak{P}}\right)\left(\frac{2u}{|D|}\right)u & \text{if } D \equiv 5 \pmod 8 \end{cases}$$

*points.*

In Theorem 1, $(a/\mathfrak{P})$ is the Legendre symbol in $H^+$ and $(2u/|D|)$ is the Jacobi symbol in $\mathbf{Q}$. The stated number of points includes one point at infinity. Besides first degree primes of $H^+$ which split into two first degree primes of $H$, there can be first degree primes in $H^+$ which remain inert in $H$. If $\mathfrak{P}$ is an unramified first degree prime of $H^+$ which is inert in the extension $H/H^+$, then $\mathbf{N}_{H^+/\mathbf{Q}}(\mathfrak{P}) = p$ is a prime of $\mathbf{Q}$ which doesn't split in $k$. In this case, it is well known that there are precisely $p+1$ points on $E_a \pmod{\mathfrak{P}}$. The $\pm$ ambiguity that

causes so much trouble for Theorem 1 does not arise for these primes, and it is for this reason that we will not treat this case in this paper.

We close this section with some examples. We present the six relevant class-number one curves and the last class-number two curve. From Weber [**13**], we have the following tabulated values (with the misprint in the value for $\gamma_3$ when $D = -67$ corrected):

| $D$ | $\gamma_2(\theta)/12$ | $\gamma_3(\theta)\sqrt{D}/216$ |
|---|---|---|
| $-7$ | $-5/4$ | $7/8$ |
| $-11$ | $-8/3$ | $7 \cdot 11/27$ |
| $-19$ | $-8$ | $19$ |
| $-43$ | $-80$ | $7 \cdot 3 \cdot 43$ |
| $-67$ | $-440$ | $7 \cdot 31 \cdot 67$ |
| $-163$ | $-16 \cdot 5 \cdot 23 \cdot 29$ | $7 \cdot 11 \cdot 19 \cdot 127 \cdot 163$ |

Our theorem then gives the following results for primes $p$ other than 2 or 3 which split in $k$,

$D = -7$. The curve

$$y^2 = 4x^3 - 5 \cdot 7a^2x/4 - 7^2a^3/8$$

has $p + 1 - (a/p)(u/7)u$ points when reduced $(\mathrm{mod}\, p)$.

$D = -11$. The curve

$$y^2 = 4x^3 - 8 \cdot 11a^2x/3 - 7 \cdot 11^2a^3/27$$

has $p + 1 + (-a/p)(u/11)u$ points when reduced $(\mathrm{mod}\, p)$.

$D = -19$. The curve

$$y^2 = 4x^3 - 8 \cdot 19a^2x - 19^2a^3$$

has $p + 1 + (-a/p)(u/19)u$ points when reduced $(\mathrm{mod}\, p)$.

$D = -43$. The curve

$$y^2 = 4x^3 - 80 \cdot 43a^2x - 21 \cdot 43^2a^3$$

has $p+1+(-a/p)(u/43)u$ points when reduced $(\mathrm{mod}\, p)$.

$D=-67$. The curve

$$y^2 = 4x^3 - 440\cdot 67a^2x - 217\cdot 67^2a^3$$

has $p+1+(-a/p)(u/67)u$ points when reduced $(\mathrm{mod}\, p)$.

$D=-163$. The curve

$$y^2 = 4x^3 - 53360\cdot 163a^2x - 185801\cdot 163^2a^3$$

has $p+1+(-a/p)(u/163)u$ points when reduced $(\mathrm{mod}\, p)$.

Our last example of this section is with the last class-number two discriminant, $D=-427$. For $\pi=(u+v\sqrt{-427})/2$ generating a first degree principal prime ideal of norm $p$ in $k$ and $a$ any integer in $\mathbf{Q}(\sqrt{61})$, the curve

$$\begin{aligned} y^2 = 4x^3 &- 440\cdot 427(236674+30303\sqrt{61})a^2x \\ &- 161\cdot 427(37121542375+4752926464\sqrt{61})a^3 \end{aligned}$$

has $p+1+(-a/\mathfrak{P})(u/427)u$ points when reduced $(\mathrm{mod}\,\mathfrak{P})$ for either of the two primes $\mathfrak{P}$ of $\mathbf{Q}(\sqrt{61})$ above $p$. The curve is defined over the field of $p$ elements by replacing $\sqrt{61}$ by either of the two square roots of $61 \pmod p$. For example, when $p=431$, $\sqrt{61}$ is replaced by $\pm 270$, the choice determining $\mathfrak{P}$ above $p$. When $a$ is rational, both choices give the same number of points.

It is possible to explicitly calculate selected division points for any fixed curve, thereby proving the result of Theorem 1 for that curve by using Deuring's well-known result that the correct choice of $\pi$ determines a Grössencharacter in $k$. For example, Rajwade [**4, 5, 6**] has managed to verify the equivalent of our examples above for $D=-7$, $D=-11$ and $D=-19$ by explicitly calculating $\sqrt{D}$ division points on the corresponding curves. In fact, from $D=-19$ onwards, 3-division points would suffice and be much easier to deal with. We will discuss how it could be that Deuring didn't have our Theorem in general in Section 5. We will also see in Sections 3 and 5 that, for any fixed $D$, verifying that Theorem 1 gives the correct number of points on a curve $E_1$ reduced $(\mathrm{mod}\,\mathfrak{P})$ for a single prime $\pi\equiv 1+2\theta \pmod 4$ suffices to prove the result of Theorem 1 for that particular curve. For

example, counting the number of points for the primes $\pi = 6 + \sqrt{-11}$ for $D = -11$ ($u = 12, p = 47$) and $\pi = 2 + \sqrt{D}$ for $D = -7$, $D = -19$, $D = -43$, $D = -67$, $D = -163$, $D = -427$ ($u = 4$ in each case and $p = 11$, $p = 23$, $p = 47$, $p = 71$, $p = 167$, $p = 431$, respectively) completely suffices to prove the results of our examples above without having to apply the general reciprocity law. Rumely [**7**] was the first to indicate that the general reciprocity law could produce a theorem such as Theorem 1 but did not carry out the required calculation. The six class-number one examples above were announced over a decade ago and Rajwade [**5**] already refers to them.

**2. The needed functions of level $N$.** Let $\Omega$ be the lattice corresponding to the curve $E$ in (1). We suppose that $\Omega$ is generated by the two periods $\omega_1$ and $\omega_2$ oriented so that $\omega_1/\omega_2$ is in the upper half plane. The curve $E$ is parameterized by the Weierstrass $\wp$-function,

$$x = \wp(w;\Omega) = w^{-2} + \sum_{\omega\in\Omega}{}' [(w+\omega)^{-2} - \omega^{-2}],$$

(where $\sum'$ means the sum over all nonzero periods) and its derivative,

$$y = \wp'(w;\Omega) = -2\sum_{\omega\in\Omega} (w+\omega)^{-3}.$$

We also have

$$g_2 = g_2(\Omega) = 60\sum_{\omega\in\Omega}{}' \omega^{-4},$$

and

$$g_3 = g_3(\Omega) = 140\sum_{\omega\in\Omega}{}' \omega^{-6}.$$

If $w$ is of the form $w = (r\omega_1 + s\omega_2)/N$, where $r$ and $s$ are both integers at least one of which is not divisible by $N$, then $g_2(\Omega)$, $g_3(\Omega)$, $\wp(w;\Omega)$ and $\wp'(w;\Omega)$ are all (homogeneous) modular forms of level $N$. The reciprocity law which we will use applies to modular functions with cyclotomic Fourier coefficients. This will require rescaling the lattice $\Omega$. The rescaling constant we will use is

$$\kappa = \left(\frac{2\pi i}{\omega_2}\right)\eta(z)^2, \quad \text{where} \quad z = \omega_1/\omega_2.$$

Let

$$\begin{aligned} X(z) = X_{r,s}(z) &= \kappa^{-2}\wp(w;\Omega) \\ &= (2\pi i)^{-2}\wp((rz+s)/N;\omega_2^{-1}\Omega)/\eta(z)^4 \end{aligned}$$

and

$$\begin{aligned} Y(z) = Y_{r,s}(z) &= \kappa^{-3}\wp'(w;\Omega) \\ &= (2\pi i)^{-3}\wp'((rz+s)/N;\omega_2^{-1}\Omega)/\eta(z)^6. \end{aligned}$$

When we multiply (1) through by $\kappa^{-6}$, we get

$$Y^2 = 4X^3 - \kappa^{-4}g_2(\Omega)X - \kappa^{-6}g_3(\omega).$$

Let $E_4(z)$ and $E_6(z)$ be the standard Eisenstein series of weights 4 and 6, respectively, on the full modular group, normalized to be 1 at $i\infty$. Since $\omega_2^4 g_2(\Omega) = 60 \cdot 2\zeta(4)E_4(z) = (4\pi^4/3)E_4(z)$, we see that

$$\kappa^{-4}g_2(\Omega) = \frac{E_4(z)}{12\eta(z)^8} = \frac{1}{12}\gamma_2(z).$$

Likewise, since $\omega_2^6 g_3(\Omega) = 140 \cdot 2\zeta(6)E_6(z) = (8\pi^6/27)E_6(z)$, we see that

$$\kappa^{-6}g_3(\Omega) = -\frac{E_6(z)}{216\eta(z)^{12}} = -\frac{1}{216}\gamma_3(z).$$

In summary, $(X(z), Y(z))$ is an $N$-division point on the rescaled curve,

$$Y^2 = 4X^3 - \frac{1}{12}\gamma_2(z)X + \frac{1}{216}\gamma_3(z). \tag{3}$$

We take $k = \mathbf{Q}(\sqrt{D})$ where $D$ is a discriminant of a complex quadratic field, $(D, 6) = 1$. In particular, for $\theta = (-3 + \sqrt{D})/2$, both $\gamma_2(\theta)$ and $\gamma_3(\theta)$ are algebraic integers in $H$, the Hilbert class field of $k$. For this reason, when $z = \theta$, the rescaling above will be suitable for the curves we will look at, but other rescalings would be required for other classes of curves.

Throughout this and the next section, $r$ and $s$ will be presumed to be integers, at least one of which isn't divisible by $N$. The critical modular functions in this paper are the functions $X_{r,s}(z)$ and $Y_{r,s}(z)$. Everything will ultimately depend upon $Y_{r,s}(z)$. To be in the field of functions of level $M$, say, these functions must both be invariant under $\Gamma(M)$ and have their Fourier coefficients at every cusp in $\mathbf{Q}(\zeta_M)$ where

$\zeta_M = \exp(2\pi i/M)$. The transformations under the full modular group are easy to establish.

For any elliptic function $f(w, \Omega)$, such as $\wp$ and $\wp'$, which varies analytically with the lattice $\Omega$, we set

$$\begin{aligned} f_{r,s}\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} &= f\left(\frac{1}{N}(r,s)\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}; \begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}\right) \\ &= f((r\omega_1 + s\omega_2)/N; \Omega). \end{aligned}$$

It is important to note that $f_{r,s}$ depends only on the values of $r$ and $s (\mathrm{mod}\ N)$. For $A$ in the modular group, we have

$$\begin{aligned} f_{r,s}\left(A\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}\right) &= f\left(\frac{1}{N}(r,s)A\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}; A\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}\right) \\ &= f_{(r,s)A}\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}. \end{aligned}$$

In particular, if $A$ is in $\Gamma(N)$, then

$$\begin{aligned} \frac{1}{N}(r,s)A &\equiv \frac{1}{N}(r,s) + \frac{1}{N}(r,s)(A - I) \\ &\equiv \frac{1}{N}(r,s) \pmod 1 \end{aligned}$$

and so

$$f_{r,s}\left(A\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}\right) = f_{r,s}\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}.$$

Thus, we see that $\wp((r\omega_1 + s\omega_2)/N; \Omega)$ and $\wp'((r\omega_1 + s\omega_2)/N; \Omega)$ are homogeneous modular forms of level $N$ (with no conditions yet on the Fourier coefficients) and weights 2 and 3, respectively.

Next we quickly examine the algebraic nature of the Fourier coefficients. For this, we do not need a simplified expression,but only an expansion where the arithmetic nature of the coefficients is plain. Recall the usual formula

$$\pi \cot \pi z = \sum (n + z)^{-1}$$

and also as a $q$-series when $z$ is in the upper half plane,

$$\begin{aligned}\pi \cot \pi z &= \pi i \frac{q^{1/2}+q^{-1/2}}{q^{1/2}-q^{-1/2}} \\ &= -\pi i \frac{1+q}{1-q} \\ &= -\pi i - 2\pi i \sum_{n=1}^{\infty} q^n.\end{aligned}$$

The derivative series is

$$-\sum (n+z)^{-2} = -(2\pi i)^2 \sum_{n=1}^{\infty} n q^n = -\pi^2 \csc^2 \pi z$$

and the next derivative series is

$$\begin{aligned}2\sum (n+z)^{-3} &= -(2\pi i)^3 \sum_{n=1}^{\infty} n^2 q^n \\ &= 2\pi^3 \csc^2 \pi z \cot \pi z.\end{aligned}$$

We now get the $q$-expansion,

$$\begin{aligned}&\frac{-2}{(2\pi i)^3} \sum\sum \left[\left(m+\frac{r}{N}\right)z + \left(n+\frac{s}{N}\right)\right]^{-3} \\ &\qquad = \sum_{\substack{m \\ (Nm+r)>0}} \sum_{n=1}^{\infty} n^2 e^{2\pi i n[(Nm+r)z+s]/N} \\ &\qquad\quad - \sum_{\substack{m \\ (Nm+r)<0}} \sum_{n=1}^{\infty} n^2 e^{2\pi i n[-(Nm+r)z-s]/N} \\ &\qquad\quad + \sum_{\substack{m \\ (Nm+r)=0}} \frac{2\pi^3}{-(2\pi i)^3} \csc^2\left(\frac{\pi s}{N}\right) \cot\left(\frac{\pi s}{N}\right).\end{aligned}$$

As far as algebraic properties of the coefficients go,

$$\begin{aligned}\frac{2\pi^3}{-(2\pi i)^3} \csc^2\left(\frac{\pi s}{N}\right) \cot\left(\frac{\pi s}{N}\right) &= -\frac{2}{(2i)^3} \frac{\cos(\pi s/N)}{\sin^3(\pi s/N)} \\ &= -\frac{\zeta_{2N}^s + \zeta_{2N}^{-s}}{(\zeta_{2N}^s - \zeta_{2N}^{-s})^3} \\ &= -\frac{\zeta_N^s(\zeta_N^s+1)}{(\zeta_N^s-1)^3}.\end{aligned}$$

Therefore, with $q_N = e^{2\pi iz/N}$,

$$\frac{-2}{(2\pi i)^3}\sum\sum\left[\left(m+\frac{r}{N}\right)z+\left(n+\frac{s}{N}\right)\right]^{-3}$$
$$= \sum_{\substack{m\\ mN+r>0}}\sum_{n=1}^{\infty} n^2\zeta_N^{ns}q_N^{(mN+r)}$$
$$- \sum_{\substack{m\\ mN+r<0}}\sum_{n=1}^{\infty} n^2\zeta_N^{-ns}q_N^{-n(mN+r)}$$
$$- \sum_{\substack{m\\ mN+r=0}}\frac{\zeta_N^s(\zeta_N^s+1)}{(\zeta_N^s-1)^3}.$$

So long as $r$ and $s$ are not both divisible by $N$, there is no blow up on either side. We have shown that $(2\pi i/\omega_2)^{-3}\wp'((r\omega_1+s\omega_2)/N;\Omega)$ has a power series in $q_N = \exp(2\pi iz/N)$ where $z = \omega_1/\omega_2$ and where the coefficients (the "Fourier coefficients") are all in $\mathbf{Q}(\zeta_N)$. Indeed, every coefficient is a rational function of $\zeta_N^s$ with rational coefficients. This is important because it enables us to easily see what an algebraic conjugation of the Fourier coefficients does.

Although messier because of the extra $\omega^{-2}$ terms which doubles the work, the expansion of the function $(2\pi i/\omega_2)^{-2}\wp((r\omega_1+s\omega_2)/N;\Omega)$ is found similarly. The expansion is well known and can be found, for example, in Lang [**3**]. Again, the result is a power series in $q_N$ with the Fourier coefficients all in $\mathbf{Q}(\zeta_N)$ and, indeed, each coefficient is again a rational function of $\zeta_N^s$ with rational coefficients.

We are interested in the modular functions $X_{r,s}(z)$ and $Y_{r,s}(z)$ which have extra quotients by $\eta(z)^4$ and $\eta(z)^6$, respectively. These modular forms transform in the following manner under a matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

in the full modular group $\Gamma$:

$$\eta(A\circ z)^4 = \zeta_6(A)(cz+d)^2\eta(z)^4,$$
$$\eta(A\circ z)^6 = \zeta_4(A)(cz+d)^3\eta(z)^6,$$

where $A \circ z = (az+b)/(cz+d)$, $\zeta_6(A) = \zeta_{12}(A)^2$ is a sixth root of unity, $\zeta_4(A) = \zeta_{12}(A)^3$ is a fourth root of unity and $\zeta_{12}(A)$ is the twelfth root of unity appearing in the transformation formula of $\eta(z)^2$. It is well known that $\zeta_{12}(A)$ is a twelfth root of unity, and there are even classical formulae for it. For example, according to Weber [**13**], when $d$ is odd,

$$\zeta_{12}(A) = (-1)^{(d-1)/2}\zeta_{12}^{[d(b-c)-(d^2-1)ac]}, \tag{4}$$

and, when $c$ is odd,

$$\zeta_{12}(A) = (-1)^{(1-c)/2}\zeta_{12}^{[c(a+d)-(c^2-1)bd-3]}. \tag{5}$$

(Warning: Weber's ordering of $a$, $b$, $c$ and $d$ differs from ours!) Weber gives the twenty-fourth root of unity in the transformation formula for $\eta(z)$ with the extra restriction that $d$ is odd and positive in the first case and that $c$ is odd and positive in the second. But for $\zeta_{12}(A)$, this positivity restriction is unnecessary since the righthand side is multiplied by $-1$ when $A$ is replaced by $-A$ as it ought to be for a modular form of weight one.

From the first of these formulae, we see that $\zeta_6(A) = 1$ for $A$ in $\Gamma(6)$ and $\zeta_4(A) = 1$ for $A$ in $\Gamma(4)$. Thus, $\eta(z)^4$ is of weight 2, level 6 and is invariant under the full modular group up to a multiplier which is a sixth root of unity. Likewise, $\eta(z)^6$ is of weight 3, level 4 and is invariant under the full modular group up to a multiplier which is a fourth root of unity. Therefore, $X_{r,s}(z)$ is in the field of modular functions of level $\operatorname{lcm}(N,6)$ and $Y_{r,s}(z)$ is in the field of modular functions of level $\operatorname{lcm}(N,4)$. Thus, at the very worst, $X_{r,s}(z)$ and $Y_{r,s}(z)$ are both modular functions in the field of functions of level $12N$.

**3. The reciprocity law.** Suppose that $k = \mathbf{Q}(\sqrt{D})$ is a complex quadratic field and that $\mathfrak{a} = [\alpha, \beta]$ where $[\alpha, \beta]$ is an integral basis for an ideal $\mathfrak{a}$ of $k$. We order $\alpha$ and $\beta$ so that $\theta = \alpha/\beta$ is in the upper half plane. (In our application in this paper, $\theta$ will be $(-3+\sqrt{D})/2$.) Suppose that $\mathfrak{p}$ is a first degree principal prime ideal in $k$ of norm $p$. If $f(z)$ is in the field of modular functions of level $M$, then $f(\theta)$ is in the ray class field $K(M)$ of $k \pmod M$. When the Fourier coefficients of $f(z)$ at every cusp are integral at $p$ and $f(z)$ is analytic in the interior of the upper half plane, $f(\theta)$ is then integral at $p$ and the reciprocity

law gives the action of the algebraic Frobenius automorphism applied to $f(\theta)$. This action is computed in two parts. One part changes the function $f(z)$ and the other part changes the point $\theta$.

In the version of the reciprocity law in Stark [**12**], both of these changes are found from an auxiliary matrix of integers $B$ which is defined by

$$\begin{pmatrix} \rho \\ \tau \end{pmatrix} = B \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \tag{6}$$

where $[\rho, \tau]$ is an integral basis for $\bar{\mathfrak{p}}\alpha$, ordered so that $\rho/\tau$ is in the upper half plane. The matrix $B$ has determinant $p$. The function change takes $f$ to $f \circ (pB^{-1})$. In [**12**], a recipe is given for calculating $f \circ (pB^{-1})$. If

$$f(z) = \sum_n a_n q_M^n,$$

with coefficients in $\mathbf{Q}(\zeta_M)$, set

$$f^{\sigma_p}(z) = \sum_n a_n^{\sigma_p} q_M^n,$$

where $\sigma_p$ is the automorphism of $\mathbf{Q}(\zeta_M)$ taking $\zeta_M$ to $\zeta_M^p$.

Write, as is always possible,

$$pB^{-1} \equiv \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} A \pmod{M}$$

where $A$ is in the modular group. Then

$$f \circ (pB^{-1})(z) = f^{\sigma_p}(A \circ z).$$

The reciprocity law is expressed in terms of the fundamental congruence

$$f(\theta)^p \equiv f \circ (pB^{-1})(B \circ \theta) \pmod{{}^*\mathfrak{p}}. \tag{7}$$

Here, $(\mathrm{mod}\, {}^*\mathfrak{p})$ is Hasse's notation meaning that the difference has a factor of $\mathfrak{p}$ in the numerator. For the applications in this paper, everything will be integral outside of $6N$ and so the congruences could

equally well be thought of as regular congruences in the $S$-integers of $k$ where $S$ consists of all primes in $k$ dividing $6N$.

In this paper we need only a special case of the reciprocity law. We continue to assume that the discriminant of $k$ satisfies $(D,6)=1$ and take $\theta=(-3+\sqrt{D})/2$. In particular, $[\theta,1]$ is an integral basis for $k$. We will apply the reciprocity law to the ideal $\mathfrak{a}=(1)=[\theta,1]$. From this point on, the letter $\pi$ will be the generator of a first degree principal prime ideal $\mathfrak{p}$ in $k$ of norm $p$. We assume that $p\nmid 12N$. We may define the matrix $B$ of determinant $p$ in the reciprocity law in this special case by

$$\bar{\pi}\begin{pmatrix}\theta\\1\end{pmatrix}=B\begin{pmatrix}\theta\\1\end{pmatrix}. \tag{8}$$

Again for a function $f(z)$ of the type above where $M=12N$, $f(\theta)$ is integral at $p$ and the fundamental congruence states that

$$\begin{aligned} f(\theta)^p &\equiv f\circ(pB^{-1})(B\circ\theta) \pmod{{}^*\pi}\\ &\equiv f\circ(pB^{-1})(\theta) \pmod{{}^*\pi}, \end{aligned}$$

since in our situation we see from (8) that $B\circ\theta=\theta$. We introduce a matrix $A$ in the modular group by

$$pB^{-1}\equiv\begin{pmatrix}1&0\\0&p\end{pmatrix}A \pmod{12N}. \tag{9}$$

The whole task is then to calculate $f\circ(pB^{-1})$.

Let

$$X=X_{r,s}(\theta),\qquad Y=Y_{r,s}(\theta).$$

Since $\gamma_2(\theta)$ and $\gamma_3(\theta)$ are in the Hilbert class field, when we set $z=\theta$ in (3) and raise both sides to the $p$th power and reduce $(\mathrm{mod}\,\mathfrak{P})$, we get

$$(Y^p)^2\equiv 4(X^p)^3-\frac{1}{12}\gamma_2(\theta)(X^p)+\frac{1}{216}\gamma_3(\theta) \pmod{{}^*\mathfrak{P}}.$$

The point $(X,Y)$ is an $N$-division point on this curve and as such has coordinates in the ray class field $(\mathrm{mod}\,12N)$ of $k$. From the expansions in Section 2, we see that $\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)$ acts on $X$ and $Y$ by

$$X_{(r,s)}\circ\begin{pmatrix}1&0\\0&p\end{pmatrix}=X_{(r,sp)}$$

and

$$Y_{(r,s)} \circ \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} = Y_{(r,sp)}.$$

In homogeneous form, we see that for $A$ in $\Gamma$ and $t = 0$ or 1,

$$\wp^{(t)}\left(\frac{1}{N}(r,sp)A\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}; A\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}\right) = \wp^{(t)}\left(\frac{1}{N}(r,sp)A\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix};\Omega\right)$$

and therefore with $A$ given by (9),

$$(X_{(r,s)} \circ pB^{-1})(z) = \zeta_6(A)^{-1} X_{(r,sp)A}(z),$$
$$(Y_{(r,s)} \circ pB^{-1})(z) = \zeta_4(A)^{-1} Y_{(r,sp)A}(z),$$

where $\zeta_6(A)$ and $\zeta_4(A)$ are the sixth and fourth roots of unity appearing in the transformation formulae of $\eta(z)^4$ and $\eta(z)^6$ above. Since

$$(r,sp)A = (r,s)\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}A \equiv (r,s)pB^{-1} \pmod{12N},$$

we find that

$$(X_{(r,s)} \circ pB^{-1})(\theta) = \zeta_6(A)^{-1} X_{(r,s)pB^{-1}}(\theta),$$

and

$$(Y_{(r,s)} \circ pB^{-1})(\theta) = \zeta_4(A)^{-1} Y_{(r,s)pB^{-1}}(\theta).$$

Multiplying (8) through by $\pi$ shows that $pB^{-1}$ satisfies

$$pB^{-1}\begin{pmatrix}\theta\\ 1\end{pmatrix} = \pi\begin{pmatrix}\theta\\ 1\end{pmatrix}. \tag{10}$$

Hence if $\Omega = [\omega_1, \omega_2]$ is a lattice with $\omega_1/\omega_2 = \theta$ and $w = (r\omega_1 + s\omega_2)/N$, then

$$\frac{1}{N}(r,s)pB^{-1}\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} = \frac{1}{N}(r,s)\pi\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} = \pi w.$$

Therefore, the reciprocity congruence gives

$$X^p \equiv \zeta_6(A)^{-1}\pi \circ X \pmod{{}^*\pi},$$
$$Y^p \equiv \zeta_4(A)^{-1}\pi \circ Y \pmod{{}^*\pi},$$

where $\pi \circ X$ and $\pi \circ Y$ are the $x$ and $y$ coordinates of complex multiplication of $(X, Y)$ by $\pi$. It is a remarkable fact that, in our situation, $\zeta_6(A)$ is always 1. Although easily verified directly, we do not need to do so here because we are dealing with the case that $\gamma_2(\theta)$ and $\gamma_3(\theta)$ are already known to be in the Hilbert class field. Since $\gamma_2(z) = E_4(z)/\eta(z)^8$, $\gamma_3(z) = E_6(z)/\eta(z)^{12}$ and $E_4(z)$ and $E_6(z)$ are modular forms of level 1 with rational Fourier coefficients. The recipe for the reciprocity congruence gives

$$\gamma_2(\theta)^p \equiv \zeta_{12}(A)^{-4}\gamma_2(\theta) \pmod{\pi},$$
$$\gamma_3(\theta)^p \equiv \zeta_{12}(A)^{-6}\gamma_3(\theta) \pmod{\pi}.$$

Since $\gamma_2(\theta)$ and $\gamma_3(\theta)$ are nonzero when $(D, 6) = 1$ and $\gamma_2(\theta)$ and $\gamma_3(\theta)$ are in $H$ and so preserved by the Frobenius congruence, this gives $\zeta_{12}(A)^4 = \zeta_{12}(A)^6 = 1$ and hence $\zeta_6(A) = \zeta_{12}(A)^2 = 1$. (Actually, the current proofs using the explicit reciprocity law which show that $\gamma_2(\theta)$ and $\gamma_3(\theta)$ are in the Hilbert class field are carried out by showing that $\zeta_{12}(A)^4 = \zeta_{12}(A)^6 = 1$.) In turn, this shows that $\zeta_4(A) = \pm 1$. Indeed, either from raising the equation for the curve to the $p$th power leaving only an ambiguity of $\pm Y$, or from noting that $\zeta_4(A)^2 = \zeta_{12}(A)^6 = 1$, we get this. Therefore, we have either

$$(X^p, Y^p) \equiv \pi \circ (X, Y) \pmod{{}^*\pi}$$

when $\zeta_4(A) = 1$ or

$$(X^p, Y^p) \equiv -\pi \circ (X, Y) \pmod{{}^*\pi}$$

when $\zeta_4(A) = -1$.

This already carries enough information to give a proof that complex multiplication by $\pi$ reduces $(\mathrm{mod}\,\pi)$ to either plus or minus Frobenius. In fact, it is well known that multiplication by $\pi$ gives an $x$-coordinate that is a rational function of $X$ alone. Upon reduction $(\mathrm{mod}\,\pi)$, this rational function agrees with $X^p$ for infinitely many values of $X$ over $\bar{\mathbf{F}}_p$, the algebraic closure of $\mathbf{F}_p$ (namely the reductions of the $x$-coordinates of $N$-division points which generate higher and higher degree ray class fields over $H = K(1)$ in which the primes above $(\pi)$ have arbitrarily high degree). Therefore, reduced $(\mathrm{mod}\,\pi)$, this rational function is $X^p$. From this, we now get that multiplication by $\pi$ of the $y$-coordinate reduces to $\pm Y^p$.

We also have enough information to see that there is a Grössencharacter involved here. Indeed, let $\varepsilon(\pi) = \pm 1$ be defined by

$$Y^p \equiv \varepsilon(\pi)\pi \circ Y \pmod{\pi},$$

i.e., $\varepsilon(\pi) = \zeta_4(A)^{-1}$. Then clearly

$$\varepsilon(-\pi) = -\varepsilon(\pi).$$

Thus $\varepsilon(\pi)\pi$ gives a well-defined generator of $(\pi)$ independent of the choice of $\pi$. Further, this generator is independent of which $N$ division point is used since $A$ is independent of $r$ and $s$. Suppose that $4|N$. Then $Y$ is in $K(N)$. We also see that $\varepsilon(\pi)\pi \circ Y$ is independent of which $(\pi)$ is chosen from its ray class $(\mathrm{mod}\, N)$. (Perhaps the most elementary reason is that if $\pi_1 \equiv \pi_2 \pmod{N}$, then $Y(\pi_1\theta) = Y(\pi_2\theta)$.) In particular, $\varepsilon(\pi)$ depends only upon the choice of $\pi \pmod{N}$. This allows us to define $\varepsilon$ on any congruence class $(\mathrm{mod}\, N)$ which is relatively prime to $N$.

Let $C_1, C_2$ and $C_3$ be ray classes $(\mathrm{mod}\, N)$ contained in the principal ideal class with $C_1C_2 = C_3$, and let $\sigma_1, \sigma_2, \sigma_3$ be the corresponding Frobenius automorphisms in $G(K(N)/k)$. Further, let $\pi_1, \pi_2, \pi_3$ generate first degree primes in $C_1, C_2, C_3$. Then we see that

$$Y \circ \sigma_j = \varepsilon(\pi_j)\pi_j \circ Y.$$

Hence

$$\begin{aligned}\varepsilon(\pi_3)\pi_3 \circ Y = Y \circ \sigma_1\sigma_2 &= [\varepsilon(\pi_1)\pi_1 \circ Y] \circ \sigma_2 \\ &= \varepsilon(\pi_1)\varepsilon(\pi_2)\pi_1\pi_2 \circ Y.\end{aligned}$$

If $\pi_3$ is chosen from the two possibilities so that $\pi_3 \equiv \pi_1\pi_2 \pmod{N}$, then we see that

$$\varepsilon(\pi_1\pi_2) = \varepsilon(\pi_1)\varepsilon(\pi_2).$$

This proves that $\varepsilon$ is a multiplicative numerical character $(\mathrm{mod}\, N)$ when $4|N$ and, indeed, we may as well take $N = 4$.

Since we are dealing with the case that $D$ is odd, $(\mathfrak{o}_k/4)^*$ is a group with either 4 or 12 elements according to whether 2 splits in $k$ ($D \equiv 1 \pmod{8}$) or is inert in $k$ ($D \equiv 5 \pmod{8}$). In either case, including the trivial character, there are four numerical characters

(mod 4) taking the values $\pm 1$. On the four element subgroup of classes $\equiv 1 \pmod 2$ of $(\mathfrak{o}_k/4)^*$, these four characters are

| | 1 | $-1$ | $1+2\theta$ | $-1+2\theta$ |
|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | 1 | $-1$ | $-1$ |
| $\chi_3$ | 1 | $-1$ | 1 | $-1$ |
| $\chi_4$ | 1 | $-1$ | $-1$ | 1 |

Indeed, if $(\alpha, 4) = 1$, then for a character $\chi$ of order two on $(\mathfrak{o}_k/4)^*$, $\chi(\alpha) = \chi(\alpha)^3 = \chi(\alpha^3)$ and $\alpha^3$ is in the four element subgroup of classes $\equiv 1 \pmod 2$. Thus, each of the four listed characters uniquely extends to a character of order two on the whole group $(\mathfrak{o}_k/4)^*$. Only $\chi_3$ and $\chi_4$ are possibilities for $\varepsilon$ since $\varepsilon(-\pi) = -\varepsilon(\pi)$ eliminates the first two characters. In fact, both $\chi_1$ and $\chi_2$ are ideal characters (mod 4); $\chi_1$ is the trivial character and $\chi_2$ corresponds to the quadratic extension $k(\sqrt{-1})$ of $k$, $\chi_2(\pi) = (-1/p)$.

The time has come to calculate $\zeta_4(A)$. Write $\pi = m + n\theta$ where $\theta = (-3 + \sqrt{D})/2$ is a root of $z^2 + 3z + (9 - D)/4 = 0$. We have

$$\pi \begin{pmatrix} \theta \\ 1 \end{pmatrix} = \begin{pmatrix} m\theta + n\theta^2 \\ m + n\theta \end{pmatrix} = \begin{pmatrix} (m - 3n)\theta + n(D-9)/4 \\ n\theta + m \end{pmatrix}$$
$$= \begin{pmatrix} m - 3n & n(D-9)/4 \\ n & m \end{pmatrix} \begin{pmatrix} \theta \\ 1 \end{pmatrix}$$

and hence, by (10),

$$pB^{-1} = \begin{pmatrix} m - 3n & n(D-9)/4 \\ n & m \end{pmatrix},$$

a matrix of determinant $p = \mathbf{N}(\pi)$. Therefore $A$ is determined (mod 4) from this by (9) as

$$A \equiv \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} pB^{-1} \equiv \begin{pmatrix} m - 3n & n(D-9)/4 \\ pn & pm \end{pmatrix} \pmod 4.$$

Since $\pi \pmod 4$ determines $m, n$ and $p \pmod 4$, the matrix $A \pmod 4$ depends only upon $\pi \pmod 4$.

From the expression for $\zeta_{12}(A)$ in (4) above, if $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is an integral matrix of determinant 1, and $d$ is odd, then

$$\begin{aligned}\zeta_4(A) &= (-1)^{3(d-1)/2} i^{\,[d(b-c)-(d^2-1)ca]} \\ &= (-1)^{(d-1)/2} i^{\,d(b-c)}.\end{aligned}$$

Hence, when $m$ is odd,

$$\begin{aligned}\zeta_4(A) &= (-1)^{(pm-1)/2} i^{\,pm[n(D-9)/4-pn]} \\ &= (-1)^{(pm-1)/2} i^{\,pmn(D-9)/4-mn}.\end{aligned} \tag{11}$$

Although knowledge of $\zeta_4(A)$ for all $A$ gives us a formula for $\varepsilon$ for every element of the group $(\mathfrak{o}_k)/4^*$, it suffices to determine $\varepsilon(1+2\theta)$ to decide whether $\varepsilon$ is $\chi_3$ or$\chi_4$. Suppose that

$$\pi \equiv 1 + 2\theta \pmod 4,$$

so that $m \equiv 1 \pmod 4$, $n \equiv 2 \pmod 4$, and $p = m^2 - 3mn + n^2(9 - D)/4 \equiv 3 \pmod 4$. From (11), we find that when $\pi \equiv 1+2\theta \pmod 4$,

$$\begin{aligned}\zeta_4(A) &= (-1)^{(3-1)/2} i^{\,6(D-9)/4-2} \\ &= (-1)^{(D-9)/4} \\ &= \begin{cases} 1 & D \equiv 1 \pmod 8 \\ -1 & D \equiv 5 \pmod 8 \end{cases}.\end{aligned}$$

Therefore,

$$\varepsilon = \begin{cases} \chi_3 & \text{if } D \equiv 1 \pmod 8 \\ \chi_4 & \text{if } D \equiv 5 \pmod 8. \end{cases}$$

Anyone wishing to directly verify our evaluation of $\varepsilon(\pi)$ for all residue classes of $\pi \pmod 4$ would need both versions (4) and (5) of Weber's formula for $\zeta_{12}(A)^3$; the point of the presentation here is that one select residue class suffices.

**4. A further rescaling of the curve.** Now we wish to rescale the curve in order to bring down the field of definition from $H$ to $H^+$. If

$\alpha$ is in $H$ with numerator and denominator relatively prime to $\mathfrak{P}$, we may rescale by multiplying (3) with $z = \theta$ through by $\alpha^3$. With

$$x = \alpha X, \qquad y = \alpha^{3/2} Y,$$

we have

$$y^2 = 4x^3 - \alpha^2 \frac{\gamma_2}{12} x + \alpha^3 \frac{\gamma_3}{216}. \tag{12}$$

Since $(\pi)$ splits completely in $H$, $\alpha$ is preserved by the Frobenius map, but

$$(\alpha^{1/2})^p \equiv \left(\frac{\alpha}{\mathfrak{P}}\right) \alpha^{1/2} \pmod{{}^*\mathfrak{P}}.$$

Therefore, $(\alpha/\mathfrak{P})\varepsilon(\pi)\pi$ serves as the Frobenius automorphism when the curve (12) is reduced $(\mathrm{mod}\,\mathfrak{P})$.

A particular case is of interest. This is the case where

$$\alpha = a\sqrt{D},$$

with $a$ in $H^+$ with numerator and denominator relatively prime to $\mathfrak{P}$. The curve (12) takes the shape

$$y^2 = 4x^3 - a^2 D \frac{\gamma_2}{12} x + a^3 D \frac{\gamma_3 \sqrt{D}}{216} \tag{13}$$

which is the curve $E_a$ in Theorem 1. Here $(a/\mathfrak{P})(\sqrt{D}/\mathfrak{P})\varepsilon(\pi)\pi$ serves as the Frobenius automorphism for this curve when it is reduced $(\mathrm{mod}\,\mathfrak{P})$.

Since $\mathfrak{P}$ is a first degree prime ideal of $H$ just as $(\pi)$ is of $k$ and since $\sqrt{D}$ is in $k$,

$$\left(\frac{\sqrt{D}}{\mathfrak{P}}\right) = \left(\frac{\sqrt{D}}{\pi}\right).$$

The Legendre symbol on the right tells us how $(\pi)$ splits in $k_2 = k((\sqrt{D})^{1/2})$ and, according to the reciprocity law, this is governed by a quadratic character with conductor precisely the relative discriminant of $k_2/k$. This relative discriminant in turn divides the polynomial discriminant $4\sqrt{D}$ of the defining polynomial $x^2 - \sqrt{D}$ of $k_2/k$ and differs from this polynomial discriminant by a square ideal factor in $k$.

Thus $\sqrt{D}$ is present in the conductor. Since there is only one numerical quadratic character (mod$\sqrt{D}$) with conductor $\sqrt{D}$, we must have

$$\left(\frac{\sqrt{D}}{\pi}\right) = \left(\frac{\pi}{\sqrt{D}}\right)\psi(\pi), \tag{14}$$

where $\psi(\pi)$ is a numerical quadratic or trivial character (mod 4) whose conductor is a square and divides 4. Thus $\psi$ is one of the four characters $\chi_1$, $\chi_2$, $\chi_3$, $\chi_4$ defined above. But, further, the left side of (14) depends only on the ideal $(\pi)$ and so is the same whether we are dealing with either $\pm\pi$. On the other hand, since

$$\left(\frac{-1}{\sqrt{D}}\right) = \left(\frac{-1}{|D|}\right) = -1,$$

we see that

$$\psi(-1) = -1.$$

Thus $\psi$ is either $\chi_3$ or $\chi_4$, and it remains to determine which. In fact, for the case that $D \equiv 1 \pmod 8$ where 2 splits in $k$ as $\mathfrak{p}_2\bar{\mathfrak{p}}_2$, with $\mathfrak{p}_2 = (2, \theta)$ and $\bar{\mathfrak{p}}_2 = (2, \theta + 1)$, general theory determines $\psi$ since the relative discriminant of $k_2/k$ is precisely $\mathfrak{p}_2^2\sqrt{D}$. Indeed, set $x = y + 1$ in the defining polynomial $x^2 - \sqrt{D}$ getting $y^2 + 2y + 1 - \sqrt{D}$ where $1 - \sqrt{D} = -2 - 2\theta$ which is divisible by $\mathfrak{p}_2$ only once but by $\bar{\mathfrak{p}}_2^2$. Thus, the power of $\mathfrak{p}_2$ in the polynomial discriminant is correct, but the power of $\bar{\mathfrak{p}}_2$ comes down by 2. Hence, $\psi$ has conductor precisely $\mathfrak{p}_2^2$. The conductor of $\chi_3$ is $\mathfrak{p}_2^2$ while the conductor of $\chi_4$ is $\bar{\mathfrak{p}}_2^2$. Therefore, for $D \equiv 1 \pmod 8$, $\psi = \chi_3$. However, for $D \equiv 5 \pmod 8$, an instance which includes the most interesting class-number one examples, $\psi$ has conductor (4), both $\chi_3$ and $\chi_4$ are primitive characters (mod 4), and so knowledge of the exact conductor does not distinguish between the two possibilities for us.

For this, we need the explicit quadratic reciprocity law in number fields. In the process, we will rederive the desired result for $D \equiv 1 \pmod 8$. Again, choose a prime $\pi$ such that

$$\pi \equiv 1 + 2\theta \equiv 2 + \sqrt{D} \pmod 4.$$

Since both $\pi$ and $\sqrt{D}$ are congruent to 1 (mod 2) and since $k$ is complex, Siegel [**10**] tells us that

$$\begin{aligned}\psi(1+2\theta) = \psi(\pi) &= \left(\frac{\sqrt{D}}{\pi}\right)\left(\frac{\pi}{\sqrt{D}}\right)\\ &= (-1)^{\mathrm{tr}\left[\left(\frac{\pi-1}{2}\right)\left(\frac{\sqrt{D}-1}{2}\right)\right]}\\ &= (-1)^{\mathrm{tr}\left[\theta\left(\frac{\sqrt{D}-1}{2}\right)\right]}\\ &= (-1)^{\mathrm{tr}\left[\left(\frac{\sqrt{D}-3}{2}\right)\left(\frac{\sqrt{D}-1}{2}\right)\right]}\\ &= 1.\end{aligned}$$

Thus $\psi = \chi_3$ always. Hence, the Frobenius automorphism for the curve $E_a$ is given by

$$\begin{aligned}\left(\frac{a}{\mathfrak{P}}\right)\left(\frac{\sqrt{D}}{\mathfrak{P}}\right)\varepsilon(\pi)\pi &= \left(\frac{a}{\mathfrak{P}}\right)\left(\frac{\pi}{\sqrt{D}}\right)\chi_3(\pi)\varepsilon(\pi)\pi\\ &= \begin{cases}\left(\frac{a}{\mathfrak{P}}\right)\left(\frac{\pi}{\sqrt{D}}\right)\pi & \text{if } D \equiv 1 \pmod 8\\ \left(\frac{-a}{\mathfrak{P}}\right)\left(\frac{\pi}{\sqrt{D}}\right)\pi & \text{if } D \equiv 5 \pmod 8.\end{cases}\end{aligned}$$

Now write

$$\pi = \frac{u + v\sqrt{D}}{2}.$$

We have

$$\left(\frac{\pi}{\sqrt{D}}\right) = \left(\frac{4\pi}{\sqrt{D}}\right) = \left(\frac{2u}{\sqrt{D}}\right) = \left(\frac{2u}{|D|}\right).$$

Therefore

$$\begin{aligned}\pi' &= \left(\frac{a}{\mathfrak{P}}\right)\left(\frac{\sqrt{D}}{\mathfrak{P}}\right)\varepsilon(\pi)\pi\\ &= \left(\frac{a}{\mathfrak{P}}\right)\left(\frac{2u}{|D|}\right)\chi_3(\pi)\varepsilon(\pi)\pi\\ &= \begin{cases}\left(\frac{a}{\mathfrak{P}}\right)\left(\frac{2u}{|D|}\right)\pi & \text{if } D \equiv 1 \pmod 8\\ \left(\frac{-a}{\mathfrak{P}}\right)\left(\frac{2u}{|D|}\right)\pi & \text{if } D \equiv 5 \pmod 8\end{cases}\end{aligned}$$

is the Frobenius automorphism for the curve $E_a$. The number of points on $E_a$ reduced $(\mathrm{mod}\,\mathfrak{P})$ is then

$$\begin{aligned}\mathbf{N}(\pi'-1) &= p+1-\mathrm{tr}\,(\pi') \\ &= p+1-\begin{cases}\left(\frac{a}{\mathfrak{P}}\right)\left(\frac{2u}{|D|}\right)u & \text{if } D\equiv 1 \pmod 8 \\ \left(\frac{-a}{\mathfrak{P}}\right)\left(\frac{2u}{|D|}\right)u & \text{if } D\equiv 5 \pmod 8.\end{cases}\end{aligned}$$

This completes the proof of Theorem 1.

**5. An historical remark.** Deuring's work [**1**] shows that the Frobenius automorphism for the curve $E_a$ of Theorem 1 is given by a Grössencharacter. Indeed, for $a = \pm 6$, the conductor of this Grössencharacter would divide $24|D|$. Thus, in fact, for any particular curve such as the seven examples of Section 1, a finite amount of experimentation would determine which Grössencharacter and hence verify the results of Theorem 1 for that curve. The question arises as to how it was possible for Deuring to have such a result and still not instantly have Theorem 1 in general. From the point of view of this paper, the answer is that there was not a good enough version of the reciprocity law for complex multiplication available at the time.

Deuring already knew that the Frobenius automorphism for the reduced curve was either $\pm\pi$. But which? Following the innovations brought to the theory of complex multiplication by Hasse in [**2**], Söhngen [**11**] proved the reciprocity congruence (7) for any principal $(\pi)$ such that $p \equiv 1 \pmod M$. (This allows $B$ in (6) to be chosen so that $B \equiv I \pmod M$ and then $pB^{-1} \equiv I \pmod M$. Thus, $f\circ(pB^{-1})(B\circ\theta)$ reduces to $f(B\circ\theta)$ which is Söhngen's theorem. By using such a $B$, he did not have to deal with the extra general complications of either introducing or finding $f\circ(pB^{-1})$.) In particular, for $\pi \equiv 1 \pmod M$, a choice of $B$ as in (8) above has both $pB^{-1} \equiv I \pmod M$ and $B\circ\theta = \theta$, and hence $f\circ(pB^{-1})(B\circ\theta)$ reduces to $f(\theta)$. This suffices to prove that $f(\theta)$ is in $K(M)$, the ray class field of $k \pmod M$. This in turn allows our proof to go through that there is a Grössencharacter $(\mathrm{mod}\,4N)$ when we consider a general $N$-division point, or even $(\mathrm{mod}\,N)$ when $4|N$.

With Söhngen's work available, and by using $N = 4$, we can already show that the desired Grössencharacter for the curve in (3) with $z = \theta$ is

$\varepsilon(\pi)\pi$ where $\varepsilon$ is either $\chi_3$ or $\chi_4$. The correct choice can be determined as soon as we know precisely the effect of the algebraic Frobenius automorphism for any single $\pi$ where $\chi_3(\pi) \neq \chi_4(\pi)$. Söhngen's theorem already has amazing utility. Unfortunately, in our situation with $N = 4$, we can apply Söhngen's theorem only when $p = \mathbf{N}(\pi) \equiv 1 \pmod 4$. Since $\chi_2(\pi) = (-1/p)$, $\chi_2(\pi) = 1$ for all $\pi$ to which Söhngen's theorem applies. Hence $\pi \pmod 4$ is always in the index two subgroup of $(\mathfrak{o}_k/4)^*$ on which $\chi_3$ agrees with $\chi_4$. In other words, with our approach, it is only with the full fledged reciprocity law, which was not available to Deuring, that we can distinguish between $\chi_3$ and $\chi_4$ and hence prove Theorem 1 in general.

In actual fact, Deuring had a completely different normalization of a CM curve to control the $y$-coordinate of a division point, but he still ultimately relies on the fact that we know what happens on the principal ray class, and this allows the proof that there is a Grössencharacter to go through. Deuring's work also provides another numerical way to help decide on the precise Grössencharacter for any fixed curve. It was this alternate way that I first used for the six class-number one examples. I hope to return to this alternate approach for the general case in the future.

## REFERENCES

**1.** Max Deuring, *Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins*, I, II, III, IV, Nachr. Akad. Math.-Phys. (1953), 85–94, (1955), 13–42, (1956), 37–76, (1957), 55–80.

**2.** Helmut Hasse, *Neue Begründung der komplexen Multiplikation*, I, II, Crelle **157** (1927), 115–139, **165** (1931), 64–88.

**3.** Serge Lang, *Elliptic functions*, 2nd Edition, Springer-Verlag, New York, 1987.

**4.** 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. **24** (1977), 286–295.

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

**6.** A.R. Rajwade, J.C. Parnami and Dharam Bir Rishi, *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.

**7.** Robert S. Rumely, *A formula for the Grössencharacter of a parameterized elliptic curve*, J. Number Theory **17** (1983), 389–402.

**8.** Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Iwanami Shoten and Princeton University Press, 1971.

**9.** ———, *Complex multiplication*, in *Modular functions of one variable* I, Lecture Notes Math. **320** (1973), 37–56.

**10.** C.L. Siegel, *Über das quadratische Reziprozitätsgesetz in algebraischen Zahlkörpern*, Nach. Akad. Wiss. Göttingen (1960), 1–16.

**11.** Heinz Söhngen, *Zur komplexen Multiplikation*, Math. Ann. **111** (1935), 302–328.

**12.** H.M. Stark, *L-functions at $s = 1$, IV. First derivatives at $s = 0$*, Adv. in Math. **35** (1980), 197–235.

**13.** Heinrich Weber, *Lehrbuch der Algebra*, III, 1909, reprinted by Chelsea, New York.

Department of Mathematics, University of California at San Diego, La Jolla, CA 92093