University of Massachusetts Amherst

ScholarWorks@UMass Amherst

2009

POWER RESIDUES OF FOURIER COEFFICIENTS OF ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

T Weston

University of Massachusetts - Amherst, weston@math.umass.edu

E Zaurova

Recommended Citation

POWER RESIDUES OF FOURIER COEFFICIENTS OF ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

TOM WESTON AND ELENA ZAUROVA

Let E be an elliptic curve over $\mathbf{Q}$. For any $m \geq 1$ and set of primes $\mathcal{C}$ (contained in the set of primes congruent to one modulo m) we define $\delta_m^1(E; \mathcal{C})$ as the relative density (in the set of $p \in \mathcal{C}$ which are ordinary for E) of primes $p \in \mathcal{C}$ for which the pth Fourier coefficient of E is an mth-power modulo p. In [4] it was conjectured that $\delta_m^1(E; \mathcal{C}) = \frac{1}{m}$ whenever E does not have complex multiplication and $\mathcal{C}$ is a set of primes defined by Galois theoretic conditions. In the present paper we extend these conjectures to the case of elliptic curves with complex multiplication; we also prove our conjectures for certain small values of m.

To be more precise, fix an imaginary quadratic field K of class number one and let E denote an elliptic curve with complex multiplication by the ring of integers $\mathcal{O}_K$; we write w for the order of $\mathcal{O}_K^\times$. For any divisor n of m we consider the density $\delta_m^n(E; \mathcal{C})$ of $p \in \mathcal{C}$ for which the mth power residue symbol of the pth Fourier coefficient of E modulo p is a primitive n^{th} root of unity. We compute the density $\delta_m^n(E; \mathcal{C})$ (in terms of certain simpler densities) for any m dividing w; most of these computations were essentially done in [4], with the exception of $K = \mathbf{Q}(i)$ and $m = 4$ (which is significantly more involved). These densities are often different from the naive expectation $\frac{\varphi(n)}{m}$. For general m, we conjecture that the density $\delta_m^n(E; \mathcal{C})$ differs from $\frac{\varphi(n)}{m}$ only to the extent that such a difference is forced upon it by its relation to the known density $\delta_{m'}^{n'}(E; \mathcal{C})$ with $m' = (m, w)$ and n' an appropriate divisor of m'. We make our conjecture entirely explicit in the case that $\mathcal{C}$ consists of all primes congruent to one modulo m.

We now outline the contents of the paper. In Section 1 we set our notation for densities and give the basic density computation coming from the Chebotarev density theorem. We give careful statements of the known results for m dividing w in Section 2; this is done most efficiently by regarding all elliptic curves with complex multiplication by $\mathcal{O}_K$ as twists of a fixed such curve. We also give some preliminary density computations for later use in explicating our general conjectures. Those conjectures are stated in Section 3, where we also verify certain natural compatibilities. In Section 4 we give the proof, based on biquadratic reciprocity, of our conjecture in the case $K = \mathbf{Q}(i)$ and $m = 4$

We emphasize that despite the essentially elementary nature of our approach for m dividing w, it remains our opinion that entirely new methods will be required to approach the general case.

It is a pleasure to thank Farshid Hajir for numerous helpful conversations.

1. Densities

1.1. **Preliminaries.** For a prime ideal $\mathfrak{p}$ of a finite extension K of $\mathbf{Q}(\zeta_m)$ and $\alpha \in \mathcal{O}_K - \mathfrak{p}$, we write $\left(\frac{\alpha}{\mathfrak{p}}\right)_m$ for the mth power residue symbol of α modulo $\mathfrak{p}$. Thus $\left(\frac{\alpha}{\mathfrak{p}}\right)_m \in \mu_m$ and

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_m \equiv \alpha^{\frac{N(\mathfrak{p})-1}{m}} \pmod{\mathfrak{p}}.$$

Most often we will be interested only in the order of $\left(\frac{\alpha}{\mathfrak{p}}\right)_m$ and in the case that $\alpha \in \mathbf{Z}$ and $K = \mathbf{Q}(\zeta_m)$. When this is the case, by abuse of notation we simply write $\left(\frac{\alpha}{p}\right)_m$ to mean $\left(\frac{\alpha}{\mathfrak{p}}\right)_m$ for some prime ideal $\mathfrak{p}$ of $\mathbf{Q}(\zeta_m)$ above p. We emphasize that while the precise root of unity $\left(\frac{\alpha}{p}\right)_m$ is not well-defined, its order is well-defined.

For a set of positive rational primes $\mathcal{P}$ we define the *zeta function* $\zeta(s; \mathcal{P})$ of $\mathcal{P}$ by

$$\zeta(s; \mathcal{P}) = \sum_{p \in \mathcal{P}} p^{-s};$$

this converges for $s > 1$. If $\mathcal{P}$ and $\mathcal{P}'$ are sets of primes with $\mathcal{P}$ of positive density (in the sense that $\lim_{s \to 1^+} \zeta(s; \mathcal{P})$ diverges), we define the *relative density* $\rho_{\mathcal{P}}(\mathcal{P}')$ of $\mathcal{P}'$ in $\mathcal{P}$ by

$$\rho_{\mathcal{P}}(\mathcal{P}') = \lim_{s \to 1^+} \frac{\zeta(s; \mathcal{P} \cap \mathcal{P}')}{\zeta(s; \mathcal{P})}$$

assuming it exists. We note that

$$\rho_{\mathcal{P}}(\mathcal{P}') = \lim_{x \to \infty} \frac{\#\{p \in \mathcal{P} \cap \mathcal{P}' \,;\, p < x\}}{\#\{p \in \mathcal{P} \,;\, p < x\}}$$

when the latter limit exists (which it will in all cases we consider).

We now introduce the sets of primes we will work with. For a finite Galois extension $K/\mathbf{Q}$ and a union C of conjugacy classes in $\mathrm{Gal}(K/\mathbf{Q})$, we write $\mathcal{C}_K^C$ for the set of rational primes p, unramified in $K/\mathbf{Q}$, with Frobenius over K lying in C. Recall that by the Chebotarev density theorem the set of primes $\mathcal{C}_K^C$ has absolute density equal to $\frac{\#C}{[K:\mathbf{Q}]}$. We say that a set $\mathcal{P}$ of primes is *Chebotarev* if it agrees with some $\mathcal{C}_K^C$ up to finite sets.

The basic density result we will need is the following.

Lemma 1.1. *Let K_1, K_2 be finite Galois extensions of $\mathbf{Q}$ and fix subsets $C_i \subseteq \mathrm{Gal}(K_i/\mathbf{Q})$ stable under conjugation. Then*

$$\rho_{\mathcal{C}_{K_1}^{C_1}}(\mathcal{C}_{K_2}^{C_2}) = \frac{\#\{(\sigma_1, \sigma_2) \subseteq C_1 \times C_2 \,;\, \sigma_1|_{K_1 \cap K_2} = \sigma_2|_{K_1 \cap K_2}\}}{\#C_1 \cdot [K_2 : K_1 \cap K_2]}.$$

Proof. Let $\pi_i : \mathrm{Gal}(K_1 K_2/\mathbf{Q}) \to \mathrm{Gal}(K_i/\mathbf{Q})$ denote the natural surjection. We then have

$$\mathcal{C}_{K_i}^{C_i} = \mathcal{C}_{K_1 K_2}^{\pi_i^{-1}(C_i)}.$$

In particular,

$$\mathcal{C}_{K_1}^{C_1} \cap \mathcal{C}_{K_2}^{C_2} = \mathcal{C}_{K_1 K_2}^{\pi_1^{-1}(C_1) \cap \pi_2^{-1}(C_2)}.$$

By the Chebotarev density theorem we thus have

$$\rho_{\mathcal{C}_{K_1}^{C_1}}(\mathcal{C}_{K_2}^{C_2}) = \frac{\#\pi_1^{-1}(C_1) \cap \pi_2^{-1}(C_2)}{\#\pi_1^{-1}(C_1)}.$$

As

$$\#\pi_1^{-1}(C_1) = [K_1 K_2 : K_1] \cdot \#C_1 = [K_2 : K_1 \cap K_2] \cdot \#C_1,$$

the lemma thus follows from noting that the injection

$$\pi_1 \times \pi_2 : \pi_1^{-1}(C_1) \cap \pi_2^{-1}(C_2) \hookrightarrow C_1 \times C_2$$

has image

$$\{(\sigma_1, \sigma_2) \subseteq C_1 \times C_2 \,;\, \sigma_1|_{K_1 \cap K_2} = \sigma_2|_{K_1 \cap K_2}\}.$$

$\square$

We fix notation for the most common Chebotarev sets we will encounter. For relatively prime integers a and b we write $\mathcal{C}_b^a$ for the set of primes congruent to a modulo b; it is a Chebotarev set with $K = \mathbf{Q}(\mu_b)$. For $t \in \mathbf{Q}^\times$, $m \geq 1$ and $\zeta \in \mu_m$ we write $\mathcal{C}_{\sqrt[m]{t}}^\zeta$ for the Chebotarev set of primes $p \equiv 1 \,(\mathrm{mod}\ m)$ such that $\left(\frac{t}{p}\right)_m$ is conjugate to ζ. We often simply write $\mathcal{C}_{\sqrt[m]{t}}^+$ (resp. $\mathcal{C}_{\sqrt[m]{t}}^-$) for $\mathcal{C}_{\sqrt[m]{t}}^1$ (resp. $\mathcal{C}_{\sqrt[m]{t}}^{-1}$). For example, $\mathcal{C}_{\sqrt{t}}^+$ (resp. $\mathcal{C}_{\sqrt{t}}^-$) is the set of odd primes which are split (resp. inert) in $\mathbf{Q}(\sqrt{t})$, where we consider all primes to be split in $\mathbf{Q}$ in the case that $t \in \mathbf{Q}^{\times 2}$.

1.2. Elliptic curves. Fix an elliptic curve E over $\mathbf{Q}$ and $m \geq 1$. For any set of primes $\mathcal{C}$ we define

$$\mathcal{P}_m(E; \mathcal{C}) = \{p \in \mathcal{C}_m^1 \cap \mathcal{C} \,;\, a_p(E) \not\equiv 0 \,(\mathrm{mod}\ p)\}.$$

When $\mathcal{P}_m(E; \mathcal{C})$ has positive density, for n dividing m we define $\delta_m^n(E; \mathcal{C})$ as the relative density of

$$\mathcal{P}_m^n(E; \mathcal{C}) = \left\{p \in \mathcal{P}_m(E; \mathcal{C}) \,;\, \left(\frac{a_p(E)}{p}\right)_m \text{ has exact order } n\right\}$$

in $\mathcal{P}_m(E; \mathcal{C})$.

In [4] it was conjectured that if E does not have complex multiplication, then $\delta_m^1(E; \mathcal{C}) = \frac{1}{m}$ for any Chebotarev set $\mathcal{C}$ contained in $\mathcal{C}_m^1$; more generally, one expects that $\delta_m^n(E; \mathcal{C}) = \frac{\varphi(n)}{m}$ for any n dividing m. Our goal in this paper is to formulate (and prove for small m) analogous conjectures when E does have complex multiplication.

2. ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

2.1. Twisting. Fix a discriminant

$$d \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}.$$

Let w_d denote the number of units in the ring of integers of $\mathbf{Q}(\sqrt{d})$. For $d \neq -3, -4, -8$, let E^d denote an elliptic curve of conductor d^2 with complex multiplication by $\mathbf{Z}[\frac{1+\sqrt{d}}{2}]$; the curve E^d is determined up to isogeny, which will suffice for our purposes. We let E^{-8} denote an elliptic curve in the isogeny class 256D in [1], with complex multiplication by $\mathbf{Z}[\sqrt{-2}]$.

For $t \in \mathbf{Q}^\times$ we define an elliptic curve E_t^d as follows:

- Let E_t^{-3} denote the elliptic curve with Weierstrass equation $y^2 = x^3 + 16t$.

- Let E_t^{-4} denote the elliptic curve with Weierstrass equation $y^2 = x^3 - tx$.
- Let E_t^{-7} denote the quadratic twist of E^{-7} by $-t$.
- For $d \le -8$, let E_t^d denote the quadratic twist of E^d by t.

(The slightly different twist in the case $d = -7$ is necessary because 2 is split in $\mathbf{Q}(\sqrt{-7})$.) In particular, for $d \ne -3, -4$ we have

$$(1) \qquad a_p(E_t^d) = \begin{cases} \left(\frac{t}{p}\right) a_p(E_1^d) & p \in \mathcal{C}_{\sqrt{d}}^+ \text{ and } (t,p) = 1; \\ 0 & p \in \mathcal{C}_{\sqrt{d}}^-. \end{cases}$$

In any case, for any Chebotarev set $\mathcal{C}$ the set of primes $\mathcal{P}_m(E_t^d; \mathcal{C})$ differs from $\mathcal{C} \cap \mathcal{C}_m^1 \cap \mathcal{C}_{\sqrt{d}}^+$ by a finite set. We thus can, and for the remainder of this section will, assume that $\mathcal{C} \subseteq \mathcal{C}_m^1 \cap \mathcal{C}_{\sqrt{d}}^+$.

2.2. Densities for $m \mid w_d$.
Let w_d denote the order of the group of units $\mathcal{O}_{\mathbf{Q}(\sqrt{d})}^\times$; thus $w_{-3} = 6$, $w_{-4} = 4$ and $w_d = 2$ for $d \ne -3, -4$. We now recall the known formulae for $\delta_m^n(E_t^d; \mathcal{C})$ for all m dividing w_d. We begin with the case $m = 2$ when such results exist for all d.

Proposition 2.1. Let $\mathcal{C}$ be a Chebotarev set contained in $\mathcal{C}_{\sqrt{d}}^+$. Then

$$\delta_2^1(E_t^d; \mathcal{C}) = \begin{cases} \rho_{\mathcal{C}}(\mathcal{C}_{\sqrt[4]{d}}^+) + \rho_{\mathcal{C}}(\mathcal{C}_4^3 \cap \mathcal{C}_{\sqrt{t}}^-) & d \ne -4; \\ \rho_{\mathcal{C}}(\mathcal{C}_8^1) + \rho_{\mathcal{C}}(\mathcal{C}_8^5 \cap \mathcal{C}_{\sqrt{t}}^-) & d = -4. \end{cases}$$

$$\delta_2^2(E_t^d; \mathcal{C}) = \begin{cases} \rho_{\mathcal{C}}(\mathcal{C}_{\sqrt[4]{d}}^-) + \rho_{\mathcal{C}}(\mathcal{C}_4^3 \cap \mathcal{C}_{\sqrt{t}}^+) & d \ne -4; \\ \rho_{\mathcal{C}}(\mathcal{C}_8^5 \cap \mathcal{C}_{\sqrt{t}}^+) & d = -4; \end{cases}$$

for any $t \in \mathbf{Q}^\times$.

Proof. This is immediate from the formulae

$$\left(\frac{a_p(E_t^d)}{p}\right) = \begin{cases} \left(\frac{-d}{p}\right)_4 & p \in \mathcal{C}_4^1 \cap \mathcal{C}_{\sqrt{d}}^+; \\ -\left(\frac{t}{p}\right) & p \in \mathcal{C}_4^3 \cap \mathcal{C}_{\sqrt{d}}^+; \end{cases}$$

(for $d \ne -4$) and

$$\left(\frac{a_p(E_t^{-4})}{p}\right) = \begin{cases} 1 & p \in \mathcal{C}_8^1; \\ -\left(\frac{t}{p}\right) & p \in \mathcal{C}_8^5; \end{cases}$$

of [4]. (Note that $\left(\frac{-d}{p}\right)_4 = \pm 1$ for $p \in \mathcal{C}_{\sqrt{d}}^+$.) $\square$

Before we can state our result for $d = -4$ and $m = 4$ we must introduce some notation. For $\alpha \in \{1, 1 + 4i, 5, 5 + 4i\}$, let $\mathcal{G}_8^\alpha$ denote the set of rational primes $p \equiv 1 \pmod 8$ for which one (or equivalently both) of the primary divisors of p in $\mathbf{Q}(i)$ are congruent to α modulo 8. (Recall that an element $\alpha \in \mathbf{Z}[i]$ is said to be *primary* if $\alpha \equiv 1 \pmod{2 + 2i}$.) These are Chebotarev sets for the ray class field $K = \mathbf{Q}(\zeta_{16}, \sqrt[4]{2})$ of $\mathbf{Q}(i)$ of conductor 8. These four sets partition $\mathcal{C}_8^1$.

The next proposition is proved in Section 4.

Proposition 2.2. *Let $\mathcal{C}$ be a Chebotarev set contained in $\mathcal{C}_4^1$. Then*

$$\delta_4^1(E_t^{-4};\mathcal{C}) = \rho_{\mathcal{C}}(\mathcal{G}_8^1) + \rho_{\mathcal{C}}(\mathcal{G}_8^5 \cap \mathcal{C}_{\sqrt{t}}^-) + \rho_{\mathcal{C}}(\mathcal{G}_8^{5+4i} \cap \mathcal{C}_{\sqrt{t}}^+) + \rho_{\mathcal{C}}(\mathcal{C}_8^5 \cap \mathcal{C}_{\sqrt[4]{t/2}}^+);$$

$$\delta_4^2(E_t^{-4};\mathcal{C}) = \rho_{\mathcal{C}}(\mathcal{G}_8^{1+4i}) + \rho_{\mathcal{C}}(\mathcal{G}_8^5 \cap \mathcal{C}_{\sqrt{t}}^+) + \rho_{\mathcal{C}}(\mathcal{G}_8^{5+4i} \cap \mathcal{C}_{\sqrt{t}}^-) + \rho_{\mathcal{C}}(\mathcal{C}_8^5 \cap \mathcal{C}_{\sqrt[4]{t/2}}^-);$$

$$\delta_4^4(E_t^{-4};\mathcal{C}) = \rho_{\mathcal{C}}(\mathcal{C}_8^5 \cap \mathcal{C}_{\sqrt{t}}^+);$$

for any $t \in \mathbf{Q}^\times$.

Finally, when $d = -3$ and $m = 3$ or $m = 6$ we have the following result. Let ω denote a primitive third root of unity.

Proposition 2.3. *Let $\mathcal{C}$ be a Chebotarev set contained in $\mathcal{C}_3^1$. Then*

$$\delta_3^1(E_t^{-3};\mathcal{C}) = \rho_{\mathcal{C}}(\mathcal{C}_9^1) + \rho_{\mathcal{C}}(\mathcal{C}_9^{4,7} \cap \mathcal{C}_{\sqrt[3]{t}}^+);$$

$$\delta_3^1(E_t^{-3};\mathcal{C}) = \rho_{\mathcal{C}}(\mathcal{C}_9^{4,7} \cap \mathcal{C}_{\sqrt[3]{t}}^\omega);$$

for any $t \in \mathbf{Q}^\times$. Furthermore,

$$\delta_6^n(E_t^{-3};\mathcal{C}) = \delta_2^{(n,2)}(E_t^{-3};\mathcal{C}) \cdot \delta_3^{(n,3)}(E_t^{-3};\mathcal{C})$$

for any $t \in \mathbf{Q}^\times$.

Here by $\mathcal{C}_9^{4,7}$ we of course mean the set of all primes p which are equivalent to either 4 or 7 modulo 9.

Proof. The densities for $m = 3$ follow from the formula

$$\left(\frac{a_p(E_t^{-3})}{\pi}\right)_3 = \begin{cases} 1 & p \equiv 1 \,(\mathrm{mod}\ 9); \\ \left(\frac{t}{\pi}\right)_3^2 & p \equiv 4 \,(\mathrm{mod}\ 9); \\ \left(\frac{t}{\pi}\right)_3 & p \equiv 7 \,(\mathrm{mod}\ 9) \end{cases}$$

of [4]. The case $m = 6$ follows immediately from the fact that the order of $\left(\frac{a_p(E_t^{-3})}{p}\right)_6$ equals the product of the orders of $\left(\frac{a_p(E_t^{-3})}{p}\right)_2$ and $\left(\frac{a_p(E_t^{-3})}{p}\right)_3$. $\qquad\square$

Remark 2.4. One can of course explicate the formula for $\delta_6^n(E_t^{-3};\mathcal{C})$. We give the formula for $n = 1$ to make it clear why we do not give it in general:

$$\delta_6^1(E_t^{-3};\mathcal{C}) = \rho_{\mathcal{C}}(\mathcal{C}_{36}^1 \cap \mathcal{C}_{\sqrt[4]{-3}}^+) + \rho_{\mathcal{C}}(\mathcal{C}_{36}^{19} \cap \mathcal{C}_{\sqrt{t}}^-) + \rho_{\mathcal{C}}(\mathcal{C}_{36}^{7,31} \cap \mathcal{C}_{\sqrt[6]{t}}^-) + \rho_{\mathcal{C}}(\mathcal{C}_{36}^{13,25} \cap \mathcal{C}_{\sqrt[4]{-3}}^+ \cap \mathcal{C}_{\sqrt[3]{t}}^+).$$

2.3. Abelian densities.

For later use we now use the results of the previous section to compute the densities $\delta_{m'}^1(E_t^d;\mathcal{C}_m^1)$ for m' dividing w_d and m with $(m, w_d) = m'$.

Lemma 2.5. *Assume that $d \neq -4$ and fix $m \geq 1$ even. Fix $t \in \mathbf{Q}^\times$ and let t' denote the unique squarefree integer with $t/t' \in \mathbf{Q}^{\times 2}$. Then*

$$\delta_2^1(E_t^d;\mathcal{C}_m^1) = \begin{cases} \frac{3}{4} & 4 \nmid m,\ t' \mid md,\ t' \equiv 3 \,(\mathrm{mod}\ 4)\ or\ d = -8,\ t' \equiv 2 \,(\mathrm{mod}\ 8); \\ \frac{1}{4} & 4 \nmid m,\ t' \mid md,\ t' \equiv 1 \,(\mathrm{mod}\ 4)\ or\ d = -8,\ t' \equiv 6 \,(\mathrm{mod}\ 8); \\ \frac{1}{2} & otherwise. \end{cases}$$

Proof. We assume $d \neq -8$; the case $d = -8$ is similar. Set $\mathcal{C} = \mathcal{C}_m^1 \cap \mathcal{C}_{\sqrt{d}}^+$. By Proposition 2.1 we must compute the densities $\rho_{\mathcal{C}}(\mathcal{C}_{\sqrt[4]{d}}^+)$ and $\rho_{\mathcal{C}}(\mathcal{C}_4^3 \cap \mathcal{C}_{\sqrt{t}}^-)$. This is straightforward using Lemma 1.1. Indeed, we have $\mathcal{C} = \mathcal{C}_{\mathbf{Q}(\zeta_m, \sqrt{d})}^{\{1\}}$ and $\mathcal{C}_{\sqrt[4]{d}}^+ =$

$\mathcal{C}^{\{1\}}_{\mathbf{Q}(i,\sqrt[4]{d})}$. (In each case $\{1\}$ stands for the identity element of the corresponding Galois group.) Since

$$\mathbf{Q}(\zeta_m, \sqrt{d}) \cap \mathbf{Q}(i, \sqrt[4]{d}) = \begin{cases} \mathbf{Q}(\sqrt{d}) & 4 \nmid m; \\ \mathbf{Q}(i, \sqrt{d}) & 4 \mid m; \end{cases}$$

it follows from Lemma 1.1 that

$$\rho_{\mathcal{C}}(\mathcal{C}^+_{\sqrt[4]{d}}) = \begin{cases} \frac{1}{4} & 4 \nmid m; \\ \frac{1}{2} & 4 \mid m. \end{cases}$$

On the other hand, clearly $\rho_{\mathcal{C}}(\mathcal{C}^3_4 \cap \mathcal{C}^-_{\sqrt{t}}) = 0$ if 4 divides m or if $t' = 1$. When $4 \nmid m$ and $t' \neq 1$, we have

$$\mathcal{C}^3_4 \cap \mathcal{C}^-_{\sqrt{t}} = \mathcal{C}^{\{\sigma\}}_{\mathbf{Q}(i,\sqrt{t})}$$

with $\sigma(i) = -i$ and $\sigma(\sqrt{t}) = -\sqrt{t}$. Thus by Lemma 1.1

$$\rho_{\mathcal{C}}(\mathcal{C}^3_4 \cap \mathcal{C}^-_{\sqrt{t}}) = \begin{cases} 0 & \sigma|_K \neq 1; \\ \frac{1}{[\mathbf{Q}(i,\sqrt{t}):K]} & \sigma|_K = 1; \end{cases}$$

where

$$K = \mathbf{Q}(i, \sqrt{t}) \cap \mathbf{Q}(\zeta_m, \sqrt{d}) = \begin{cases} \mathbf{Q}(\sqrt{t}) & t' \mid md,\ t' \equiv 1 \,(\mathrm{mod}\ 4); \\ \mathbf{Q}(\sqrt{-t}) & t' \mid md,\ t' \equiv 3 \,(\mathrm{mod}\ 4); \\ \mathbf{Q} & \text{otherwise.} \end{cases}$$

When $K = \mathbf{Q}$ we thus have $\rho_{\mathcal{C}}(\mathcal{C}^3_4 \cap \mathcal{C}^-_{\sqrt{t}}) = \frac{1}{4}$. When $K = \mathbf{Q}(\sqrt{t})$ (resp. $K = \mathbf{Q}(\sqrt{-t})$) we have $\sigma|_K \neq 1$ (resp. $\sigma|_K = 1$); the lemma follows easily from this. $\square$

Lemma 2.6. *Fix $m \geq 1$ even. Let t be a fourth-power free integer and let t' denote the unique squarefree integer with t/t' a square. If $4 \nmid m$, then*

$$\delta^1_2(E_t^{-4}; \mathcal{C}^1_m) = \begin{cases} 1 & t' \mid m,\ t'\ even; \\ \frac{1}{2} & t' \mid m,\ t'\ odd; \\ \frac{3}{4} & otherwise. \end{cases}$$

If $4 \mid m$, then

$$\delta^1_4(E_t^{-4}; \mathcal{C}^1_m) = \begin{cases} \frac{3}{4} & 8 \nmid m,\ t \in \{2, -8\}; \\ \frac{1}{2} & 8 \mid m\ or\ t' \mid m,\ t'\ even,\ t \notin \{\pm 2, \pm 8\}; \\ \frac{1}{4} & 8 \nmid m,\ t' \mid m,\ t'\ odd\ or\ t \in \{-2, 8\}; \\ \frac{3}{8} & otherwise. \end{cases}$$

Proof. The case $4 \nmid m$ is similar to Lemma 2.5; we omit the details. Assume therefore that $4 \mid m$; we must compute the four densities occurring in Proposition 2.2. We begin with $\rho_{\mathcal{C}^1_m}(\mathcal{G}^1_8)$. We have $\mathcal{C}^1_m = \mathcal{C}^{\{1\}}_{\mathbf{Q}(\zeta_m)}$ and $\mathcal{G}^1_8 = \mathcal{C}^{\{1\}}_K$, where $K = \mathbf{Q}(\zeta_{16}, \sqrt[4]{-2})$ is the ray class field of $\mathbf{Q}(i)$ of conductor 8. (Note that $[K : \mathbf{Q}] = 16$.) As

$$\mathbf{Q}(\zeta_m) \cap K = \mathbf{Q}(\zeta_{(m,16)}),$$

it follows from Lemma 1.1 that

$$\rho_{\mathcal{C}^1_m}(\mathcal{G}^1_8) = \frac{(m, 16)}{32}.$$

We consider the two densities $\rho_{\mathcal{C}_m^1}(\mathcal{G}_8^5 \cap \mathcal{C}_{\sqrt{t}}^-)$ and $\rho_{\mathcal{C}_m^1}(\mathcal{G}_8^{5+4i} \cap \mathcal{C}_{\sqrt{t}}^+)$ together. These densities are both zero if $16 \mid m$, so we may assume that $16 \nmid m$. It follows easily from the fact that K is a non-abelian extension of $\mathbf{Q}$ and a quadratic extension of $\mathbf{Q}(\zeta_{16})$ that

$$\rho_{\mathcal{C}_m^1}(\mathcal{G}_8^5 \cap \mathcal{C}_{\sqrt{t}}^-) + \rho_{\mathcal{C}_m^1}(\mathcal{G}_8^{5+4i} \cap \mathcal{C}_{\sqrt{t}}^+) = \frac{1}{2}\rho_{\mathcal{C}_m^1}(\mathcal{C}_{16}^9 \cap \mathcal{C}_{\sqrt{t}}^-) + \frac{1}{2}\rho_{\mathcal{C}_m^1}(\mathcal{C}_{16}^9 \cap \mathcal{C}_{\sqrt{t}}^+)$$
$$= \frac{1}{2}\rho_{\mathcal{C}_m^1}(\mathcal{C}_{16}^9) = \frac{(m,8)}{32}.$$

It remains to compute $\rho_{\mathcal{C}_m^1}(\mathcal{C}_8^5 \cap \mathcal{C}_{\sqrt[4]{t/2}}^+)$. This density is zero if $8 \mid m$, so we may assume that $8 \nmid m$. We have $\mathcal{C}_{\mathbf{Q}(\zeta_8, \sqrt[4]{t/2})}^{\{\sigma\}}$, where $\sigma(\zeta_8) = \zeta_8^5$ and $\sigma(\sqrt[4]{t/2}) = \sqrt[4]{t/2}$ so long as such a σ exists. There is no such σ exactly when $t' = \pm 1$ or $t \in \{2, -8\}$, in which case the desired density is zero. Otherwise, as

$$\mathbf{Q}(\zeta_m) \cap \mathbf{Q}(\zeta_8, \sqrt[4]{t/2}) = \begin{cases} \mathbf{Q}(i, \sqrt{t'}) & t' \mid m, \ t' \ \text{odd}; \\ \mathbf{Q}(i, \sqrt{t'/2}) & t' \mid m, \ t' \ \text{even}; \\ \mathbf{Q}(i) & t' \nmid m; \end{cases}$$

and $\sigma(\sqrt{t'/2}) = \sqrt{t'/2}$ and $\sigma(\sqrt{2}) = -\sqrt{2}$, it is now a straightforward computation with Lemma 1.1 to determine that for $8 \nmid m$ we have

$$\rho_{\mathcal{C}_m^1}(\mathcal{C}_8^5 \cap \mathcal{C}_{\sqrt[4]{t/2}}^+) = \begin{cases} \frac{1}{2} & t \in \{2, -8\}; \\ \frac{1}{4} & t' \mid m, \ t' \ \text{even}; \\ \frac{1}{8} & t' \nmid m; \\ 0 & t' \mid m, \ t' \ \text{odd or } t \in \{-2, 8\}. \end{cases}$$

The lemma follows on combining these density computations. $\quad\square$

Lemma 2.7. *Fix $m \geq 1$ divisible by 3. Let t be a cube-free integer. Then*

$$\delta_3^1(E_t^{-3}; \mathcal{C}_m^1) = \begin{cases} 1 & 9 \mid m \ \text{or } t = 1; \\ \frac{5}{9} & 9 \nmid m \ \text{and } t \neq 1; \end{cases}$$

Proof. This is immediate from Proposition 2.3 and the fact that

$$\rho_{\mathcal{C}_m^1}(\mathcal{C}_9^{4,7} \cap \mathcal{C}_{\sqrt[3]{t}}^+) = \begin{cases} \frac{2}{3} & 9 \nmid m \ \text{and } t = 1; \\ \frac{2}{9} & 9 \nmid m \ \text{and } t \neq 1; \\ 0 & 9 \mid m. \end{cases}$$

$\quad\square$

3. Conjectures

3.1. Statements. We continue with the notation of the previous section. Our basic conjecture is that the power residue symbol $\left(\frac{a_p(E_t^d)}{p}\right)_m$ is "random" except to the extent that its $m/(m, w_d)^{\text{th}}$ power is determined by the formulae of the previous section. More precisely, we make the following conjecture.

Conjecture 3.1. *Fix $m \geq 1$ and let $\mathcal{C}$ be a Chebotarev set contained in $\mathcal{C}_m^1 \cap \mathcal{C}_{\sqrt{d}}^+$. Then*

$$\delta_m^n(E_t^d; \mathcal{C}) = \frac{\varphi(n)}{m} \cdot \frac{\delta_{m'}^{n'}(E_t^d; \mathcal{C})}{\varphi(n')/m'}$$

where $m' = (m, w_d)$ and $n' = \frac{m'}{(\frac{m}{n}, w_d)}$.

Conjecture 3.1 is of course based on a great deal of numerical evidence. As the number of cases involved is somewhat overwhelming, we will not report any of it here; we will leave it to the curious reader to numerically verify our conjectures in any particular case.

It is worth noting that this conjecture satisfies certain compatibilities.

Proposition 3.2.

(1) *Let m_1, m_2 be relatively prime integers and let $\mathcal{C}$ be a Chebotarev set contained in $\mathcal{C}_{\sqrt{d}}^+$. Fix divisors n_i of each m_i and $t \in \mathbf{Q}^\times$. If Conjecture 3.1 holds for each $\delta_{m_i}^{n_i}(E_t^d; \mathcal{C} \cap \mathcal{C}_{m_i}^1)$, then it holds for $\delta_{m_1 m_2}^{n_1 n_2}(E_t^d; \mathcal{C} \cap \mathcal{C}_{m_1 m_2}^1)$.*

(2) *Fix $m \geq 1$. If Conjecture 3.1 holds for $\delta_m^n(E_1; \mathcal{C})$ (for all divisors n of m and all Chebotarev sets $\mathcal{C} \subseteq \mathcal{C}_m^1 \cap \mathcal{C}_{\sqrt{d}}^+$), then it holds for $\delta_m^n(E_t^d; \mathcal{C})$ for all $t \in \mathbf{Q}^\times$.*

Proof. The proof of (1) is straightforward; we leave it to the reader. For (2) we consider only the case $d \neq -3, -4$; the excluded cases are similar but much more painful. The case of m odd is clear so we assume that m is even. Fix n dividing m and a Chebotarev set contained in $\mathcal{C}_m^1 \cup \mathcal{C}_{\sqrt{d}}^+$. By (1) we have

$$\left(\frac{a_p(E_t^d)}{\mathfrak{p}} \right)_m = \left(\frac{t}{p} \right)^{\frac{p-1}{m}} \left(\frac{a_p(E_1^d)}{\mathfrak{p}} \right)_m$$

where $\mathfrak{p}$ is some prime of $\mathbf{Q}(\zeta_m)$ lying over p. It follows that $\left(\frac{a_p(E_t^d)}{\pi} \right)_m$ and $\left(\frac{a_p(E_1^d)}{\pi} \right)_m$ have the same order unless $\frac{p-1}{m}$ is odd, $\left(\frac{t}{p} \right) = -1$ and one has odd order, in which case the other has twice that order. That is,

(2) $\mathcal{P}_m^n(E_t^d; \mathcal{C}) = \mathcal{P}_m^n(E_1^d; \mathcal{C} \cap \mathcal{C}_{2m}^1) \cup \mathcal{P}_m^n(E_1^d; \mathcal{C} \cap \mathcal{C}_{2m}^{m+1} \cap \mathcal{C}_{\sqrt{t}}^+) \cup \mathcal{P}_m^{\tilde{n}}(E_1^d; \mathcal{C} \cap \mathcal{C}_{2m}^{m+1} \cap \mathcal{C}_{\sqrt{t}}^-)$

where

$$\tilde{n} = \begin{cases} 2n & n \text{ odd}; \\ n/2 & n \equiv 2 \,(\text{mod } 4); \\ n & 4 \mid n. \end{cases}$$

When m is divisible by 4, we either have that n is also divisible by 4 or else $n' = 1$. It follows easily that applying Conjecture 3.1 and Proposition 2.1 to (2) thus yields

$$\delta_m^n(E_t^d; \mathcal{C}) = \frac{2\varphi(n)}{m} \cdot \left(\rho_{\mathcal{C} \cap \mathcal{C}_{2m}^1}(\mathcal{C}_{\sqrt[4]{d}}^+) + \rho_{\mathcal{C} \cap \mathcal{C}_{2m}^{m+1} \cap \mathcal{C}_{\sqrt{t}}^+}(\mathcal{C}_{\sqrt[4]{d}}^+) + \rho_{\mathcal{C} \cap \mathcal{C}_{2m}^{m+1} \cap \mathcal{C}_{\sqrt{t}}^-}(\mathcal{C}_{\sqrt[4]{d}}^+) \right)$$

$$= 2 \frac{\varphi(n)}{m} \cdot \rho_{\mathcal{C}}(\mathcal{C}_{\sqrt[4]{d}}^+)$$

$$= \frac{\varphi(n)}{m} \cdot \frac{\delta_2^{n'}(E_t^d; \mathcal{C})}{\varphi(n')/m'}$$

as desired.

When $m \equiv 2 \,(\mathrm{mod}\ 4)$ we have $\mathcal{C} \cap \mathcal{C}^1_{2m} = \mathcal{C} \cap \mathcal{C}^1_4$ and $\mathcal{C} \cap \mathcal{C}^{m+1}_{2m} = \mathcal{C} \cap \mathcal{C}^3_4$. If n is even, so that $n' = 2$, $\tilde{n} = \frac{n}{2}$ and $\tilde{n}' = 1$, from (2) we obtain

$$
\begin{aligned}
\delta^n_m(E^d_t;\mathcal{C}) &= \frac{2\varphi(n)}{m} \cdot \left(\rho_{\mathcal{C}\cap\mathcal{C}^1_4}(\mathcal{C}^-_{\sqrt[4]{d}}) + \rho_{\mathcal{C}\cap\mathcal{C}^3_4\cap\mathcal{C}^+_{\sqrt{t}}}(\mathcal{C}^3_4) + \rho_{\mathcal{C}\cap\mathcal{C}^3_4\cap\mathcal{C}^-_{\sqrt{t}}}(\emptyset) \right) \\
&= \frac{2\varphi(n)}{m} \cdot \left(\rho_{\mathcal{C}\cap\mathcal{C}^1_4}(\mathcal{C}^-_{\sqrt[4]{d}}) + \rho_{\mathcal{C}}(\mathcal{C}^3_4 \cap \mathcal{C}^+_{\sqrt{t}}) \right) \\
&= \frac{\varphi(n)}{m} \cdot \frac{\delta^{n'}_2(E^d_t;\mathcal{C})}{\varphi(n')/m'}.
\end{aligned}
$$

Finally, if n is odd we have $n' = 1$, $\tilde{n} = 2n$ and $\tilde{n} = 2$, so that (2) yields

$$
\begin{aligned}
\delta^n_m(E^d_t;\mathcal{C}) &= \frac{2\varphi(n)}{m} \cdot \left(\rho_{\mathcal{C}\cap\mathcal{C}^1_4}(\mathcal{C}^+_{\sqrt[4]{d}}) + \rho_{\mathcal{C}\cap\mathcal{C}^3_4\cap\mathcal{C}^+_{\sqrt{t}}}(\emptyset) + \rho_{\mathcal{C}\cap\mathcal{C}^3_4\cap\mathcal{C}^-_{\sqrt{t}}}(\mathcal{C}^3_4) \right) \\
&= \frac{2\varphi(n)}{m} \cdot \left(\rho_{\mathcal{C}\cap\mathcal{C}^1_4}(\mathcal{C}^+_{\sqrt[4]{d}}) + \rho_{\mathcal{C}}(\mathcal{C}^3_4 \cap \mathcal{C}^-_{\sqrt{t}}) \right) \\
&= \frac{\varphi(n)}{m} \cdot \frac{\delta^{n'}_2(E^d_t;\mathcal{C})}{\varphi(n')/m'}.
\end{aligned}
$$

$\square$

3.2. Abelian densities.

Combining Conjecture 3.1 with the calculations of Section 2.3 we obtain the following explicit conjectures for the densities $\delta^1_m(E^d_t;\mathcal{C}^1_m)$.

Proposition 3.3. *Fix $m \geq 1$ and fix a non-zero integer t; if $d = -4$ (resp. $d = -3$) assume also that t is fourth-power free (resp. sixth-power-free). Let t' denote the unique squarefree integer with $t/t' \in \mathbf{Q}^{\times 2}$. Assume that Conjecture 3.1 holds for E^d_t and m.*

(1) *If $(m, w_d) = 1$, then*

$$
\delta^1_m(E^d_t;\mathcal{C}^1_m \cap \mathcal{C}^+_{\sqrt{d}}) = \frac{1}{m}.
$$

(2) *If $(m, w_d) = 2$ and $d \neq -4$, then*

$$
\delta^1_m(E^d_t;\mathcal{C}^1_m \cap \mathcal{C}^+_{\sqrt{d}}) = \begin{cases} \frac{3}{2m} & 4 \nmid m,\ t' \mid md,\ t' \equiv 3 \,(\mathrm{mod}\ 4) \\ & \quad \text{or } d = -8,\ t' \equiv 2 \,(\mathrm{mod}\ 8); \\ \frac{1}{2m} & 4 \nmid m,\ t' \mid md,\ t' \equiv 1 \,(\mathrm{mod}\ 4) \\ & \quad \text{or } d = -8,\ t' \equiv 6 \,(\mathrm{mod}\ 8); \\ \frac{1}{m} & \text{otherwise.} \end{cases}
$$

(3) *If $(m, w_d) = 2$ and $d = -4$, then*

$$
\delta^1_m(E^d_t;\mathcal{C}^1_m \cap \mathcal{C}^1_4) = \begin{cases} \frac{2}{m} & t' \mid m,\ t' \text{ even}; \\ \frac{1}{m} & t' \mid m,\ t' \text{ odd}; \\ \frac{3}{2m} & \text{otherwise.} \end{cases}
$$

(4) *If $(m, w_d) = 3$ (so that $d = -3$), then*

$$
\delta^1_m(E^d_t;\mathcal{C}^1_m) = \begin{cases} \frac{3}{m} & 9 \mid m \text{ or } t \in \mathbf{Q}^{\times 3}; \\ \frac{5}{3m} & \text{otherwise.} \end{cases}
$$

(5) *If $(m, w_d) = 4$ (so that $d = -4$), then*

$$\delta_m^1(E_t^d; \mathcal{C}_m^1) = \begin{cases} \frac{3}{m} & 8 \nmid m, \, t \in \{2, -8\}; \\ \frac{2}{m} & 8 \mid m \text{ or } t' \mid m, \, t' \text{ even }, \, t \notin \{\pm 2, \pm 8\}; \\ \frac{1}{m} & 8 \nmid m, \, t' \mid m, \, t' \text{ odd or } t \in \{-2, 8\}; \\ \frac{3}{2m} & \text{otherwise.} \end{cases}$$

(6) *If $(m, w_d) = 6$ (so that $d = -3$), then*

$$\delta_m^1(E_t^d; \mathcal{C}_m^1) = \begin{cases} \frac{9}{2m} & 4 \nmid m, \, t' \mid md, \, t' \equiv 3 \, (mod \, 4), \, t \in \mathbf{Q}^{\times 3}; \\ \frac{3}{2m} & 4 \nmid m, \, t' \mid md, \, t' \equiv 1 \, (mod \, 4), \, t \in \mathbf{Q}^{\times 3}; \\ \frac{3}{m} & 4 \mid m \text{ or } t' \nmid md \text{ or } t' \text{ even and } t \in \mathbf{Q}^{\times 3}; \\ \frac{5}{2m} & 4 \nmid m, \, t' \mid md, \, t' \equiv 3 \, (mod \, 4), \, t \notin \mathbf{Q}^{\times 3}; \\ \frac{5}{6m} & 4 \nmid m, \, t' \mid md, \, t' \equiv 1 \, (mod \, 4), \, t \notin \mathbf{Q}^{\times 3}; \\ \frac{5}{3m} & 4 \mid m \text{ or } t' \nmid md \text{ or } t' \text{ even and } t \notin \mathbf{Q}^{\times 3}; \end{cases}$$

Proof. This is all immediate from the results of Section 2.3. $\qquad\square$

4. Biquadratic residues

In this section we give the proof of Proposition 2.2. Recall that in this setting E_t^{-4} denotes the elliptic curve $y^2 = x^3 - tx$ with complex multiplication by $\mathbf{Z}[i]$. By [3] we have that $a_p(E_t^{-4}) = 0$ for $p \equiv 3 \, (\text{mod } 4)$ or not relatively prime to t; otherwise

$$a_p(E_t^{-4}) = \left(\frac{t}{\bar{\pi}}\right)_4 \pi + \left(\frac{t}{\pi}\right)_4 \bar{\pi} \tag{3}$$

where $p = \pi\bar{\pi}$ with $\pi, \bar{\pi}$ primary irreducibles in $\mathbf{Z}[i]$.

We begin with a computation with biquadratic reciprocity.

Lemma 4.1. *Let $\pi = a + bi$ be a primary irreducible of prime norm p in $\mathbf{Z}[i]$ and let ℓ be an odd rational prime divisor of a. Then*

$$\left(\frac{\ell}{\pi}\right)_4 = (-1)^{\frac{\ell-1}{2} \cdot \frac{p-1}{4}} \left(\frac{2}{\ell}\right).$$

Proof. If $\ell \equiv 1 \, (\text{mod } 4)$, then ℓ factors as $\ell = \lambda\bar{\lambda}$ into primary irreducibles. Thus

$$\left(\frac{\ell}{\pi}\right)_4 = \left(\frac{\lambda}{\pi}\right)_4 \left(\frac{\bar{\lambda}}{\pi}\right)_4 = \left(\frac{\pi}{\lambda}\right)_4 (-1)^{\frac{\ell-1}{4} \cdot \frac{p-1}{4}} \cdot \left(\frac{\pi}{\bar{\lambda}}\right)_4 (-1)^{\frac{\ell-1}{4} \cdot \frac{p-1}{4}} = \left(\frac{\pi}{\lambda}\right)_4 \left(\frac{\pi}{\bar{\lambda}}\right)_4$$

by biquadratic reciprocity. Thus

$$\left(\frac{\ell}{\pi}\right)_4 = \left(\frac{a + bi}{\lambda}\right)_4 \left(\frac{a + bi}{\bar{\lambda}}\right)_4 = \left(\frac{bi}{\lambda}\right)_4 \left(\frac{bi}{\bar{\lambda}}\right)_4$$

since ℓ divides a. As

$$\overline{\left(\frac{bi}{\lambda}\right)_4} = \left(\frac{-bi}{\bar{\lambda}}\right)_4$$

we conclude that

$$\left(\frac{\ell}{\pi}\right)_4 = \left(\frac{-1}{\lambda}\right)_4 = (-1)^{\frac{\ell-1}{4}}.$$

Since

$$\frac{\ell-1}{4} \equiv \frac{\ell^2-1}{8} \quad (\text{mod } 2)$$

for $\ell \equiv 1 \pmod 4$, the lemma follows in this case.

If $\ell \equiv 3 \pmod 4$, then $-\ell$ is primary, so that by biquadratic reciprocity we have

$$\left(\frac{\ell}{\pi}\right)_4 = \left(\frac{-1}{\pi}\right)_4 \left(\frac{-\ell}{\pi}\right)_4 = (-1)^{\frac{p-1}{4}} \left(\frac{\pi}{\ell}\right)_4 (-1)^{\frac{\ell^2-1}{4}\cdot\frac{p-1}{4}} = (-1)^{\frac{p-1}{4}} \left(\frac{\pi}{\ell}\right)_4$$

since $\ell^2 - 1$ is divisible by 8. We now have

$$\left(\frac{\ell}{\pi}\right)_4 = (-1)^{\frac{p-1}{4}} \left(\frac{\pi}{\ell}\right)_4 = (-1)^{\frac{p-1}{4}} \left(\frac{bi}{\ell}\right) = (-1)^{\frac{p-1}{4}} \left(\frac{b}{\ell}\right)_4 i^{\frac{\ell^2-1}{4}}.$$

Since

$$b^{\frac{\ell^2-1}{4}} \equiv 1 \pmod \ell$$

by Fermat's little theorem, the lemma follows in this case from the fact that

$$i^{\frac{\ell^2-1}{4}} = (-1)^{\frac{\ell^2-1}{8}} = \left(\frac{2}{\ell}\right).$$

$\square$

It will also be useful to recall the computation of the biquadratic character of 2.

Lemma 4.2. *Let $a + bi$ be a primary irreducible of norm p. Then*

$$\left(\frac{2}{a+bi}\right)_4 = (-i)^{b/2}.$$

Proof. Factoring 2 as

$$2 = -i(1+i)^2,$$

we find that

$$\left(\frac{2}{a+bi}\right)_4 = \left(\frac{-i}{\pi}\right)_4 \cdot \left(\frac{1+i}{\pi}\right)_4^2 = (-i)^{\frac{p-1}{4}} \cdot i^{\frac{a-b-b^2-1}{2}}$$

by [2, Theorem 6.9]. From here a lengthy but elementary calculation yields the asserted formula. $\square$

We are now in a position to give a formula for the biquadratic residue symbol $\left(\frac{a_p(E_t^{-4})}{\pi}\right)_4$ with π a primary irreducible divisor of p.

Proposition 4.3. *Let $p \equiv 1 \,(mod\ 4)$ be a prime relatively prime to t and let $a + bi$ be a primary irreducible of norm p. Then*

$$\left(\frac{a_p(E_t^{-4})}{a+bi}\right)_4 = i^{\frac{a-1}{2}} \cdot (-1)^{\frac{b^2+2b}{8}} \cdot \left(\frac{t}{a+bi}\right)_4^{\frac{p-1}{4}}.$$

Proof. Set $\pi = a + bi$. By (3) we have

$$a_p(E_t^{-4}) \equiv \left(\frac{t}{\pi}\right)_4 \bar\pi \pmod \pi$$

so that

$$\left(\frac{a_p(E_t^{-4})}{\pi}\right)_4 = \left(\frac{\left(\frac{t}{\pi}\right)_4 \bar\pi}{\pi}\right)_4 = \left(\frac{t}{\pi}\right)_4^{\frac{p-1}{4}} \left(\frac{\bar\pi}{\pi}\right)_4$$

It thus suffices to compute $\left(\frac{\bar\pi}{\pi}\right)_4$.

Let

$$a = p_1^{e_1} \cdots p_r^{e_r} q_1^{f_1} \cdots q_s^{f_s}$$

be the prime of factorization of a, where $p_i \equiv 1 \,(\mathrm{mod}\ 4)$ and $q_i \equiv 3 \,(\mathrm{mod}\ 4)$. (Here a is odd since π is primary.) Since

$$\bar{\pi} \equiv \pi + \bar{\pi} \equiv 2a \quad (\mathrm{mod}\ \pi),$$

applying Lemma 4.1 we find that

$$\left(\frac{\bar{\pi}}{\pi}\right)_4 = \left(\frac{2}{\pi}\right)_4 \left(\frac{p_1}{\pi}\right)_4^{e_1} \cdots \left(\frac{p_r}{\pi}\right)_4^{e_r} \left(\frac{q_1}{\pi}\right)_4^{f_1} \cdots \left(\frac{q_s}{\pi}\right)_4^{f_s}$$

$$= \left(\frac{2}{\pi}\right)_4 \left(\frac{2}{p_1}\right)^{e_1} \cdots \left(\frac{2}{p_r}\right)^{e_r} \left(\frac{2}{q_1}\right)^{f_1} \cdots \left(\frac{2}{q_s}\right)^{f_s} (-1)^{\frac{p-1}{4} \cdot (f_1 + \cdots + f_s)}.$$

By the multiplicativity of the Jacobi symbol and the fact that

$$f_1 + \cdots + f_s \equiv \frac{a-1}{2} \quad (\mathrm{mod}\ 2),$$

we conclude that

$$\left(\frac{\bar{\pi}}{\pi}\right)_4 = \left(\frac{2}{\pi}\right)_4 \left(\frac{2}{a}\right) (-1)^{\frac{p-1}{4} \cdot \frac{a-1}{2}}.$$

Combining this with Lemma 4.2 and simplifying yields the theorem.   □

Proposition 2.2 follows immediately.

Corollary 4.4. *Let $\mathcal{C}$ be a Chebotarev set. For any $t \in \mathbf{Q}^{\times}$ we have*

$$\delta_4^1(E_t^{-4}; \mathcal{C}) = \rho_{\mathcal{C}}(\mathcal{G}_8^1) + \rho_{\mathcal{C}}(\mathcal{G}_8^5 \cap \mathcal{C}_{\sqrt{t}}^-) + \rho_{\mathcal{C}}(\mathcal{G}_8^{5+4i} \cap \mathcal{C}_{\sqrt{t}}^+) + \rho_{\mathcal{C}}(\mathcal{C}_8^5 \cap \mathcal{C}_{\sqrt[4]{t/2}}^+);$$

$$\delta_4^2(E_t^{-4}; \mathcal{C}) = \rho_{\mathcal{C}}(\mathcal{G}_8^{1+4i}) + \rho_{\mathcal{C}}(\mathcal{G}_8^5 \cap \mathcal{C}_{\sqrt{t}}^+) + \rho_{\mathcal{C}}(\mathcal{G}_8^{5+4i} \cap \mathcal{C}_{\sqrt{t}}^-) + \rho_{\mathcal{C}}(\mathcal{C}_8^5 \cap \mathcal{C}_{\sqrt[4]{t/2}}^-);$$

$$\delta_4^4(E_t^{-4}; \mathcal{C}) = \rho_{\mathcal{C}}(\mathcal{C}_8^5 \cap \mathcal{C}_{\sqrt{t}}^+).$$

Proof. Since the nine sets of primes listed above partition the set of all primes (relatively prime to t), it suffices to show that $\left(\frac{a_p(E_t^{-4})}{\pi}\right)_4$ has the asserted order for each set. This is straightforward from Proposition 4.3. Indeed, fix $p \in \mathcal{C}_4^1$ and a primary divisor π of p. Proposition 4.3 (together with Lemma 4.2 when $p \equiv 5 \,(\mathrm{mod}\ 8)$) then yields

$$\left(\frac{a_p(E_t^{-4})}{\pi}\right)_4 = \begin{cases} 1 & p \in \mathcal{G}_8^1; \\ -1 & p \in \mathcal{G}_8^{1+4i}; \\ -\left(\frac{t}{p}\right) & p \in \mathcal{G}_8^5; \\ \left(\frac{t}{p}\right) & p \in \mathcal{G}_8^{5+4i}; \\ \left(\frac{t/2}{\pi}\right)_4 & p \in \mathcal{C}_8^5. \end{cases}$$

The corollary follows easily.   □

References

[1] Cremona, J.E. *Algorithms for modular elliptic curves*, second edition. Cambridge University Press, Cambridge, 1997.

[2] Lemmermeyer, F. *Reciprocity laws*, Springer–Verlag, Berlin, 2000.

[3] Silverman, J. *Advanced topics in the arithmetic of elliptic curves.* Springer–Verlag, New York, 1994.

[4] Weston, T. *Power residues of Fourier coefficients of modular forms.* Canad. J. Math. **57** (2005), 1102–1120.

(Tom Weston) Dept. of Mathematics, University of Massachusetts, Amherst, MA

(Elena Zaurova) Dept. of Mathematics, University of Massachusetts, Amherst, MA
E-mail address, Tom Weston: `weston@math.umass.edu`
E-mail address, Elena Zaurova: `ezaurova@student.umass.edu`