ON ELLIPTIC CURVES AND BINARY QUARTIC FORMS

W. DUKE

Abstract. A Dirichlet series is defined whose coefficients are determined by counting certain integral points on the quadratic twists of an elliptic curve. The function defined by this series has a meromorphic continuation with at most a simple pole at a certain distinguished point. In certain cases the residue there gives a class number formula for positive definite binary quartic forms.

To John Friedlander, in honor of his eightieth birthday...

1. Introduction

Mordell was among the first to exploit directly the close relationship between rational or integral points on an elliptic curve and binary quartic forms. His first proof [24] of the finiteness of the rank of an elliptic curve over the rational numbers made use of a correspondence between rational points on the curve and integral squares represented by associated binary quartic forms. Further developments of this relationship have been applied recently by Bhargava and Shankar [1] to obtain striking results on the average rank of elliptic curves defined over the rational numbers.

In this paper I give a different kind of application of the connection between elliptic curves and binary quartic forms. For integers A and B let

$$y^2 = x^3 + Ax + B$$

be the Weierstrass equation in global minimal form of an elliptic curve E. There is a Dirichlet series whose coefficients count certain integral points on the quadratic twists of E. I will show that for certain E the function defined by this series has a simple pole whose residue gives a class number formula for positive definite integral binary quartic forms. The formula is analogous to one for Gaussian binary quadratic forms of the kind proven by Dirichlet, when that is given as the residue of a Dirichlet series whose coefficients count integer points on a family of conics.

It is instructive to review this genus zero result. For $\Delta \in \mathbb{Z}^+$ consider the affine conic C defined by

$$y = x^2 + \Delta$$

and for $n \in \mathbb{Z}^+$ let C_n denote the "twisted" conic given by $ny = x^2 + \Delta$. Define

$$\nu(n) = \#\{(x,y) \in \mathbb{Z}^2;\ ny = x^2 + \Delta \ \text{ where } \gcd(x,n) = 1 \text{ and } 0 \le \tfrac{x}{n} < 1\}, \tag{1.1}$$

so that $\nu(n)$ counts certain integral points on C_n. Consider the associated Dirichlet series defined for $\mathrm{Re}(s) > 1$ by

$$Z(s) = \zeta(2s) \prod_{p|\Delta} (1 + p^{-s}) \sum_{n \ge 1} \nu(n)\, n^{-s}. \tag{1.2}$$

2010 *Mathematics Subject Classification.* 11Exx, 11Mxx.

Research supported by NSF grant DMS 1701638 and Simons Foundation Award Number 554649.

This function has an analytic continuation to the s-plane with only a simple pole at $s = 1$. The residue there gives a version of Dirichlet's class number formula for the integral binary quadratic forms of Gauss.

To explain this, let $\mathcal{F}$ be the set of all (primitive) Gaussian binary quadratic forms

$$Q(x, y) = (a, b, c) = ax^2 + 2bxy + cy^2 \qquad \text{(note the 2!)},$$

where a, b, c are integers such that $\gcd(a, b, c) = 1$ and $\Delta = ac - b^2 > 0$. Assume that $a > 0$ so that the forms are positive definite. Suppose that $g = \left(\begin{smallmatrix} m_1 & m_2 \\ m_1' & m_2' \end{smallmatrix}\right) \in \Gamma = \mathrm{SL}(2, \mathbb{Z})$ acts as usual on any binary form F by

$$(F|g)(x, y) = F(m_1x + m_2y, m_1'x + m_2'y). \tag{1.3}$$

Let $\mathrm{Aut}\, Q \subset \Gamma$ be the group of automorphs of Q, which is well-known to be finite with two elements unless $Q = (1, 0, 1)$ or $Q = (2, 1, 2)$, when it has four or six elements, respectively. Define the weighted class number by

$$h = h_\Delta = \sum_{Q \in \mathcal{F}/\Gamma} \tfrac{2}{\#\mathrm{Aut}\, Q}, \tag{1.4}$$

which is also known to be finite. The family $\mathcal{F}$ splits into two orders, comprising properly primitive or improperly primitive forms, according to whether the value of $\gcd(a, 2b, c)$ is one or two. Thus h accounts for both types. For example, $h_3 = \frac{4}{3}$ since $\mathcal{F}/\Gamma$ is represented by the improperly primitive $(2, 1, 2)$ and the properly primitive $(3, 0, 1)$.

The following result is a restatement of a fundamental theorem of Dirichlet [10, §5][1]:

Theorem 1. *For any $\Delta \in \mathbb{Z}^+$ the function $Z(s)$ has an analytic continuation to the s-plane with only a simple pole at $s = 1$ where*

$$\mathrm{Res}_{s=1}\, Z(s) = \tfrac{1}{2}\Omega\, h. \tag{1.5}$$

Here $\Omega = \int_{\mathbb{R}} \frac{dx}{y} = \int_{\mathbb{R}} \frac{dx}{x^2+\Delta} = \frac{\pi}{\sqrt{\Delta}}$.

Note that (1.5) holds for any positive integer Δ and yet it still applies to (properly or improperly) primitive forms. It yields the limit formula

$$\lim_{N\to\infty} \tfrac{1}{N} \sum_{n \le N} \nu(n) = \tfrac{3\sqrt{\Delta}}{\pi\,\psi(\Delta)}\, h,$$

where $\psi(n) = n\prod_{p|n}(1 + \frac{1}{p})$ is the Dedekind ψ-function.

For a discriminant d let χ_d be the Kronecker symbol, which is a Dirichlet character defined modulo $|d|$, with associated Dirichlet L-function given by

$$L(s, \chi_d) = \sum_{n \ge 1} \chi_d(n) n^{-s}.$$

From (1.2) we can derive the factorization $Z(s) = L(s)\zeta(s)$, where

$$L(s) = \begin{cases} L(s, \chi_{-4\Delta}), & \Delta \not\equiv 3 \pmod 4 \\ \big(1 - \chi_{-\Delta}(2)2^{-s} + 2^{1-2s}\big)L(s, \chi_{-\Delta}), & \Delta \equiv 3 \pmod 4. \end{cases} \tag{1.6}$$

Now (1.5) implies that

$$h = \tfrac{2\sqrt{\Delta}}{\pi}\, L(1), \tag{1.7}$$

[1] For a translation to English see [11].

so (1.6) allows us to express h as a finite sum.[2] Furthermore, the Euler product expansion of $L(1)$ realizes Dirichlet's formula as special case of Siegel's main theorem [31, p.113].

2. A Dirichlet series for integral points on twists of an elliptic curve

It is natural to consider the genus one case. For integers A and B let

$$y^2 = x^3 + Ax + B \tag{2.1}$$

be the Weierstrass equation of an elliptic curve E in global minimal form with discriminant

$$\Delta = -16(4A^3 + 27B^2).$$

The real period of E is

$$\Omega_E = \int \frac{dx}{y} = \int \frac{dx}{\sqrt{x^3 + Ax + B}}, \tag{2.2}$$

where the integral is taken over $\{x;\ x^3 + Ax + B \geq 0\}$.

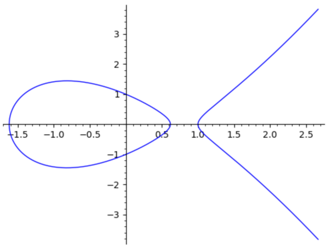

Figure 1. $E(\mathbb{R}) : y^2 = x^3 - 2x + 1$

For $n \in \mathbb{Z}^+$ let

$$y^2 = x^3 + n^2Ax + n^3B \tag{2.3}$$

represent the twisted curve E_n. Denote by $E_n(\mathbb{Z})$ the set of integral points on the model (2.3) and by $E_n^*(\mathbb{Z})$ the subset of those $(x, y) \in E_n(\mathbb{Z})$ with $\gcd(x, n) = 1$.

Assume that $\Delta > 0$. Then $A < 0$ and $E_n(\mathbb{R})$ is the disjoint union of two connected components: the connected component of the identity and a compact component that contains those $(x, y) \in E_n(\mathbb{R})$ with $e_1 \leq \frac{x}{n} \leq e_2$. Here $e_1 < e_2 < e_3$ are the zeros of $x^3 + Ax + B$. See Figure 1 for an illustration of $E(\mathbb{R})$ when E is given by $y^2 = x^3 - 2x + 1$.

Let $\nu_E(n)$ denote the number of points in $E_n^*(\mathbb{Z})$ that are on the compact component. Thus

$$\nu_E(n) = \#\{(x, y) \in \mathbb{Z}^2;\ y^2 = x^3 + An^2x + Bn^3 \text{ where } \gcd(n, x) = 1 \text{ and } e_1 \leq \tfrac{x}{n} \leq e_2\}. \tag{2.4}$$

Although in general it is non-trivial that $E_n(\mathbb{Z})$ is finite for a fixed n, the finiteness of the restricted counting function $\nu_E(n)$ for a fixed n is obvious.[3] Actually, we have the estimate $\nu_E(n) \ll n$ since for (x, y) in the compact component we have that $|x| \ll n$ and y is determined up to sign. On the other hand, it might happen that $\nu(n) = 0$ for all n, but

[2] Formulas (1.7) and (1.6) yield the usual class number formula for primitive integral quadratic forms of the type $ax^2 + bxy + cy^2$ with negative (but not necessarily fundamental) discriminant $d = b^2 - 4ac$. If h' denotes the sum in (1.4) restricted to properly primitive classes then $h = h'$ unless $\Delta \equiv 3 \pmod 4$ when $h = 2h'$ if $\Delta \equiv 7 \pmod 8$ and $h = \frac{4}{3}h'$ otherwise [13, art. 256]. It is now straightforward to deduce the usual class number formula as given in [9] for fundamental d and in [6] in general.

[3] The general result was first deduced by Mordell [25] from a theorem of Thue in [34]. See also [30].

we will see that if the binary quartic forms of interest exist then $\nu(n) > 0$ for infinitely many n. In any case, the Dirichlet series

$$Z_E(s) = \zeta(4s) \prod_{p|\Delta}(1+p^{-2s}) \sum_{n\geq 1} \nu_E(n)\, n^{-s} \tag{2.5}$$

clearly converges for $\operatorname{Re} s > 2$. In fact, it converges for $\operatorname{Re} s > \frac{1}{2}$ since it will be shown that $Z_E(s)$ has an analytic continuation to a meromorphic function that is holomorphic for $\operatorname{Re} s > \frac{1}{4}$ except for a (possible) simple pole at $s = \frac{1}{2}$. The convergence claim then follows from a well-known theorem of Landau [20, II, p. 697]. Our main goal is to show that, under an additional assumption on the discriminant, the residue at $s = \frac{1}{2}$ gives a class number formula for positive definite binary quartic forms.

3. A class number formula for binary quartic forms

For integers a, b, c, d, e let

$$F(x,y) = (a,b,c,d,e) = ax^4 + 4bx^3y + 6cx^2y^2 + 4dxy^3 + ey^4 \tag{3.1}$$

be a binary quartic form of Gaussian type, meaning that it comes with binomial coefficients. By an arithmetic invariant of F we mean a function $K_F(a,b,c,d,e)$ such that $K_{F|g} = K_F$ for all $g \in \Gamma = \mathrm{SL}(2,\mathbb{Z})$. Say that F is primitive if $\gcd(a,b,c,d,e) = 1$. Another basic invariant is $\hat{F} = \gcd(a, 4b, 6c, 4d, e)$. Note that this is the gcd of the actual coefficients of F. If F is primitive then $\hat{F} \in \{1,2,3,4,6,12\}$. Those primitive forms F with $\hat{F} = 1$ are said to be properly primitive while those with $\hat{F} > 1$ are said to be improperly primitive. The other basic invariants of F are given by

$$I = I_F := ae - 4bd + 3c^2 \quad \text{and} \quad J = J_F := ace + 2bcd - b^2e - d^2a - c^3 \tag{3.2}$$

and the discriminant of F, which is defined to be $\Delta_F = I_F^3 - 27J_F^2$.

Suppose that $\Delta_F \neq 0$. Then the group $\operatorname{Aut} F$ of all Γ–automorphs of F is finite. Every form has the trivial automorphs ± 1. For F in (3.1) a non-trivial automorph must be conjugate in Γ to one of $\pm\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, which fix precisely those F that are reciprocal: $F = (a,b,c,-b,a)$. Thus $\#\operatorname{Aut} F \in \{2,4\}$. Given integers I_0,J_0 which are such that $\Delta_F = I_0^3 - 27J_0^2$ let

$$\mathcal{F} = \mathcal{F}(I_0,J_0) = \{F = (a,b,c,d,e);\ F \text{ primitive with } I_F = I_0,\ J_F = J_0\ \}.$$

This $\mathcal{F}$ may contain both properly and improperly primitive forms F.

After Hermite [14, 15] and Julia [19], cf. [26, p.163], $\mathcal{F}/\Gamma$ consists of finitely many equivalence classes.[4] For a collection of classes $\mathcal{F}_0 \subset \mathcal{F}$ define the weighted class number

$$h(\mathcal{F}_0) = \sum_{F\in\mathcal{F}_0/\Gamma} \tfrac{2}{\#\operatorname{Aut} F}. \tag{3.3}$$

A form F is positive definite if $\Delta_F > 0$ and $F(x,y) > 0$ unless $x = y = 0$. Let $\mathcal{F}^+ \subset \mathcal{F}$ be the collection of classes consisting of those $F \in \mathcal{F}$ that are positive definite.

Given the elliptic curve E in (2.1) set

$$\mathcal{F}_E = \mathcal{F}^+(-4A,-4B) \quad \text{and} \quad h_E = h(\mathcal{F}_E^+). \tag{3.4}$$

Note that for each $F \in \mathcal{F}_E$ we have $\Delta_F = \Delta$. The following result includes a genus one version of the class number formula (1.5).

[4] In fact, there are only finitely many classes of forms with a given discriminant. For a general result that includes the quartic case see [2].

Theorem 2. *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve as in (2.1) with positive discriminant and define $Z_E(s)$ by (2.5). Then $Z_E(s)$ has a meromorphic continuation to $\mathbb{C}$ that is holomorphic for $\operatorname{Re} s > \frac{1}{4}$ except for a (possible) simple pole at $s = \frac{1}{2}$. Suppose that 2 is the only prime whose square divides Δ. Then*

$$\operatorname{Res}_{s=\frac{1}{2}} Z_E(s) = \tfrac{1}{8}\,\Omega_E\, h_E, \tag{3.5}$$

where Ω_E was given in (2.2).

By Ikehara's version of the Wiener-Ikehara theorem [18], Theorem 2 yields the limit formula

$$\lim_{N\to\infty} \tfrac{1}{\sqrt{N}} \sum_{n\leq N} \nu_E(n) = \tfrac{3\Delta\Omega_E}{2\pi^2\,\psi(\Delta)}\, h_E. \tag{3.6}$$

Although it converges slowly, (3.6) is still useful for computing examples.

It follows from the final theorem of [16] that the curves to which Theorem 2 applies exist in abundance. Explicitly, if B is a fixed odd integer, then for a positive proportion of values of $-A \in \mathbb{Z}^+$ we have that $\Delta = 2^4 N$ with $N \in \mathbb{Z}^+$ square-free. See the end of §8 for a remark about weakening the assumption that 2 is the only prime whose square divides Δ.

As was done in the genus zero case, it is possible to define

$$\mathcal{L}(s) = \sum_{n\geq 1} \alpha(n) n^{-s}$$

through the factorization $\zeta(2s)\mathcal{L}(s) = Z_E(s)$. Explicitly

$$\alpha(n) = \sum_{\substack{d^2|n \\ \gcd(d,\Delta)=1}} \lambda(d)\, \nu_E(\tfrac{n}{d^2}),$$

where λ is the Liouville function defined by $\lambda(n) = (-1)^{a_1+\cdots+a_\ell}$, when the prime factorization of n is $n = p_1^{a_1}\cdots p_\ell^{a_\ell}$. By Theorem 2, $\mathcal{L}(s)$ is holomorphic for $\operatorname{Re}(s) \geq \frac{1}{2}$ and, if we assume RH, for $\operatorname{Re}(s) > \frac{1}{4}$. In any case, we have that

$$\mathcal{L}(\tfrac{1}{2}) = \tfrac{1}{4}\Omega_E\, h_E.$$

Whether or not $\mathcal{L}(s)$ is entire is open.

4. Examples

One may in practice always determine a complete set of representatives for the classes $\mathcal{F}_E/\Gamma$. The method is explained in an appendix. Here I will record the results for some examples.

Example 1. The curve $E : y^2 = x^3 - x$ has CM. Here $\Delta = 2^6$ and $I = 4, J = 0$ and

$$\Omega_E = \frac{\sqrt{\pi}\,\Gamma\left(\frac{1}{4}\right)}{\Gamma\left(\frac{3}{4}\right)}.$$

There are two classes in $\mathcal{F}_E^+$ represented by $F_1 = (1, 0, 1, 0, 1)$ and $F_2 = (1, 0, 0, 0, 4)$, both properly primitive. Only F_1 has non-trivial automorphs. Thus

$$h_E = \tfrac{3}{2}.$$

By Theorem 2 we have

$$\operatorname{Res}_{s=1} Z_E(s) = \tfrac{3}{16}\Omega_E.$$

As can be easily checked, for $N = 5000$

$$\frac{\pi^{\frac{3}{2}}\Gamma(\frac{3}{4})}{\Gamma(\frac{1}{4})}\frac{1}{\sqrt{N}}\sum_{n\leq N}\nu_E(n) = 1.4905\ldots. \tag{4.1}$$

Example 2. The example illustrated in Figure 1 is $E : y^2 = x^3 - 2x + 1$, for which $\Delta = 2^4\,5$ with $I = 8$ and $J = -4$. Here

$$\Omega_E = 5.93764989368\ldots.$$

There are four classes in $\mathcal{F}_E^+$ represented by

$$\begin{aligned} F_1 &= (1,1,1,-1,1) \quad & F_1' &= (1,-1,1,1,1) \\ F_2 &= (2,1,0,-1,2) \quad & F_2' &= (2,-1,0,1,2). \end{aligned}$$

Note that F_2 and F_2' are improperly primitive: $\hat{F}_2 = \hat{F}_2' = 2$. All of the forms have non-trivial automorphs. Thus $h_E = 2$. By Theorem 2 we have

$$\operatorname{Res}_{s=1} Z_E(s) = \tfrac{1}{4}\Omega_E.$$

Now for $N = 5000$

$$\frac{6\pi^2}{5\Omega_E}\frac{1}{\sqrt{N}}\sum_{n\leq N}\nu_E(n) = 2.03102\ldots.$$

Example 3. Take $E : y^2 = x^3 - 13x + 5$, with $\Delta = 2^4 \cdot 7 \cdot 19 \cdot 61$, $I = 52$ and $J = -20$. Here

$$\Omega_E = 2.88096982267237\ldots.$$

There are four classes in $\mathcal{F}_E^+$ represented by

$$\begin{aligned} F_1 &= (2,-1,2,4,12) \quad & F_1' &= (2,1,2,-4,12) \\ F_2 &= (3,2,2,-2,8) \quad & F_2' &= (3,-2,2,2,8). \end{aligned}$$

All are properly primitive. None have nontrivial automorphs. Thus $h_E = 4$. By Theorem 2 we have

$$\operatorname{Res}_{s=1} Z_E(s) = \tfrac{1}{2}\Omega_E$$

and for $N = 5000$

$$\frac{9920\,\pi^2}{8113\,\Omega_E}\frac{1}{\sqrt{N}}\sum_{n\leq N}\nu_E(n) = 4.02824\ldots.$$

5. Arithmetic covariants and a syzygy of Cayley and Hermite

The proof of Theorem 2 relies on the arithmetic invariant theory[5] of binary quartic forms. Given any integral quartic form $F = (a, b, c, d, e)$, say that a binary form $P_F(x, y)$ whose coefficients are integral polynomials in a, b, c, d, e is an (arithmetic) covariant for F if

$$P_F|g = P_{F|g}$$

for all $g \in \Gamma$. An invariant is also a covariant. The most basic arithmetic covariant of F is F itself. Clearly the gcd of the coefficients of a covariant P_F is an invariant, say $\hat{P}_F$. The (normalized) Hessian of F is

$$H_F(x,y) = \tfrac{1}{144}\det\begin{pmatrix} F_{xx} & F_{xy} \\ F_{yx} & F_{yy}\end{pmatrix} = a_1x^4 + b_1x^3y + c_1x^2y^2 + d_1xy^3 + e_1y^4. \tag{5.1}$$

[5] The qualifer "arithmetic" was employed in [28] to distinguish the theory of invariants with respect to $\mathrm{SL}(2,\mathbb{Z})$ from the theory over $\mathbb{R}$ or $\mathbb{C}$.

The coefficients of H_F are integers and are given by

$$a_1 = ac - b^2,\ b_1 = 2(ad - bc),\ c_1 = ae + 2bd - 3c^2,\ d_1 = 2(eb - dc),\ e_1 = ec - d^2. \tag{5.2}$$

The sextic covariant T_F of F is defined in terms of Jacobian of F and H_F:

$$\begin{aligned} T_F(x,y) &= -\tfrac{1}{8}\det\begin{pmatrix} \partial_x F & \partial_y F \\ \partial_x H_F & \partial_y H_F \end{pmatrix} \\ &= a_2x^6 + b_2x^5y + c_2x^4y^2 + d_2x^3y^3 + c_2'x^2y^4 + b_2'xy^5 + a_2'y^6. \end{aligned} \tag{5.3}$$

Here the coefficients are given by

$$\begin{aligned} a_2 &= a^2d - 3abc + 2b^3 & a_2' &= -e^2b + 3edc - 2d^3 \\ b_2 &= a^2e + 2abd - 9ac^2 + 6b^2c & b_2' &= -e^2a - 2edb + 9ec^2 - 6d^2c \\ c_2 &= 5abe - 15acd + 10b^2d & c_2' &= -5eda + 15ecb - 10d^2b \\ d_2 &= 10eb^2 - 10ad^2. \end{aligned} \tag{5.4}$$

Conventions: In the following I will usually omit the subscript for an invariant or a covariant when the form is F, e.g. assume that $H = H_F$. Also, I will use the notation

$$[a,b,c] = ax^2 + bxy + cy^2,\quad [a,b,c,d] = ax^3 + bx^2y + cxy^2 + dy^3,\quad \text{etc.}$$

for forms without binomial coefficients.

The relationship that exists between binary quartic forms and elliptic curves is due to a remarkable identity, or syzygy, discovered independently by Cayley [4] and Hermite [14] (cf. [35] and [36]). Its application to Diophantine equations was apparently first made by Mordell in 1914 [23] (see also [26]). This syzygy is an identity that relates F, I, J, H and T. Once given, it may be verified by direct computation.

Proposition 1. *The covariants and invariants F, I, J, H and T satisfy for all x, y*

$$T^2 = -4H^3 + IF^2H - JF^3. \tag{5.5}$$

Clearly, invariants and covariants of covariants give new invariants and covariants. The following identities, which were also given by Cayley [5, §134], can be verified by direct calculation as well. For more on their derivation see [3, §180] (see also [29, p. 201]).

Lemma 1. *For a binary quartic form F and its Hessian H we have for all x, y*

i) $\Delta_{xF+6yH} = \Delta[1, 0, -9I, -54J]^2 = \Delta(x^3 - 9Ixy^2 - 54Jy^3)^2$

ii) $H_{xF+6yH} = [0, I, 9J]F + [1, 0, -3I]H = (Ixy + 9Jy^2)F + (x^2 - 3Iy^2)H.$

A special quartic covariant we will need is

$$K_F(x,y) = 2IH(x,y) - 3JF(x,y). \tag{5.6}$$

Here Lemma 1 gives the elegant formulas

$$\Delta_{K_F} = J^2\Delta^3 \quad \text{and} \quad H_{3K_F} = -3\Delta\, H. \tag{5.7}$$

Suppose that

$$P(x,y) = [a_1, a_2, \ldots, a_7]$$

is a sextic. Denote its (normalized) discriminant by Δ_P, so that

$$\Delta_P = (a_1a_2a_3a_4a_5)^2 + \cdots$$

is of degree ten as a homogeneous form in the coefficients of P. A straightforward computation yields the following formula, which we will need in the proof of Theorem 2.

Lemma 2. *The discriminant of the sextic covariant T of F satisfies*

$$\Delta_T = -2^8\Delta^5. \tag{5.8}$$

6. A correspondence of Mordell

The Cayley-Hermite syzygy leads one to suspect that a correspondence exists between integral points on E_n^* and binary quartic forms. The suspicion is correct and we must make the correspondence precise.

Say $F = (a, b, c, d, e)$ is *admissible* if $\gcd(a, b) = 1$. Clearly an admissible F is primitive. The set of all admissible binary quartic forms $F = (a, b, c, d, e)$ with invariants $I = -4A$ and $J = -4B$ splits into classes under

$$\Gamma_\infty = \{\pm \left(\begin{smallmatrix} 1 & \ell \\ 0 & 1 \end{smallmatrix}\right)\}; \ell \in \mathbb{Z}\}.$$

Note that while the condition $\gcd(a, b) = 1$ is not preserved in general under Γ-equivalence, it is preserved under Γ_∞-equivalence since

$$(a, b, c, d, e)|(\pm \left(\begin{smallmatrix} 1 & \ell \\ 0 & 1 \end{smallmatrix}\right)) = (a, b + \ell a, *, *, *). \tag{6.1}$$

The following result[6] is a refinement and reworking of a theorem of Mordell [26, p.233].

Proposition 2. *Suppose that $A, B \in \mathbb{Z}$ have $\Delta = -4(4A^3 - 27B^2) \neq 0$. The map*

$$F \mapsto \big(-H(1, 0), \tfrac{1}{2}T(1, 0), F(1, 0)\big) \tag{6.2}$$

gives a well-defined bijection from the set $\mathcal{F}$ of all Γ_∞-classes of admissible binary quartic forms F with invariants $I = -4A$ and $J = -4B$ and with $F(1, 0) > 0$ to the set of integer triples

$$\mathcal{S} = \{(x, y, n) \in \mathbb{Z}^2 \times \mathbb{Z}^+; \ \ \textit{with } y^2 = x^3 + Axn^2 + Bn^3 \textit{ and } \gcd(x, n) = 1\}.$$

Proof. First, F with $F(1, 0) > 0$ is admissible if and only if $\gcd(F(1, 0), H(1, 0)) = 1$ since $H(1, 0) = ac - b^2$ by (5.2). By the Cayley-Hermite syzygy (5.5) we see that

$$\big(-H(1, 0), \tfrac{1}{2}T(1, 0), F(1, 0)\big) \in \mathcal{S}$$

for $F \in \mathcal{F}$, upon noticing that $4|I$ and $4|J$ implies that $2|T(1, 0)$. The values $-H(1, 0)$, $\frac{1}{2}T(1, 0)$ and $F(1, 0)$ are semi-invariants, meaning that they are invariant under Γ_∞, so the map from $\mathcal{F}$ to $\mathcal{S}$ determined by (6.2) is well-defined.

We next show it is surjective. Given $(x, y, n) \in \mathcal{S}$ we must find $F = (a, b, c, d, e)$ with $a = F(1, 0) = n$, $-H(1, 0) = x$, and $\frac{1}{2}T(1, 0) = y$. Also we require that $I = -4A$ and $J = -4B$. We have that $\gcd(x, n) = 1$ so any F we find will be admissible. As is forced, choose $a = n$.

If $x = 0$ then $a = 1$ and let $b = 0$. Otherwise choose

$$b \equiv y/x \pmod{a^2}.$$

Then c, d, e are determined as rational numbers from (3.2), (5.2) and (5.4):

$$x = b^2 - ac, \quad 2y = a^2d - 3abc + 2b^3, \quad -4A = ae - 4bd + 3c^2. \tag{6.3}$$

If $x = 0$ these require that $F = [1, 0, 0, 2y, -4A]$, which has the correct invariants.

Otherwise,

$$ac \equiv (y^2 - x^2)/x^2 \pmod{a^2}$$

[6] In the published version the condition $F(1, 0) > 0$ was left out in the statement and in the first line of the proof.

implies that $c \in \mathbb{Z}$. Similarly,

$$a^2 d = b^3 - 3bx + 2y \equiv \tfrac{y(y^2-x^3)}{x^3} \equiv 0 \pmod{a^2}$$

so $d \in \mathbb{Z}$. Finally, from (6.3) and using

$$y^2 = x^3 + Aa^2x + Ba^3$$

we get after a calculation that

$$-4B = ace + 2bcd - ad^2 - b^2e - c^3. \tag{6.4}$$

By the formula for $-4A$ in (6.3) we see that ae is an integer and $(ac - b^2)e$ is an integer by (6.4). Since $\gcd(a, b) = \gcd(a, ac - b^2) = 1$, we have that $e \in \mathbb{Z}$. That $F = (a, b, c, d, e)$ has the correct invariants follows from (6.3) and (6.4).

To see that the map is injective observe that once b is chosen $\pmod{a^2}$, the other coefficients are determined. But in view of (6.1) different choices of b result in Γ_∞-equivalent forms. □

Next we restrict this correspondence to the positive definite forms.

Proposition 3. *If $\Delta > 0$ the bijection of Proposition 2 restricts to one between those classes in $\mathcal{F}$ consisting of positive definite forms and triples $(x, y, n) \in \mathcal{S}$ where $e_1 \leq \frac{x}{n} \leq e_2$. Here $e_1 < e_2 < e_3$ are the zeros of $x^3 + Ax + B$.*

Proof. It is enough to show that F with $\Delta_F = \Delta > 0$ and invariants $I = -4A$ and $J = -4B$ is positive definite precisely when

$$e_1 \leq \frac{-H(1,0)}{F(1,0)} \leq e_2. \tag{6.5}$$

Given that $\Delta > 0$, F is positive definite if and only if $a > 0$ and $F(x, 1) = 0$ has no real roots. By [3, §68] this is equivalent to $\Delta > 0, a > 0$ and

$$a^2 I + 12H(1,0) \geq 0.$$

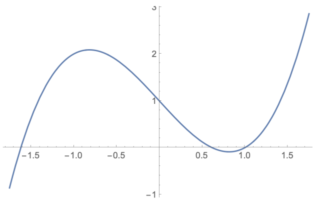

Figure 2. $y = x^3 - 2x + 1$

Thus the form F is positive definite if and only if $\Delta_F > 0$, $F(1, 0) = a > 0$ and

$$\frac{-H(1,0)}{F(1,0)} \leq \sqrt{\frac{I}{12}}. \tag{6.6}$$

Now (6.5) holds if and only if $\frac{-H(1,0)}{F(1,0)} < e_3$. This is equivalent to (6.6) since the local minimum on the curve $y = x^3 + Ax + B$ occurs when

$$x = \sqrt{\frac{|A|}{3}} = \sqrt{\frac{I}{12}}$$

See Figure 2 for the case $A = -2, B = 1$ and $\sqrt{|A|/3} = .816\ldots.$ □

7. The counting function

We need to express $\nu_E(n)$ from (2.4) in an analytically usable form. For this we will rephrase Mordell's correspondence. For a fixed form $F \in \mathcal{F} = \mathcal{F}(I, J)$ and prime p define

$$B_F(p) = \{r = (r_1, r_2) \in (\mathbb{Z}/p\mathbb{Z})^2; F(r) \equiv 0 \text{ and } H(r) \equiv 0 \pmod{p}\}. \tag{7.1}$$

Let $q = \prod_{p|\Delta} p$ be the product of all distinct primes dividing Δ and define R_F to be the set of all $r \in (\mathbb{Z}/q\mathbb{Z})^2$ which, when reduced mod p, are not in $B_F(p)$ for any $p|\Delta$.

Proposition 4. *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve as in (2.1) with positive discriminant. Notation as above, for $n \in \mathbb{Z}^+$ we have*

$$\nu_E(n) = \sum_{F \in \mathcal{F}_E/\Gamma} \frac{\#\{m \in \mathbb{Z}^2; \gcd(m_1, m_2) = 1,\ \ \overline{m} \in R_F; \textit{and } F(m) = n\}}{\#\mathrm{Aut}\, F}, \tag{7.2}$$

where $\overline{m}$ denotes the reduction of m modulo q.

Proof. Note that as a set R_F is not a class invariant. Nonetheless, the sum in (7.2) is well-defined. To see this recall that H, which occurs in the definition (7.1), is a covariant.

Observe that the Γ_∞-classes of a form F are represented by

$$\mathcal{M} = \{m = (m_1, m_2) \in \mathbb{Z}^2 \text{ with } \gcd(m_1, m_2) = 1\}$$

via $F \mapsto F| \left(\begin{smallmatrix} m_1 & * \\ m_2 & * \end{smallmatrix}\right)$. Here m and $-m$ give rise to the same class and if $\#\mathrm{Aut}\, F = 4$ so do two other pairs. With this proviso, the representation is unique. For any form F say that m is admissible (for F) if $F| \left(\begin{smallmatrix} m_1 & * \\ m_2 & * \end{smallmatrix}\right)$ is admissible, as defined near the beginning of §6. The map of Proposition 2 induces a map

$$m \mapsto \big(-H(m_1, m_2), \tfrac{1}{2}T(m_1, m_2), F(m_1, m_2)\big)$$

from admissible m for F to $\mathcal{S}$, where F is a fixed representative of a class in $\mathcal{F}/\Gamma$. It is either two-to-one or four-to-one and, when applied to a full set of representatives for $\mathcal{F}/\Gamma$, it is surjective. By Proposition 3 it restricts appropriately when we only choose representatives from $\mathcal{F}_E/\Gamma$.

Recall that F is admissible if and only if $\gcd(F(1,0), H(1,0)) = 1$. In order to isolate admissible m for each representative F, we must remove all $m \in \mathcal{M}$ with

$$p| \gcd(F(m), H(m))$$

for any prime p. The following lemma shows that we need only do this for $p|\Delta$.

Lemma 3. *Let $F = (a, b, c, d, e)$. If $p| \gcd(a, b)$ then $p|\Delta_F$.*

Proof. The discriminant of F expanded out is

$$\begin{aligned} \Delta_F = {} & -27a^2d^4 - 27b^4e^2 - 54b^2c^3e + 54ab^2ce^2 - 180abc^2ed + \\ & 108b^3ced - 6ab^2ed^2 + 81ac^4e + a^3e^3 + 54a^2ced^2 - 12a^2be^2d \\ & - 18a^2c^2e^2 - 54ac^3d^2 + 108abcd^3 - 64b^3d^3 + 36b^2c^2d^2. \end{aligned} \tag{7.3}$$

If $p| \gcd(a, b)$ then an examination of each term shows that $p|\Delta_F$.

□

Proposition 4 now follows from the next lemma. □

Lemma 4. *The admissible $m \in \mathcal{M}$ for F are precisely those that reduce modulo q to some $r \in R_F$. Every $r \in R_F$ will be represented by some admissible $m \in \mathcal{M}$ reduced modulo q.*

Proof. The first statement follows by Lemma 3 and the definition of R_F given below (7.1). For the second, if $r = (r_1, r_2) \in R_F$ then $\gcd(r_1, r_2, q) = 1$. If $r_1 = 0$ choose $m = (q, r_2)$. Otherwise, let

$$P = \prod_{\substack{p \mid r_1,\, p \nmid q \\ p \text{ prime}}} p$$

and choose $m_1 = r_1$ and $m_2 = r_2 + \ell q$ where ℓ satisfies

$$\ell q \equiv 1 - r_2 \,(\operatorname{mod} P).$$

This is possible since $\gcd(q, P) = 1$. □

8. Arithmetic invariants and covariants modulo a prime

In this section I will provide some results about the reductions of arithmetic invariants and covariants of a primitive quartic form F modulo a prime p. These are applied to count elements in $B_F(p)$ and hence determine the class invariant $\#R_F$. It is crucial that, under our assumptions, $\#R_F$ is actually independent of the class of F and non-zero.

Proposition 5. *Suppose that* $4|I$, $4|J$ *and that* $p^2|\Delta$ *implies that* $p = 2$. *Then*

$$\#R_F = q^2 \prod_{p|\Delta} (1 - p^{-1}).$$

For short we write $x \equiv y$ for $x \equiv y \pmod p$. Recall the definition of $B_F(p)$ from (7.1):

$$B_F(p) = \{m \in (\mathbb{Z}/p\mathbb{Z})^2; F(m) \equiv 0 \text{ and } H(m) \equiv 0\}.$$

By the Chinese remainder theorem we have

$$\#R_F = \prod_{p|\Delta} \big(p^2 - \# B_F(p)\big). \tag{8.1}$$

To prove Proposition 5 we must show that $\#B_F(p) = p$ for all $p \mid \Delta$ with $p^2 \nmid \Delta$ or $p = 2$.

Case $p = 2$**.** Here we will show that $F = (a, b, c, d, e)$ and H always share two zeros in $(\mathbb{Z}/2\mathbb{Z})^2$. When $p = 2$ we must allow the possibility that $\hat{F} \equiv 0$. Since $4|I$ it follows from this that we must have $2|c$. But then

$$H(x, y) \equiv (x + y)^4 \quad \text{or} \quad H(x, y) \equiv x^4; \quad \text{or} \quad H(x, y) \equiv y^4$$

and our claim holds.

Suppose that $\hat{F} \not\equiv 0$. There are three possibilities. If $F(x, y) \equiv x^4 + y^4$ then since $4|I$ and $4|J$ we have that $c \equiv 1$ and $b + d \equiv 0$. Thus $H(1, 1) \equiv 0$ and again F and H share two zeros. If $F(x, y) \equiv y^4$ then $c \equiv 0$ and $b \equiv 0$ so now $H(1, 0) \equiv 0$ and again the claim holds. The case $F(x, y) \equiv x^4$ is similar.

Therefore $\#B_F(2) = 2$.

Case $p \neq 2$**.** Since $\Delta = I^3 - 27J^2$, if $3|\Delta$ we must have that $3^3|\Delta$ so we may also assume that $p \neq 3$. By a well-known property of discriminants, if $\Delta \equiv 0$ then either

$$F(x, y) \equiv (rx + sy)^2 Q(x, y) \quad \text{or} \tag{8.2}$$

$$F(x, y) \equiv t\, Q''(x, y)^2, \tag{8.3}$$

where Q and Q'' are quadratic forms over $Z/p\mathbb{Z}$ and Q is either irreducible modulo p or has two distinct roots.

The proof of Proposition 5 is thus reduced to the proof of the following lemma.

Lemma 5. *Suppose that $\Delta \equiv 0$ but $p^2 \nmid \Delta$. Then (8.2) holds and*

$$H(x,y) \equiv (rx+sy)^2 Q'(x,y), \tag{8.4}$$

where the only possible (x,y) with $Q(x,y) \equiv 0$ and $Q'(x,y) \equiv 0$ satisfy $rx+sy \equiv 0$.

To prove Lemma 5 we need the following result about the Hessian and sextic covariants modulo p.

Lemma 6. *Let $F = (a,b,c,d,e)$ be a primitive quartic form. Suppose that $p \neq 2,3$.*

i) Then $\hat{H}_F \equiv 0$ if and only if

$$F(x,y) \equiv t(rx+sy)^4.$$

ii) If $H(x,y) \equiv cF(x,y)$ for some c then $\hat{T} \equiv 0$.
iii) If $F(x,y) \equiv Q(x,y)^2$ then $\hat{T} \equiv 0$.

Proof. The "if" part of the first statement always holds and follows by a direct calculation. For the converse we use (5.2). If $a \equiv 0$ then $b,c,d \equiv 0$ and $F(x,y) \equiv ey^4$. If $c \equiv 0$ then $b \equiv 0$ and either $a \equiv 0$ or $d \equiv 0$. If $a \equiv 0$ we are done from before. If $a \not\equiv 0$ and $d \equiv 0$ we have that $e \equiv 0$ and so $F(x,y) \equiv ax^4$. If $b \equiv 0$ then either $a \equiv 0$ or $c \equiv 0$ and we are done. Thus we may assume that $a \not\equiv 0, b \not\equiv 0$ and $c \not\equiv 0$. Then we have

$$F(x,y) \equiv a^{-3}(ax+by)^4,$$

upon using that $ac \equiv b^2$, $ec \equiv d^2$ and $bd \equiv c^2$, which follow from (5.2).

The second statement is an immediate consequence of the definition of the sextic $T(x,y)$ and always holds, while the third statement follows by direct calculation of $T(x,y)$, using that $p \neq 2,3$.

□

Proof of Lemma 5. By assumption we have that $p \neq 2,3$. An immediate consequence of Lemma 2 is that $p^2 \nmid \Delta$ implies that $\hat{T} \not\equiv 0$, for $p \neq 2$.

If $\hat{T} \not\equiv 0$ then by iii) of Lemma 6 it is not possible for (8.3) to hold so (8.2) must hold.

We now prove that (8.4) is true when $\hat{T} \not\equiv 0$. Our assumption that $p^2 \nmid \Delta$ implies that $I \not\equiv 0$ and $J \not\equiv 0$. By ii) of Lemma 6 we know that $\hat{K}_F \not\equiv 0$, where K_F was defined in (5.6). Since $\Delta \equiv 0$ and $p \neq 3$ we see that the second formula of (5.7) together with i) of Lemma 6 imply that

$$2I\,H(x,y) - 3JF(x,y) \equiv t(rx+sy)^4$$

for some $t \not\equiv 0$. Therefore (8.4) holds with

$$2I\,Q'(x,y) - 3JQ(x,y) \equiv t(rx+sy)^2,$$

from which it is clear that the only possible (x,y) with $Q(x,y) \equiv 0$ and $Q'(x,y) \equiv 0$ satisfy $rx+sy \equiv 0$. □

This completes the proof of Proposition 5.

Remark. It is possible to determine the number of common roots of F and H modulo p without assuming that $p^2 \nmid \Delta$. The answer entails a refinement of Lemma 5 that takes into account the possibility that F factors as the square of a quadratic. This brings into play a kind of quadratic "genus" character whose modulus is a prime divisor of $\hat{T}$. This character would likely play a role in extensions of Theorem 2 covering more general discriminants.

9. Analytic properties of $Z_E(s)$

In this final section we prove Theorem 2. This requires that we establish some analytic properties of $Z_E(s)$. Recall that

$$q = \prod_{p|\Delta} p.$$

For $m = (m_1, m_2)$ and $r = (r_1, r_2) \in (\mathbb{Z}/q\mathbb{Z})^2$ let

$$\Psi^*(s;r) = \sideset{}{'}\sum_{\substack{m \equiv r \,(\mathrm{mod}\, q) \\ \gcd(m_1,m_2)=1}} F(m)^{-s} \qquad \text{for } \mathrm{Re}(s) > 2$$

where $F \in \mathcal{F}_E$ and, as usual, a prime in a sum means that a term where division by zero occurs is omitted. The following result is an immediate consequence of Proposition 4.

Proposition 6. *For* $\mathrm{Re}(s) > 2$

$$\sum_{n \geq 1} \nu_E(n) n^{-s} = \sum_{F \in \mathcal{F}_E/\Gamma} \tfrac{1}{\#\mathrm{Aut}\, F} \sum_{r \in R_F} \Psi^*(s;r).$$

Next define

$$\Psi(s;r) = \sideset{}{'}\sum_{m \equiv r \,(\mathrm{mod}\, q)} F(m)^{-s}.$$

Proposition 7. $\Psi(s;r)$ *has analytic continuation in* s *to an entire function except for a simple pole at* $s = \frac{1}{2}$. *The residue there is given by*

$$\mathrm{Res}_{s=\frac{1}{2}} \Psi(s;r) = \tfrac{1}{4} q^{-2} \int_0^{2\pi} F(\cos\theta, \sin\theta)^{-\frac{1}{2}} d\theta.$$

Proof. We will prove this rather standard result using Poisson summation and the function

$$\Theta(t) = \sum_{\substack{m \in \mathbb{Z}^2 \\ m \equiv r \bmod q}} e^{-tF(m)},$$

defined and convergent for $t > 0$. Recall that $F \in \mathcal{F}_E$ is positive definite so that for some constant $c > 0$ we have

$$|F(u)| \geq c|u|^4$$

for all $u \in \mathbb{R}^2$. Let $\Phi(v)$ be the Fourier transform of $e^{-tF(u)}$, defined for $v = (v_1, v_2) \in \mathbb{R}^2$ by

$$\Phi(v) = \int_{\mathbb{R}^2} e^{-tF(u)} e(-u \cdot v)\, du_1\, du_2, \quad e(x) = e^{2\pi i x}.$$

As is well-known, $\Phi(v)$ is of rapid decay. The Poisson summation formula (see e.g. [32]) yields the following for $t > 0$:

$$\Theta(t^{-1}) = q^{-2} t^{\frac{1}{2}} \sum_{m \in \mathbb{Z}^2} \Phi(q^{-1} t^{\frac{1}{4}}\, m) e(\tfrac{m \cdot r}{q}). \tag{9.1}$$

As in Riemann's second proof of the analytic continuation and functional equation for $\zeta(s)$, start with

$$\Gamma(s)\Psi(s;r) = \int_0^\infty (\Theta(t) - 1) t^s \tfrac{dt}{t} = \int_0^1 + \int_1^\infty = I + II,$$

say. Now II is clearly an entire function. On the other hand, changing variable $t \mapsto \frac{1}{t}$ and using (9.1) we have

$$I = q^{-2}\int_1^\infty t^{\frac{1}{2}-s}\sideset{}{'}\sum_{m\in\mathbb{Z}^2}\Phi(q^{-1}t^{\frac{1}{4}}m)e(\tfrac{m\cdot r}{q})\tfrac{dt}{t} - \tfrac{1}{s} + q^{-2}\Phi(0)\,\tfrac{1}{s-\frac{1}{2}}.$$

Again the integral here is entire. The proof is completed by computing

$$\begin{aligned}\Phi(0) = \int_{\mathbb{R}^2} e^{-tF(u)}du &= \int_0^{2\pi}\int_0^\infty \rho\, e^{-F(\rho\cos\theta,\rho\sin\theta)}d\rho d\theta \\ &= \tfrac{1}{4}\int_0^{2\pi}\int_0^\infty t^{\frac{1}{2}}e^{-\rho F(\cos\theta,\sin\theta)}\tfrac{d\rho}{\rho}d\theta \\ &= \tfrac{\sqrt{\pi}}{4}\int_0^{2\pi} F(\cos\theta,\sin\theta)^{-\frac{1}{2}}d\theta.\end{aligned}$$

□

Proposition 8. *The function $\Psi^*(s;r)$ has a meromorphic continuation to $\mathbb{C}$ and it is holomorphic for* $\mathrm{Re}(s) > \frac{1}{4}$ *except for a simple pole at $s = \frac{1}{2}$ with*

$$\mathrm{Res}_{s=\frac{1}{2}}\Psi^*(s;r) = \tfrac{1}{4}\,q^{-2}\prod_{p\nmid q}(1-p^{-2})\Omega_E.$$

Proof. In order to represent $\Psi^*(s;r)$ we will use the Möbius function μ, which satisfies the identity

$$\sum_{d|n}\mu(d) = \begin{cases}1 & \text{if } n=1\\ 0 & \text{if } n\neq 1.\end{cases}$$

Thus

$$\begin{aligned}\Psi^*(s;r) &= \sideset{}{'}\sum_{\substack{m\in\mathbb{Z}^2\\ m\equiv r\,(\mathrm{mod}\,q)}}\ \sum_{d|\gcd(m_1,m_2)}\mu(d)F(m)^{-s} \\ &=\sum_{d\geq 1}\ \sideset{}{'}\sum_{\substack{m\in\mathbb{Z}^2\\ dm\equiv r\,(\mathrm{mod}\,q)}}\mu(d)F(dm)^{-s} \\ &= \sum_{\substack{\ell\,(\mathrm{mod}\,q)\\ \gcd(\ell,q)=1}}\ \sum_{d\equiv\ell\,(\mathrm{mod}\,q)}\mu(d)d^{-4s}\ \sideset{}{'}\sum_{\substack{m\in\mathbb{Z}^2\\ m\equiv\ell^{-1}r\,(\mathrm{mod}\,q)}}F(m)^{-s} \\ &= \sum_{\substack{\ell\,(\mathrm{mod}\,q)\\ \gcd(\ell,q)=1}}\ \sum_{d\equiv\ell\,(\mathrm{mod}\,q)}\mu(d)d^{-4s}\Psi(s;\ell^{-1}r).\end{aligned}$$

Note that we have

$$\sum_{d\equiv\ell\,(\mathrm{mod}\,q)}\mu(d)d^{-4s} = \frac{1}{\phi(q)}\sum_{\chi}\overline{\chi}(\ell)L(4s,\chi)^{-1},$$

where $L(4s,\chi)$ is the Dirichlet L-function, and the sum on the right hand side is over all Dirichlet characters modulo q. It is now easy to see using Proposition 7 and standard properties of Dirichlet L functions that $\Psi^*(s;r)$ has a meromorphic continuation to $\mathbb{C}$ and that it is holomorphic for $\mathrm{Re}(s) > \frac{1}{4}$, except for a simple pole at $s = \frac{1}{2}$ with

$$\begin{aligned}\mathrm{Res}_{s=\frac{1}{2}}\Psi^*(s;r) &= \sum_{\substack{\ell \,(\mathrm{mod}\, q)\\ \gcd(\ell,q)=1}} \sum_{d\equiv \ell \,(\mathrm{mod}\, q)} \mu(d)d^{-4s}\mathrm{Res}_{s=\frac{1}{2}}\Psi(s;\ell^{-1}r)\\ &= \tfrac{1}{4}\, q^{-2}\prod_{p\nmid q}(1-p^{-2})\int_0^{2\pi} F(\cos\theta,\sin\theta)^{-\frac{1}{2}}d\theta.\end{aligned}$$

To finish the proof we apply the following standard evaluation:

$$\int_0^{2\pi} F(\cos\theta,\sin\theta)^{-\frac{1}{2}}d\theta = \Omega_E.$$

□

We are now ready to complete the proof of Theorem 2. First note that by (2.5) and Proposition 6

$$\begin{aligned}Z_E(s) &= \zeta(4s)\prod_{p\mid q}(1+p^{-2s})\sum_{n\geq 1}\nu_E(n)n^{-s}\\ &= \zeta(4s)\prod_{p\mid q}(1+p^{-2s})\sum_{F\in\mathcal{F}_E/\Gamma}\tfrac{1}{\#\mathrm{Aut}\,F}\sum_{r\in R_F}\Psi^*(s;r).\end{aligned} \tag{9.2}$$

Therefore Proposition 8 implies the first statement of Theorem 2. From the residue evaluation of Proposition 8 we have

$$\mathrm{Res}_{s=\frac{1}{2}}Z_E(s) = \tfrac{1}{4}\,\Omega_E\, q^{-2}\prod_{p\nmid q}(1-p^{-2})\prod_{p\mid q}(1+p^{-1})\zeta(2)\sum_{F\in\mathcal{F}_E/\Gamma}\tfrac{\#R_F}{\#\mathrm{Aut}\,F}.$$

Note that, in general, $\#R_F$ depends on the class of F. To finish the proof of Theorem 2 we apply Proposition 5, which was proven under the condition that 2 is the only prime whose square divides Δ. It gives

$$\begin{aligned}\mathrm{Res}_{s=\frac{1}{2}}Z_E(s) =& \tfrac{\Omega_E}{2}\prod_{p\nmid q}(1-p^{-2})\prod_{p\mid q}(1-p^{-2})\zeta(2)\sum_{F\in\mathcal{F}_E/\Gamma}\tfrac{1}{\#\mathrm{Aut}\,F}\\ =& \tfrac{\Omega_E}{4}\sum_{F\in\mathcal{F}_E/\Gamma}\tfrac{1}{\#\mathrm{Aut}\,F},\end{aligned}$$

as desired. □

Remarks. This part of the proof of Theorem 2 comes down to counting certain integers represented by binary quartic forms, which is a well-studied problem (see [17], [22], [33]).

The family of twisted elliptic curves we study may be considered as a single elliptic surface and it is natural to seek asymptotic formulas for the count of integral points on more general elliptic surfaces. The methods of this paper may also be applied to estimate the number of rational points of bounded height on some elliptic surfaces, such as those treated in [21], [27].

For certain potential generalizations, the spectral technique for counting integer points on varieties introduced in [12] should be applicable.

Acknowledgements. I thank Özlem Imamoḡlu, Ze'ev Rudnick and Peter Sarnak for their many comments and valuable suggestions that helped me improve an earlier version of this paper. I am also grateful to the referee for some insightful suggestions.

Appendix A. Reduction of positive quartic forms

This appendix shows how to determine a complete set of representatives

$$F = (a, b, c, d, e)$$

for $\mathcal{F}_E/\Gamma$ with $\mathcal{F}_E$ defined in (3.4). The proofs of Propositions 2 and 3, when combined with an estimate for the minimum of a form, provide the method.

First list all possible values of $a \leq M$ where M depends only on E and is large enough to bound the minimum of any form $F \in \mathcal{F}_E$. Next find by inspection all $(x, y) \in E_a(\mathbb{Z})$ where $ae_1 \leq x \leq ae_2$ and then all solutions b of $b^2 \equiv x \pmod{a}$. Note that we are not assuming that $\gcd(x, a) = 1$. For each such b we can check to see if c, d and e as determined in (6.3) are integers. When they are integers we get a form with the needed invariants. In view of the proofs of Propositions 2 and 3, we are assured that every class will be represented. Now remove from the set any form whose a-value in not its minimum, which is possible since the forms are positive definite.

Different forms F, F' produced in this way must be inequivalent. First they must have the same minimum to be equivalent. But two equivalent forms with the same minimum a are equivalent with respect to Γ_∞. Also, if (x, y) belongs to F and (x', y') to F' then $x = -H_F(1, 0), x' = -H_{F'}(1, 0), y = \frac{1}{2}T_F(1, 0)$ and $y' = \frac{1}{2}T_{F'}(1, 0)$. But $H_F(1, 0)$ and $T_F(1, 0)$ are both semi-invariants (invariant under Γ_∞) so $x = x'$ and $y = y'$. Finally, b is fixed modulo a so all coefficients are determined.

A simple and useful value for M can be derived from [7, Prop. 11 (i)]:

$$M = \tfrac{4}{3}(e_2 - e_1). \tag{A.1}$$

To find the optimal M for the set of all positive (not necessarily integral) quartic forms with given invariants is a problem in the geometry of numbers. By using results from [8], one can reduce the value of M in (A.1) in some cases.

References

1. Bhargava, Manjul; Shankar, Arul. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. Ann. of Math. (2) 181 (2015), no. 1, 191–242.
2. Birch, B. J.; Merriman, J. R. Finiteness theorems for binary forms with given discriminant. Proc. London Math. Soc. (3) 24 (1972), 385–394.
3. Burnside, William Snow; Panton, Arthur William. The theory of equations: With an introduction to the theory of binary algebraic forms. 2 volumes Dover Publications, Inc., New York 1960 xiv+286, 318 pp.
4. Cayley, A. Note sur les covariants d'une fonction quadratique, cubique, ou biquadratique à deux indéterminnées, J. Reine Angew. Math. 50 (1855), 285–287, in Collected Papers Vol. 2. #135.
5. Cayley, A. A fifth memoir upon quantics, Phil. Trans. Royal Soc. 148 (1858), 429–460, in Collected Papers 2, # 156.
6. Cox, David A. Primes of the form $x^2 + ny^2$. Fermat, class field theory, and complex multiplication. Second edition. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, 2013. xviii+356 pp.
7. Cremona, J. E. Reduction of binary cubic and quartic forms. LMS J. Comput. Math. 2 (1999), 64–94.
8. Davis, C. S. The minimum of a binary quartic form. I. Acta Math. 84 (1951), 263–298.
9. Davenport, Harold. Multiplicative number theory. Third edition. Revised and with a preface by Hugh L. Montgomery. Graduate Texts in Mathematics, 74. Springer-Verlag, New York, 2000. xiv+177 pp.
10. Dirichlet, P. G. L. Vorlesungen über Zahlentheorie. Herausgegeben und mit Zusätzen versehen von R. Dedekind. Vierte, umgearbeitete und vermehrte Auflage Chelsea Pub. Co., New York 1968 xvii+657 pp.
11. Dirichlet, P. G. L. Lectures on number theory. Supplements by R. Dedekind. Translated from the 1863 German original and with an introduction by John Stillwell. History of Mathematics, 16. American Mathematical Society, Providence, RI; London Mathematical Society, London, 1999. xx+275 pp.

12. Duke, W.; Rudnick, Z.; Sarnak, P. Density of integer points on affine homogeneous varieties. Duke Math. J. 71 (1993), no. 1, 143–179.
13. Gauss, Carl Friedrich. Disquisitiones arithmeticae. Translated into English by Arthur A. Clarke, S. J. Yale University Press, New Haven, Conn.-London 1966 xx+472 pp.
14. Hermite, C. Note sur la réduction des fonctions homogènes à coefficients entiers et à deux indéterminées. J. Reine Angew. Math. 36 (1848), 357–364, in Oeuvres I, 84–93.
15. Hermite, C. Sur l'introduction des variables continues dans la théorie des nombres. J. Reine Angew. Math. 41 (1851), 191–216, in Oeuvres, I, 164–192.
16. Hooley, Christopher. On the square-free values of cubic polynomials. J. Reine Angew. Math. 229 (1968), 147–154.
17. Hooley, Christopher. On binary quartic forms. J. Reine Angew. Math. 366 (1986), 32–52.
18. Ikehara, S. An extension of Landau's theorem in the analytic theory of numbers. Journal of Mathematics and Physics of the Massachusetts Institute of Technology. 10 (1931).
19. G. Julia, 'Étude sur les formes binaires non quadratiques à indéterminées réelles ou complexes', Mem. Acad. Sci. l'Inst. France 55 (1917), 1–293.
20. Landau, Edmund. Handbuch der Lehre von der Verteilung der Primzahlen. 2 Bände. Chelsea, New York, 1974.
21. Le Boudec, Pierre. Linear growth for certain elliptic fibrations. Int. Math. Res. Not. IMRN 2015, no. 21, 10859–10871.
22. Mahler, Kurt. Zur Approximation algebraischer Zahlen. III. Über die mittlere Anzahl der Darstellungen grosser Zahlen durch binäre Formen. Acta Math. 62 (1933), no. 1, 91–166.
23. Mordell, L.J. Indeterminate equations of the third and fourth degrees, Q. J. Pure appl. Math. 45 (1914), 170–186.
24. Mordell, L. J. On the rational solutions of the indeterminate equations of the third and fourth degrees. Proc. Cambridge Phil. Soc. 21 (1922), 179–192.
25. Mordell, L. J. Note on the Integer Solutions of the Equation $y^2 = Ax^3 + Bx^2 + Cx + D$. Messenger of Mathematics 51 (1922), pp. 169–171.
26. Mordell, L. J. Diophantine equations. Pure and Applied Mathematics, Vol. 30 Academic Press, London-New York 1969 xi+312 pp.
27. Munshi, Ritabrata. Density of rational points on elliptic fibrations. II. Acta Arith. 134 (2008), no. 2, 133–140.
28. Poincaré, Henri. Sur les invariants arithmétiques, J. Reine Angew. Math. 129 (1905), 89–150 . Also in Oeuvres V, p. 203–266.
29. Salmon, G. Lessons introductory to the modern higher algebra, 5th ed. Chelsea. New York.
30. Siegel, Carl Ludwig. The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + ... + k$, J. London Math. Soc.,1 (1926), 66–68.
31. Siegel, Carl Ludwig. Lectures on the analytical theory of quadratic forms. Notes by Morgan Ward. Third revised edition Buchhandlung Robert Peppmüller, Göttingen 1963 iii+243 pp.
32. Stein, Elias M.; Weiss, Guido. Introduction to Fourier analysis on Euclidean spaces. Princeton Mathematical Series, No. 32. Princeton University Press, Princeton, N.J., 1971. x+297 pp.
33. Stewart, C. L.; Xiao, Stanley Yao. On the representation of integers by binary forms. Math. Ann. 375 (2019), no. 1-2, 133–163.
34. Thue, Axel. Über Annäherungswerte algebraischer Zahlen. J. Reine Angew. Math. 135 (1909), 284–305.
35. Weil, André. Remarques sur un mémoire d'Hermite. (French) Arch. Math. (Basel) 5 (1954), 197–202.
36. Weil, André. Euler and the Jacobians of elliptic curves. Arithmetic and geometry, Vol. I, 353–359, Progr. Math., 35, Birkhäuser Boston, Boston, MA, 1983.

UCLA Mathematics Department, Box 951555, Los Angeles, CA 90095-1555
Email address: wdduke@ucla.edu