

Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves

Manjul Bhargava and Arul Shankar

December 24, 2013

Abstract

We prove a theorem giving the asymptotic number of binary quartic forms having bounded invariants; this extends, to the quartic case, the classical results of Gauss and Davenport in the quadratic and cubic cases, respectively. Our techniques are quite general, and may be applied to counting integral orbits in other representations of algebraic groups.

We use these counting results to prove that the average rank of elliptic curves over \mathbb{Q} , when ordered by their heights, is bounded. In particular, we show that when elliptic curves are ordered by height, the mean size of the 2-Selmer group is 3. This implies that the limsup of the average rank of elliptic curves is at most 1.5.

1 Introduction

1.1 Average ranks of elliptic curves

Any elliptic curve E over \mathbb{Q} is isomorphic to a unique curve of the form $E_{A,B} : y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{Z}$ and for all primes p : $p^6 \nmid B$ whenever $p^4 \mid A$. Let $H(E_{A,B})$ denote the (naive) *height* of $E_{A,B}$, defined by $H(E_{A,B}) := \max\{4|A^3|, 27B^2\}$. Let $\Delta(E_{A,B})$ and $C(E_{A,B})$ denote the discriminant and conductor of $E_{A,B}$, respectively.

It is an old conjecture, originating in works of Goldfeld [28] and Katz-Sarnak [32], that a density of 50% of all elliptic curves over \mathbb{Q} have rank 0 and 50% have rank 1. These densities are expected to hold true regardless of whether one orders curves by height, discriminant, or conductor. In particular, one expects the average rank of all elliptic curves to be $1/2$. However, it has not previously been known that the average rank of all elliptic curves is even *finite* (i.e., bounded). Computations have also not been very helpful in this regard; see [2] for a nice survey.

In [11], Brumer showed that the generalized Riemann hypothesis and the Birch–Swinnerton-Dyer conjectures together imply that the average rank of all elliptic curves, when ordered by their heights, is finite and is in fact bounded above by 2.3. Still assuming the generalized Riemann hypothesis and the Birch–Swinnerton-Dyer conjectures, this constant was subsequently improved to 2 by Heath-Brown [30] and to $25/14 \sim 1.79$ by Young [45].

The purpose of this article is to prove unconditionally that the average rank of all elliptic curves, when ordered by their heights, is finite. In fact, we prove the same for the 2-Selmer rank. Recall that the 2-Selmer group $S_2(E)$ of an elliptic curve E over \mathbb{Q} fits into an exact sequence

$$0 \rightarrow E(\mathbb{Q})/2E(\mathbb{Q}) \rightarrow S_2(E) \rightarrow \text{III}_E[2] \rightarrow 0, \quad (1)$$

where $\text{III}_E[2]$ denotes the 2-torsion subgroup of the Tate-Shafarevich group III_E of E . The 2-Selmer group is an elementary abelian 2-group of order 2^s for some integer $s \geq 0$, and the quantity s is called the 2-Selmer rank of E . Thus the 2-Selmer rank of E gives an upper bound for the rank of E .

Our main theorem on the 2-Selmer group is as follows:

Theorem 1.1 *When all elliptic curves E/\mathbb{Q} are ordered by height, the average size of the 2-Selmer group $S_2(E)$ is 3.*

We immediately conclude that:

Corollary 1.2 *When all elliptic curves over \mathbb{Q} are ordered by height, their average 2-Selmer rank is at most 1.5; thus their average rank is also at most 1.5.*

Indeed, note that Equation (1) implies that

$$r_2(S_2(E)) = r(E) + r_2(E(\mathbb{Q})[2]) + r_2(\text{III}_E[2]), \quad (2)$$

where we have used $r(E)$ to denote the rank of E and $r_2(G)$ (for an elementary abelian 2-group G) to denote $\dim_{\mathbb{F}_2}(G)$. Due to the inequality $2r_2(S_2(E)) \leq 2^{r_2(S_2(E))} = |S_2(E)|$, Theorem 1.1 bounds the mean of the left hand side of (2) by 1.5, and thus the same bound holds also for the average size of each of the terms on the right hand side of (2). In particular, the average size of $r_2(\text{III}_E[2])$ is also at most 1.5. Meanwhile, it is elementary that the mean size of $r_2(E(\mathbb{Q})[2])$ is 0, i.e., 0% of elliptic curves possess rational 2-torsion.

We will in fact prove a stronger version of Theorem 1.1, namely:

Theorem 1.3 *When elliptic curves $E : y^2 = x^3 + Ax + B$, in any family defined by finitely many congruence conditions on the coefficients A and B , are ordered by height, the average size of the 2-Selmer group $S_2(E)$ is 3.*

Thus the average size of the 2-Selmer group remains 3 even when one averages over any subset of elliptic curves defined by finitely many congruence conditions. We will actually prove Theorem 1.3 for an even larger class of families, including some that are defined by certain natural *infinite* sets of congruence conditions.

We note that the boundedness of the average rank of elliptic curves has been known previously in certain special one-parameter families of elliptic curves. For example, in [26], Fouvry shows that the average rank is bounded in the family of cubic twists $y^2 = x^3 + k$ as k varies. In [29], Heath-Brown shows that the average rank is bounded for the family of “congruent number curves” $y^2 = x^3 - d^2x$ as d varies, and in fact he determines the exact distribution of 2-Selmer ranks, which implies that the average size of the 2-Selmer group in this family is 3. In more recent work, Swinnerton-Dyer [42] and Kane [31] have proven that the same distributions hold for any family of quadratic twists of a single curve with full rational 2-torsion. Our Theorem 1.1 shows that, as far as 2-Selmer ranks are concerned, general elliptic curves seem to behave, on average, in a manner similar to curves in a family of twists.

In the function field case, the boundedness of the average rank of all elliptic curves was proven by de Jong [20], who showed that for a finite field of characteristic not equal to 3, the average size of the 3-Selmer group of all elliptic curves over $\mathbb{F}_q(t)$ is bounded (and is in fact at most $4 + \varepsilon(q)$ for an explicit function $\varepsilon(q)$ that tends to 0 as $q \rightarrow \infty$). Our main result, Theorem 1.1, may be viewed as a precise version of de Jong’s theorem over the number field \mathbb{Q} , with the 3-Selmer group replaced by the 2-Selmer group. We will treat the case of the 3-Selmer group over \mathbb{Q} in a forthcoming article.

Theorems 1.1 and 1.3 also confirm two remarkable sets of heuristics in the literature. In [21], Delaunay used a Cohen–Lenstra-style model to conjecture the distribution of the Tate-Shafarevich group of elliptic curves. Delaunay’s heuristics, coupled with the rank distribution conjecture of Goldfeld and Katz–Sarnak, imply that the average size of the 2-Selmer group is 3. More recently, by a completely different approach, Poonen and Rains [37] model the Selmer group as a random intersection of isotropic subspaces of a quadratic space, and again, they predict that the average size of the 2-Selmer group should be 3. These heuristics thus give an interpretation for the number 3 that appears in Theorems 1.1 and 1.3. For a further interpretation of the number 3 in terms of local masses of 2-coverings of elliptic curves and the Tamagawa number of PGL_2 , see Sections 3.3 and 3.6.

1.2 Counting binary forms having bounded invariants (particularly quartic forms)

We prove the above theorems by developing techniques to count integral orbits, having bounded invariants, in certain coregular representations over \mathbb{Z} . We define a *coregular representation* as a pair (G, V) , where G is an algebraic group and V is a representation of G (for our purposes, both defined over \mathbb{Z}) such that the ring of relative polynomial invariants of $G(\mathbb{C})$ on $V(\mathbb{C})$ is a polynomial ring. Although our techniques are quite

general, in this article we concentrate primarily on the case where $G = \mathrm{GL}_2$ and V is the space of **binary quartic forms** $ax^4 + bx^3y + cx^2y^2 + dx^3y + ey^4$.

The problem of counting integral binary forms having bounded invariants is a classical one. The case of binary quadratic forms was first treated in the influential work *Disquisitiones Arithmeticae* of Gauss in 1801. Gauss studied the action of $\mathrm{SL}_2(\mathbb{Z})$ on the space of integral binary quadratic forms $f(x, y) = ax^2 + bxy + cy^2$ ($a, b, c \in \mathbb{Z}$)¹ via linear substitution of variable, in terms of the unique polynomial invariant for this action, namely the discriminant $\Delta(f) = b^2 - 4ac$. (The polynomial invariant $\Delta(f)$ is “unique” in the sense that the ring of polynomial invariants is generated by one element, namely $\Delta(f)$.)

Gauss conjectured, and Mertens [34] and Siegel [40] proved, respectively, that:

Theorem 1.4 (Mertens 1874/Siegel 1944) *Let h_D denote the number of $\mathrm{SL}_2(\mathbb{Z})$ -equivalence classes of irreducible integral binary quadratic forms having discriminant D . Then:*

$$(a) \quad \sum_{-X < D < 0} h_D \sim \frac{\pi}{18} \cdot X^{3/2};$$

$$(b) \quad \sum_{0 < D < X} h_D \log \varepsilon_D \sim \frac{\pi^2}{18} \cdot X^{3/2};$$

here $\varepsilon_D = (t + u\sqrt{D})/2$, where t, u are the smallest positive integral solutions of $t^2 - Du^2 = 4$.

Note that h_D and $\log \varepsilon_D$ have important algebraic number theoretic interpretations, namely, $h(D)$ is the (narrow) class number and $\log \varepsilon_D$ is the regulator of the unique quadratic order of discriminant D . Thus Theorem 1.4(a) gives the average size of the class number of imaginary quadratic orders up to a given absolute discriminant, while (b) gives the average size of the class number times the regulator of real quadratic orders up to a given discriminant.

The next natural case to consider is that of integral binary cubic forms $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ ($a, b, c, d \in \mathbb{Z}$). The group $\mathrm{GL}_2(\mathbb{Z})$ (or $\mathrm{SL}_2(\mathbb{Z})$) again naturally acts on such forms, and there is again a unique polynomial invariant for this action, namely, the discriminant

$$\Delta(f) = b^2c^2 + 18abcd - 4ac^3 - 4b^3d - 27a^2d^2.$$

The question, as in the case of binary quadratic forms, is: how many classes $h(D)$ of irreducible binary cubic forms are there with discriminant D , on average, as D varies?

This question was first answered by Davenport [18]:

Theorem 1.5 (Davenport 1951) *Let $h(D)$ denote the number of $\mathrm{GL}_2(\mathbb{Z})$ -equivalence classes of irreducible integral binary cubic forms having discriminant D . Then:*

$$(a) \quad \sum_{-X < D < 0} h(D) \sim \frac{\pi^2}{24} \cdot X;$$

$$(b) \quad \sum_{0 < D < X} h(D) \sim \frac{\pi^2}{72} \cdot X.$$

Davenport’s theorem thus states that the number of equivalence classes of irreducible binary cubic forms per discriminant is a constant on average. This too has an important algebraic number theoretic interpretation. Since equivalence classes of irreducible integral binary cubic forms are in bijection with orders in cubic fields (see Delone–Faddeev’s work [23]), Theorem 1.5 states that there are a constant number of (isomorphism classes) of cubic orders per discriminant, on average. Davenport’s theorem was an essential ingredient in the classical work of Davenport and Heilbronn on the density of discriminants of cubic fields (see [19]).

¹Gauss actually considered only forms where b is even; however, from the modern point of view, it is natural to allow all three coefficients a, b, c to be arbitrary integers.

The next natural case to consider is that of binary quartic forms. The group $\mathrm{GL}_2(\mathbb{Z})$ again acts on the space of binary quartic forms $f(x, y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ ($a, b, c, d, e \in \mathbb{Z}$) by linear substitution of variable. Note that in each of the cases of binary quadratic and binary cubic forms, the ring of invariants was generated by one element. Binary quartic forms historically have been more difficult to treat because the ring of invariants is now generated by two independent invariants, traditionally denoted I and J . For $f(x, y)$ as above, we have the following explicit formulae for these invariants:

$$\begin{aligned} I(f) &= 12ae - 3bd + c^2, \\ J(f) &= 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3. \end{aligned}$$

Any other polynomial invariant for the action of $\mathrm{GL}_2(\mathbb{Z})$ on binary quartic forms can be expressed as a polynomial in these invariants; for example, the discriminant $\Delta(f)$ of a binary quartic form can be expressed in terms of $I(f)$ and $J(f)$ as follows:

$$\Delta(f) := \Delta(I(f), J(f)) := (4I(f)^3 - J(f)^2)/27.$$

It follows from work of Borel and Harish-Chandra [10, Theorem 6.9] that the number of equivalence classes of integral binary quartic forms, having any given fixed values of I and J (so long as I and J are not both equal to zero), is finite.² This raises the question as to how many classes $h(I, J)$ of irreducible binary quartic forms with invariants I, J are there, on average, as the pair (I, J) varies?

To answer this question, we require just a bit of notation. Let us define the (naive) *height* of $f(x, y)$ by $H(f) := H(I, J) := \max\{|I^3|, J^2/4\}$ (the constant $1/4$ on J^2 is present for convenience, and is not of any real importance). Thus $H(f)$ is a “degree 6” function on the coefficients of f , in the sense that $H(rf) = r^6 H(f)$ for any constant r . We prove:

Theorem 1.6 *Let $h^{(i)}(I, J)$ denote the number of $\mathrm{GL}_2(\mathbb{Z})$ -equivalence classes of irreducible binary quartic forms having $4 - 2i$ real roots in \mathbb{P}^1 and invariants equal to I and J . Then:*

$$\begin{aligned} \text{(a)} \quad \sum_{H(I, J) < X} h^{(0)}(I, J) &= \frac{4}{135} \zeta(2) X^{5/6} + O(X^{3/4+\epsilon}); \\ \text{(b)} \quad \sum_{H(I, J) < X} h^{(1)}(I, J) &= \frac{32}{135} \zeta(2) X^{5/6} + O(X^{3/4+\epsilon}); \\ \text{(c)} \quad \sum_{H(I, J) < X} h^{(2)}(I, J) &= \frac{8}{135} \zeta(2) X^{5/6} + O(X^{3/4+\epsilon}). \end{aligned}$$

In order to obtain the average size of $h^{(i)}(I, J)$, as (I, J) varies, we first wish to know which pairs (I, J) can actually occur as the invariants of an integral binary quartic form. In the quadratic and cubic cases, this is easy and well-known: a number occurs as the discriminant of a binary quadratic (resp. cubic) form if and only if it is congruent to 0 or 1 (mod 4).

In the binary quartic case, we prove that a similar scenario occurs, namely, an (I, J) is *eligible*—i.e., it occurs as the invariants of some integral binary quartic form—if and only if it satisfies any one of a certain specified finite set of congruence conditions modulo 27. More precisely, we prove:

Theorem 1.7 *A pair $(I, J) \in \mathbb{Z} \times \mathbb{Z}$ occurs as the invariants of an integral binary quartic form if and only if it satisfies one of the following congruence conditions:*

- (a) $I \equiv 0 \pmod{3}$ and $J \equiv 0 \pmod{27}$,
- (b) $I \equiv 1 \pmod{9}$ and $J \equiv \pm 2 \pmod{27}$,

²It is also true that the number of equivalence classes of binary quartic forms having a fixed nonzero value of the single invariant $\Delta(f) = \frac{1}{27}(4I(f)^3 - J(f)^2)$ is finite, since the set of integral points on the elliptic curve $4x^3 - y^2 = 27d$ is finite for each $d \neq 0$. However, the latter fact will not be used here.

- (c) $I \equiv 4 \pmod{9}$ and $J \equiv \pm 16 \pmod{27}$,
- (d) $I \equiv 7 \pmod{9}$ and $J \equiv \pm 7 \pmod{27}$.

It follows that the number of eligible (I, J) , with $H(I, J) < X$, is a constant times $X^{5/6}$; thus, by Theorem 1.6, the number of classes of binary quartic forms per eligible (I, J) is a finite constant on average. We have the following theorem:

Theorem 1.8 *Let $h^{(i)}(I, J)$ denote the number of $\mathrm{GL}_2(\mathbb{Z})$ -equivalence classes of irreducible binary quartic forms having $4 - 2i$ real roots and invariants equal to I and J . Let $n_0 = 4$, $n_1 = 2$, and $n_2 = 2$. Then, for $i = 0, 1, 2$, we have:*

$$\lim_{X \rightarrow \infty} \frac{\sum_{\substack{H(I, J) < X \\ (I, J) \text{ eligible} \\ (-1)^i \Delta(I, J) > 0}} h^{(i)}(I, J)}{\sum_{\substack{H(I, J) < X \\ (I, J) \text{ eligible} \\ (-1)^i \Delta(I, J) > 0}} 1} = \frac{2\zeta(2)}{n_i}.$$

Thus, Theorem 1.8 says that the number of equivalence classes of binary quartic forms per eligible (I, J) , having a given number of real roots, is a constant on average. This constant is either $\zeta(2)/2$ or $\zeta(2)$, depending on whether the given number of real roots is 4 or less than 4, respectively.

We in fact prove a strengthening of Theorem 1.6; namely, we obtain the asymptotic count of binary quartic forms, having bounded invariants, satisfying any specified finite set of congruence conditions. Such a modification will be crucial for the applications to elliptic curves, which we discuss next.

1.3 Binary quartic forms and 2-Selmer groups of elliptic curves

To use the latter counting results involving binary quartic forms to understand the average size of 2-Selmer groups of elliptic curves (as in Theorem 1.1), we recall that an element of the 2-Selmer group of an elliptic curve E/\mathbb{Q} may be thought of as a “locally soluble 2-covering”. A 2-covering of E/\mathbb{Q} is a genus one curve C/\mathbb{Q} together with maps $\phi : C \rightarrow E$ and $\theta : C \rightarrow E$, where ϕ is an isomorphism defined over \mathbb{C} , and θ is a degree 4 map defined over \mathbb{Q} , such that the following diagram commutes:

$$\begin{array}{ccc} E & \xrightarrow{[2]} & E \\ \uparrow \phi & \nearrow \theta & \\ C & & \end{array}$$

Thus a 2-covering $C = (C, \phi, \theta)$ may be viewed as a “twist over \mathbb{Q} of the multiplication-by-2 map on E ”. Two 2-coverings C and C' are said to be *isomorphic* if there exists an isomorphism $\Phi : C \rightarrow C'$ defined over \mathbb{Q} , and a 2-torsion point $P \in E$, such that the following diagram commutes:

$$\begin{array}{ccc} E & \xrightarrow{+P} & E \\ \uparrow \phi & & \uparrow \phi' \\ C & \xrightarrow{\Phi} & C' \end{array}$$

A *soluble 2-covering* C is one that possesses a rational point, while a *locally soluble 2-covering* C is one that possesses an \mathbb{R} -point and a \mathbb{Q}_p -point for all primes p . Then we have natural bijections

$$\begin{aligned} \{\text{soluble 2-coverings}\} / \sim &\longleftrightarrow E(\mathbb{Q})/2E(\mathbb{Q}); \\ \{\text{locally soluble 2-coverings}\} / \sim &\longleftrightarrow S_2(E), \end{aligned}$$

giving each set on the left too the structure of a finite abelian 2-group.

How does counting elements of $S_2(E)$ lead to counting binary quartic forms? There is a result of Birch and Swinnerton-Dyer (see [9, Lemma 2]) that states that any locally soluble 2-covering C possesses a canonically associated degree 2 divisor defined over \mathbb{Q} , thus yielding a double cover $C \rightarrow \mathbb{P}^1$ ramified at 4 points. We thus obtain a binary quartic form over \mathbb{Q} , well-defined up to $\mathrm{GL}_2(\mathbb{Q})$ -equivalence! This connection between 2-Selmer group elements and binary quartic forms was first introduced and used in the original elliptic curve computations of Birch and Swinnerton-Dyer, which led them to their celebrated conjecture. Indeed, this interpretation of binary quartic forms in terms of 2-Selmer groups is still one of the fastest ways of computing and enumerating ranks of elliptic curves in practice, as in, e.g., Cremona's influential `mrank` program.

We use this connection and the above counting results on binary quartic forms to prove Theorems 1.1 and 1.3, as follows:

- Given $A, B \in \mathbb{Z}$, construct an *integral* binary quartic form f for each element of $S_2(E_{A,B})$ such that
 - $y^2 = f(x)$ gives the desired 2-covering;
 - the invariants $(I(f), J(f))$ of f agree with the invariants (A, B) of the elliptic curve (at least up to bounded powers of 2 and 3);
- Count these integral binary quartic forms via congruence versions of Theorem 1.6. The relevant binary quartic forms are actually defined by infinitely many congruence conditions, so a sieve has to be performed.
- A uniformity estimate, which shows that the error term does not grow too large as more and more of the relevant congruence conditions are imposed, must be proven to perform this sieve. This is perhaps the most technical ingredient in this work. It is accomplished by embedding the space of binary quartic forms into a certain larger space—namely, the space of pairs of ternary quadratic forms—where such uniformity estimates are more amenable and have been studied previously in the context of counting quartic fields [4].

This paper is organized as follows. In Section 2, we study the distribution of $\mathrm{GL}_2(\mathbb{Z})$ -equivalence classes of binary quartic forms with respect to their fundamental invariants I and J ; in particular, we prove Theorems 1.6–1.8. We also prove the uniformity estimates that are necessary to count binary quartic forms satisfying our desired infinite sets of congruence conditions.

In Section 3, we describe the precise connection between binary quartic forms and elements in the 2-Selmer groups of elliptic curves. This connection allows us, through the use of certain mass formulae for elliptic curves over \mathbb{Q}_p , to compute the average size of the 2-Selmer groups of elliptic curves (or of appropriate families of elliptic curves) via a count of binary quartic forms satisfying a certain weighted infinite set of congruence conditions. We then apply the uniformity results of Section 2 to count these binary quartic forms, thus completing the proofs of Theorems 1.1 and 1.3.

2 The number of classes of integral binary quartic forms having bounded invariants

Let $V_{\mathbb{R}}$ denote the vector space of binary quartic forms over the real numbers \mathbb{R} . We express an element $f \in V_{\mathbb{R}}$ in the form $f(x, y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$, where a, b, c, d , and e are real numbers. Such an $f \in V_{\mathbb{R}}$ is said to be *integral* if $a, b, c, d, e \in \mathbb{Z}$.

In this section, we derive asymptotics for the number of $\mathrm{GL}_2(\mathbb{Z})$ -equivalence classes of irreducible integral binary quartic forms having bounded invariants. We also describe how these asymptotics change when we restrict to counting those binary quartic forms satisfying certain specified sets of congruence conditions. In particular, we prove Theorems 1.6–1.8.

The group $\mathrm{GL}_2(\mathbb{R})$ naturally acts on $V_{\mathbb{R}}$; namely, an element $\gamma \in \mathrm{GL}_2(\mathbb{R})$ acts on $f(x, y)$ by linear substitution of variable:

$$\gamma \cdot f(x, y) = f((x, y) \cdot \gamma). \quad (3)$$

This action of $\mathrm{GL}_2(\mathbb{R})$ on $V_{\mathbb{R}}$ is a left action, i.e., $(\gamma_1 \gamma_2) \cdot f = \gamma_1 \cdot (\gamma_2 \cdot f)$.

We also consider the action of $\mathrm{SL}_2^{\pm}(\mathbb{R})$ on $V_{\mathbb{R}}$, where $\mathrm{SL}_2^{\pm}(\mathbb{R}) \subset \mathrm{GL}_2(\mathbb{R})$ is the subgroup of elements in $\mathrm{GL}_2(\mathbb{R})$ having determinant equal to ± 1 . The ring of invariants for this action is generated by two independent generators of degrees 2 and 3 which are traditionally denoted by I and J , respectively. If $f(x, y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$, then

$$\begin{aligned} I(f) &= 12ae - 3bd + c^2, \\ J(f) &= 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3. \end{aligned} \quad (4)$$

The quantities $I(f)$ and $J(f)$ are also *relative invariants* for the action of $\mathrm{GL}_2(\mathbb{R})$ on $V_{\mathbb{R}}$: we have

$$\begin{aligned} I(\gamma \cdot f) &= (\det \gamma)^4 I(f), \\ J(\gamma \cdot f) &= (\det \gamma)^6 J(f). \end{aligned} \quad (5)$$

The discriminant $\Delta(f)$ of a binary quartic form f , being a relative invariant of degree 6, can thus be expressed in terms of I and J , namely, $\Delta(f) = (4I(f)^3 - J(f)^2)/27$. We define the *height* $H(f)$ of a binary quartic form f by

$$H(f) := H(I, J) = \max\{|I|^3, J^2/4\}. \quad (6)$$

The action of $\mathrm{GL}_2(\mathbb{Z})$ on $V_{\mathbb{R}}$ evidently preserves the lattice $V_{\mathbb{Z}}$ consisting of the integral elements of $V_{\mathbb{R}}$, and so we may ask: how many $\mathrm{GL}_2(\mathbb{Z})$ -classes of forms are there having height at most X ? More precisely, we may ask: how many $\mathrm{GL}_2(\mathbb{Z})$ -classes of forms are there with height at most X and a given number of real roots?

To this end, for $i = 0, 1$, and 2 , let $V_{\mathbb{Z}}^{(i)}$ denote the set of elements in $V_{\mathbb{Z}}$ having nonzero discriminant and i pairs of complex conjugate roots and $4 - 2i$ real roots in $\mathbb{P}_{\mathbb{C}}^1$. For any $\mathrm{GL}_2(\mathbb{Z})$ -invariant set $S \subset V_{\mathbb{Z}}$, let $N(S; X)$ denote the number of $\mathrm{GL}_2(\mathbb{Z})$ -equivalence classes of irreducible elements $f \in S$ satisfying $H(f) < X$. Then the main theorem of this section is the following restatement of Theorem 1.6:

Theorem 2.1 *We have*

- (a) $N(V_{\mathbb{Z}}^{(0)}; X) = \frac{4}{135}\zeta(2)X^{5/6} + O(X^{3/4+\epsilon});$
- (b) $N(V_{\mathbb{Z}}^{(1)}; X) = \frac{32}{135}\zeta(2)X^{5/6} + O(X^{3/4+\epsilon});$
- (c) $N(V_{\mathbb{Z}}^{(2)}; X) = \frac{8}{135}\zeta(2)X^{5/6} + O(X^{3/4+\epsilon}).$

Our strategy to prove Theorem 2.1 is as follows. In §2.1, we develop the necessary reduction theory needed to establish convenient fundamental domains for the action of $\mathrm{GL}_2(\mathbb{Z})$ on $V_{\mathbb{R}}$. The primary difficulty in counting points in these fundamental domains is that they are not bounded, but instead have a rather complicated cuspidal region going off to infinity. To deal with and effectively handle this cusp, in §2.2 we investigate the distribution of reducible and irreducible points inside these fundamental domains. Specifically, we prove that the cusp contains only reducible points, while the remainder of the domain outside the cuspidal region contains primarily irreducible points. In §2.3, we develop a refinement of an averaging method introduced in [4], [5] to count points in these fundamental regions in terms of the volumes of these domains. The volumes of the fundamental regions are then computed in §2.4, completing the proof of Theorem 2.1.

In §2.5, we prove a stronger version of Theorem 2.1 where we restrict to counting those binary quartic forms whose coefficients satisfy finitely many congruence conditions. In §2.6, we prove the necessary estimates that uniformly bound the number of $\mathrm{GL}_2(\mathbb{Z})$ -orbits on binary quartic forms having bounded height whose discriminants are divisible by the square of some large prime. In §2.7, we then describe how these uniformity estimates allow one to count the number of $\mathrm{GL}_2(\mathbb{Z})$ -orbits of binary quartic forms of bounded height having squarefree discriminant (or satisfying other similar sets of infinitely many congruence conditions). We will require such results when we prove Theorems 1.1 and 1.3 in Section 3.

2.1 Reduction theory

For $i = 0, 1$, and 2 , let $V_{\mathbb{R}}^{(i)}$ denote the set of points in $V_{\mathbb{R}}$ having nonzero discriminant and i pairs of complex roots and $4 - 2i$ real roots in $\mathbb{P}_{\mathbb{C}}^1$. Then $V_{\mathbb{R}}^{(2)}$ is the set of *definite* forms in $V_{\mathbb{R}}$, i.e., forms $f(x, y)$ that take only positive or only negative values when evaluated at nonzero vectors $(x_0, y_0) \in \mathbb{R}^2$. Let $V_{\mathbb{R}}^{(2+)}$ (resp. $V_{\mathbb{R}}^{(2-)}$) denote the subset of $V_{\mathbb{R}}^{(2)}$ consisting of the *positive definite forms* (resp. *negative definite forms*). Note that for $i = 0, 1$, and 2 we have $V_{\mathbb{Z}}^{(i)} = V_{\mathbb{R}}^{(i)} \cap V_{\mathbb{Z}}$. We analogously define $V_{\mathbb{Z}}^{(i)} = V_{\mathbb{R}}^{(i)} \cap V_{\mathbb{Z}}$ for $i = 2+$ and $2-$.

We then have the following facts (see [14, Remark 2]):

1. The set of binary quartic forms in $V_{\mathbb{R}}$ having fixed invariants I and J consists of just one $\mathrm{SL}_2^{\pm}(\mathbb{R})$ -orbit if $4I^3 - J^2 < 0$; this orbit lies in $V_{\mathbb{R}}^{(1)}$.
2. The set of binary quartic forms in $V_{\mathbb{R}}$ having fixed invariants I and J consists of three $\mathrm{SL}_2^{\pm}(\mathbb{R})$ -orbits if $4I^3 - J^2 > 0$; in that case, there is one such orbit from each of $V_{\mathbb{R}}^{(0)}$, $V_{\mathbb{R}}^{(2+)}$, and $V_{\mathbb{R}}^{(2-)}$.

Since $I(g \cdot f) = (\det g)^4 I(f)$ and $J(g \cdot f) = (\det g)^6 J(f)$, it follows that two forms $f_1, f_2 \in V_{\mathbb{R}}^{(i)}$ are $\mathrm{GL}_2(\mathbb{R})$ -equivalent if and only if there exists a positive constant $\lambda \in \mathbb{R}$ with $I(f_1) = \lambda^2 I(f_2)$ and $J(f_1) = \lambda^3 J(f_2)$. Given a pair $(I, J) \neq (0, 0)$, there always exists a positive constant λ such that $H(\lambda^2 I, \lambda^3 J) = 1$. Therefore, for $i = 0, 2+$, or $2-$ (resp. for $i = 1$), a fundamental set $L^{(i)}$ for the action of $\mathrm{GL}_2(\mathbb{R})$ on $V_{\mathbb{R}}^{(i)}$ can be constructed by choosing one form $f \in V_{\mathbb{R}}^{(i)}$, having invariants I and J , for each (I, J) such that $H(I, J) = 1$ and $4I^3 - J^2 > 0$ (resp. $4I^3 - J^2 < 0$). Table 1 provides explicit constructions of such fundamental sets $L^{(i)}$.

$$\begin{aligned}
 L^{(0)} &= \left\{ x^3 y - \frac{1}{3} x y^3 - \frac{J}{27} y^4 : -2 < J < 2 \right\} \\
 L^{(1)} &= \left\{ x^3 y - \frac{I}{3} x y^3 + \frac{\pm 2}{27} y^4 : -1 \leq I < 1 \right\} \cup \left\{ x^3 y + \frac{1}{3} x y^3 - \frac{J}{27} y^4 : -2 < J < 2 \right\} \\
 L^{(2+)} &= \left\{ \frac{1}{16} x^4 - \frac{\sqrt{2-J}}{3\sqrt{3}} x^3 y + \frac{1}{2} x^2 y^2 + y^4 : -2 < J < 2 \right\} \\
 L^{(2-)} &= \{ f : -f \in L^{2+} \}
 \end{aligned}$$

Table 1: Explicit constructions of fundamental sets $L^{(i)}$ for $\mathrm{GL}_2(\mathbb{R}) \backslash V_{\mathbb{R}}^{(i)}$

The key fact that we use about these chosen fundamental sets $L^{(i)}$ is that the coefficients of all the binary quartic forms in these $L^{(i)}$ are bounded; i.e., the $L^{(i)}$ all lie in a bounded subset of $V_{\mathbb{R}}$. It follows that, for any h lying in a fixed compact subset $G_0 \subset \mathrm{GL}_2(\mathbb{R})$, the set $h \cdot L^{(i)}$ is also a fundamental set for the action of $\mathrm{GL}_2(\mathbb{R})$ on $V_{\mathbb{R}}^{(i)}$, and all coefficients are then bounded independent of h .

We will have need for the following lemma, whose proof is postponed to §2.8:

Lemma 2.2 *Let f be an element in $V_{\mathbb{R}}^{(i)}$ having nonzero discriminant. Then the order of the stabilizer of f in $\mathrm{GL}_2(\mathbb{R})$ is 8 if $i = 0$ or 2 , and 4 if $i = 1$.*

Let \mathcal{F} denote Gauss's usual fundamental domain for $\mathrm{GL}_2(\mathbb{Z}) \backslash \mathrm{GL}_2(\mathbb{R})$ in $\mathrm{GL}_2(\mathbb{R})$. It follows from [39, Ch. 7, Th. 1] that \mathcal{F} may be expressed in the form $\mathcal{F} = \{ n \alpha k \lambda : n(u) \in N'(t), \alpha(t) \in A', k \in K, \lambda \in \Lambda \}$, where

$$N'(t) = \left\{ \begin{pmatrix} 1 & \\ u & 1 \end{pmatrix} : u \in \nu(t) \right\}, \quad A' = \left\{ \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} : t \geq \sqrt[4]{3}/\sqrt{2} \right\}, \quad \Lambda = \left\{ \begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix} : \lambda > 0 \right\}, \quad (7)$$

and K is as usual the (compact) real orthogonal group $\mathrm{SO}_2(\mathbb{R})$; here $\nu(t)$ is a union of one or two subintervals of $[-\frac{1}{2}, \frac{1}{2}]$ depending only on the value of t .

For $i = 0, 1, 2+,$ and $2-,$ let $2n_i$ denote the cardinality of the stabilizer in $\mathrm{GL}_2(\mathbb{R})$ of an irreducible element $v \in V_{\mathbb{R}}^{(i)}$. Then, by Lemma 2.2, we have $n_0 = 4, n_1 = 2, n_{2+} = 4,$ and $n_{2-} = 4$. For $h \in \mathrm{GL}_2(\mathbb{R}),$ we regard $\mathcal{F}h \cdot L^{(i)}$ as a multiset, where the multiplicity of a point x in $\mathcal{F}h \cdot L^{(i)}$ is given by the cardinality of the set $\{g \in \mathcal{F} : x \in gh \cdot L^{(i)}\}$. We claim that the $\mathrm{GL}_2(\mathbb{Z})$ -equivalence class of x in $V_{\mathbb{R}}^{(i)}$ is represented $m(x) := \#\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{R})}(x)/\#\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(x)$ times in the multiset $\mathcal{F}h \cdot L^{(i)}$; i.e., the multiplicity of x' in $\mathcal{F}h \cdot L^{(i)},$ summed over all $x' \in V_{\mathbb{Z}}$ that are $\mathrm{GL}_2(\mathbb{Z})$ -equivalent to $x,$ is equal to $m(x)$. Indeed, for any element $x \in V_{\mathbb{R}}^{(i)},$ there exists a unique element $x_L \in h \cdot L^{(i)}$ that is $\mathrm{GL}_2(\mathbb{R})$ -equivalent to x . Suppose $g \in \mathrm{GL}_2(\mathbb{R})$ satisfies $g \cdot x_L = x$. Then for an element $g' \in \mathrm{GL}_2(\mathbb{R}),$ the element $g' \cdot x_L \in V_{\mathbb{Z}}$ is $\mathrm{GL}_2(\mathbb{Z})$ -equivalent to x if and only if $g' = \gamma g g_0$ for some $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ and $g_0 \in \mathrm{Stab}_{\mathrm{GL}_2(\mathbb{R})}(x_L),$ i.e., if and only if g and g' map to the same element in the double coset space

$$\mathrm{GL}_2(\mathbb{Z}) \backslash \mathrm{GL}_2(\mathbb{R}) / \mathrm{Stab}_{\mathrm{GL}_2(\mathbb{R})}(x_L).$$

The number of such double cosets in the single right coset $\mathrm{GL}_2(\mathbb{Z})g$ is equal to

$$\frac{\#[g\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{R})}(x_L)g^{-1}]}{\#[\mathrm{GL}_2(\mathbb{Z}) \cap g\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{R})}(x_L)g^{-1}]} = \frac{\#\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{R})}(x)}{\#\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(x)} = m(x) \quad (8)$$

as desired.

Since the stabilizer in $\mathrm{GL}_2(\mathbb{Z})$ of an element $x \in V_{\mathbb{R}}$ always contains the identity and its negative, $m(x)$ is always a number between 1 and n_i . In fact, for almost all $x \in V_{\mathbb{R}}^{(i)},$ the quantity $m(x)$ is equal to n_i . Indeed, for any fixed $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ not equal to plus or minus the identity, the set of elements in $V_{\mathbb{R}}$ that are fixed by γ has measure 0. Since $\mathrm{GL}_2(\mathbb{Z})$ is countable, it follows that the set of elements $x \in V_{\mathbb{R}}^{(i)}$ such that $m(x) < n_i$ also has measure 0. Thus for any $h \in \mathrm{GL}_2(\mathbb{R}),$ away from a measure zero set, the multiset $\mathcal{F}h \cdot L^{(i)}$ is the union of n_i fundamental domains for the action of $\mathrm{GL}_2(\mathbb{Z})$ on $V_{\mathbb{R}}^{(i)}$.

Therefore, for any $h \in \mathrm{GL}_2(\mathbb{R}),$ if we let $\mathcal{R}_X(h \cdot L^{(i)})$ denote the multiset $\{w \in \mathcal{F}h \cdot L^{(i)} : |H(w)| < X\},$ then the product $n_i N(V_{\mathbb{Z}}^{(i)}; X)$ is equal to the number of irreducible integral points in $\mathcal{R}_X(h \cdot L^{(i)}),$ with the slight caveat that the (relatively rare—see Lemma 2.4) points with $\mathrm{GL}_2(\mathbb{Z})$ -stabilizers of cardinality $2r$ ($r > 1$) are counted with weight $1/r$.

As mentioned earlier, the main obstacle to counting integral points in this region $\mathcal{R}_X(h \cdot L^{(i)})$ is that it is not bounded, but rather has a cusp going off to infinity (namely, the part of $\mathcal{R}_X(h \cdot L^{(i)})$ where the first coordinate a becomes small in absolute value, or equivalently, where the parameter t in (7) becomes large). We simplify the counting in this cuspidal region by “thickening” the cusp; more precisely, we compute the number of integral points in the region $\mathcal{R}_X(h \cdot L^{(i)})$ by averaging over a “compact continuum” of such fundamental regions, i.e., by averaging over the domains $\mathcal{R}_X(h \cdot L^{(i)})$ where h ranges over a certain compact subset $G_0 \subset \mathrm{GL}_2(\mathbb{R}).$ This refinement of the method of [5] is described in more detail in §2.3.

However, we first turn in §2.2 to bounding the number of reducible points in the main bodies (i.e., away from the cusps) of our fundamental regions.

2.2 Estimates on reducibility

We consider the integral elements in the multiset $\mathcal{R}_X(h \cdot L^{(i)}) := \{w \in \mathcal{F}h \cdot L^{(i)} : |H(w)| < X\}$ that are reducible over $\mathbb{Q},$ where h is any element in a fixed compact subset G_0 of $\mathrm{GL}_2(\mathbb{R}).$ Note that if a binary quartic form $ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ satisfies $a = 0$ (so that, in particular, it lies in the cusp of the region $\mathcal{R}_X(h \cdot L^{(i)}),$ then it is automatically reducible over $\mathbb{Q},$ since y is a factor. The following lemma shows that for integral binary quartic forms in $\mathcal{R}_X(h \cdot L^{(i)}),$ reducibility with $a \neq 0$ does not occur very often (i.e., there are a negligible number of reducible points in the main body of the fundamental domain):

Lemma 2.3 *Let $h \in G_0$ be any element, where G_0 is any fixed compact subset of $\mathrm{GL}_2(\mathbb{R}).$ Then the number of integral binary quartic forms $ax^4 + bx^3y + cy^2 + dxy^3 + ey^4 \in \mathcal{R}_X(h \cdot L^{(i)})$ that are reducible over \mathbb{Q} with $a \neq 0$ is $O(X^{2/3+\epsilon}),$ where the implied constant depends only on G_0 and $\epsilon.$*

Proof: Let $f(x, y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ be any element in $\mathcal{R}_X(h \cdot L^{(i)})$. We know that $\mathcal{R}_X(h \cdot L^{(i)}) \subset N'A'K\Lambda h \cdot L^{(i)}$, where $h \cdot L^{(i)}$ lies in a fixed compact set and $0 < \lambda < X^{1/24}$. Since all the coefficients of all the elements in $K\Lambda h \cdot L^{(i)}$ are bounded by $O((X^{1/24})^4) = O(X^{1/6})$, it follows that in $N'A'K\Lambda h \cdot L^{(i)}$, we still have $a = O(X^{1/6})$, $b = O(X^{1/6})$, $c = O(X^{1/6})$, $ad = O(X^{2/6})$, $bd = O(X^{2/6})$, and $ae = O(X^{2/6})$. In particular, the latter estimates clearly imply that the number of points in $\mathcal{R}_X(h \cdot L^{(i)})$ with $a \neq 0$ and $e = 0$ is $O(X^{4/6+\epsilon})$.

Let us now assume that $a \neq 0$ and $e \neq 0$. We first estimate the number of forms that have a rational linear factor. The above estimates show that the number of possibilities for the quadruple (a, b, d, e) is at most $O(X^{4/6+\epsilon})$. If $px + qy$ is a linear factor of $f(x, y)$, where $p, q \in \mathbb{Z}$ are relatively prime, then p must be a factor of a , while q must be a factor of e ; they are thus both determined up to $O(X^\epsilon)$ possibilities. Once p and q are determined, computing $f(-q, p)$ and setting it equal to zero then uniquely determines c (if it is an integer at all) in terms of a, b, d, e, p, q . Thus the total number of forms $f \in \mathcal{R}_X(h \cdot L^{(i)})$ having a rational linear factor and $a \neq 0$ is $O(X^{4/6+\epsilon})$.

We now estimate the number of binary quartic forms in $\mathcal{R}_X(h \cdot L^{(i)})$ that factor into two irreducible binary quadratic forms over \mathbb{Z} , say

$$ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 = (px^2 + qxy + ry^2)\left(\frac{a}{p}x^2 + sxy + \frac{e}{r}y^2\right)$$

where $p, q, r, s \in \mathbb{Z}$ and p, q, r are relatively prime. Since $ae = O(X^{2/6})$ and $a, e \neq 0$, the number of possibilities for the pair (a, e) is $O(X^{2/6+\epsilon})$. We then see that p divides a and r divides e , and hence the number of possibilities for (p, r) , once a and e have been fixed, is bounded by $O(X^\epsilon)$.

Next, equating coefficients, we see that:

$$\begin{aligned} \frac{a}{p}q + ps &= b, \\ \frac{e}{r}q + rs &= d. \end{aligned} \tag{9}$$

We split into two cases. We first consider the case where $\frac{ar}{pe} \neq \frac{p}{r}$, i.e., the linear system (9) in the variables q and s is nonsingular. Then the values of b and d uniquely determine q and s , and so the total number of quadruples (a, b, d, e) —and hence the total number of octuples (a, b, d, e, p, r, q, s) —is at most $O(X^{4/6+\epsilon})$. Furthermore, once this octuple has been fixed, this also then determines c by equating coefficients of x^2y^2 . Hence there are at most $O(X^{4/6+\epsilon})$ possibilities for (a, b, c, d, e) in this case.

Next, we consider the case where $\frac{ar}{pe} = \frac{p}{r}$, so that the system (9) is singular. In this case, the value of b determines the value of d uniquely, namely $d = (r/p)b$. We have already seen that there are $O(X^{2/6+\epsilon})$ possibilities for the quadruple (a, e, p, r) . Since there are only $O(X^{1/6})$ choices for each of b and c , and then d is determined by b , the total number of choices for (a, b, c, d, e) is again $O(X^{4/6+\epsilon})$, as desired. \square

We also have the following lemma which bounds the number of $\mathrm{GL}_2(\mathbb{Z})$ -equivalence classes of integral binary quartic forms having large stabilizers inside $\mathrm{GL}_2(\mathbb{Z})$ (in fact, in $\mathrm{GL}_2(\mathbb{Q})$); we defer the proof to §2.8.

Lemma 2.4 *The number of $\mathrm{GL}_2(\mathbb{Z})$ -orbits of integral binary quartic forms $f \in V_{\mathbb{Z}}$ such that $\Delta(f) \neq 0$ and $H(f) < X$ whose stabilizer in $\mathrm{GL}_2(\mathbb{Q})$ has size greater than 2 is $O(X^{3/4+\epsilon})$.*

2.3 Averaging and cutting off the cusp

Let G_0 be a compact, semialgebraic, left K -invariant set in $\mathrm{GL}_2(\mathbb{R})$ that is the closure of a nonempty open set and in which every element has determinant greater than or equal to 1. Then for $i = 0, 1, 2+$, and $2-$, we may write

$$N(V_{\mathbb{Z}}^{(i)}; X) = \frac{\int_{h \in G_0} \#\{x \in \mathcal{F}h \cdot L \cap V_{\mathbb{Z}}^{\mathrm{irr}} : H(x) < X\} dh}{n_i \int_{h \in G_0} dh}, \tag{10}$$

where $V_{\mathbb{Z}}^{\mathrm{irr}}$ denotes the set of irreducible elements in $V_{\mathbb{Z}}$, the set L is equal to $L^{(i)}$, and dh denotes Haar-measure on $\mathrm{GL}_2(\mathbb{R})$. We normalize dh as follows: if we write $h \in \mathrm{GL}_2(\mathbb{R})$ in its Iwasawa decomposition as

$h = n(u)\alpha(t)k\lambda$, then $dh = t^{-2}du d^\times t dk d^\times \lambda$, where $d^\times t = t^{-1}dt$, $d^\times \lambda = \lambda^{-1}d\lambda$, and $\int_K dk = 1$. Thus, the denominator of the right hand side of (10) is an absolute constant $C_{G_0}^{(i)}$ greater than zero.

More generally, for any $\mathrm{GL}_2(\mathbb{Z})$ -invariant subset $S \subset V_{\mathbb{Z}}^{(i)}$, let $N(S; X)$ denote the number of irreducible $\mathrm{GL}_2(\mathbb{Z})$ -orbits in S having height less than X . Let S^{irr} denote the subset of irreducible points of S . Then $N(S; X)$ can be similarly expressed as

$$N(S; X) = \frac{\int_{h \in G_0} \#\{x \in \mathcal{F}h \cdot L \cap S^{\mathrm{irr}} : H(x) < X\} dh}{C_{G_0}^{(i)}}. \quad (11)$$

We use (11) to define $N(S; X)$ even for sets $S \subset V_{\mathbb{Z}}$ that are not necessarily $\mathrm{GL}_2(\mathbb{Z})$ -invariant.

Now, given $x \in V_{\mathbb{R}}^{(i)}$, let x_L denote the unique point in L that is $\mathrm{GL}_2(\mathbb{R})$ -equivalent to x . We have

$$N(S; X) = \frac{1}{C_{G_0}^{(i)}} \sum_{\substack{x \in S^{\mathrm{irr}} \\ H(x) < X}} \int_{h \in G_0} \#\{g \in \mathcal{F} : x = gh \cdot x_L\} dh. \quad (12)$$

For a given $x \in S^{\mathrm{irr}}$, there exist a finite number of elements $g_1, \dots, g_n \in \mathrm{GL}_2(\mathbb{R})$ satisfying $g_j \cdot x_L = x$. We then have

$$\int_{h \in G_0} \#\{g \in \mathcal{F} : x = gh \cdot x_L\} dh = \sum_j \int_{h \in G_0} \#\{g \in \mathcal{F} : gh = g_j\} dh = \sum_j \int_{h \in G_0 \cap \mathcal{F}^{-1}g_j} dh.$$

As dh is an invariant measure on G , we have

$$\sum_j \int_{h \in G_0 \cap \mathcal{F}^{-1}g_j} dh = \sum_j \int_{g \in G_0 g_j^{-1} \cap \mathcal{F}^{-1}} dg = \sum_j \int_{g \in \mathcal{F}} \#\{h \in G_0 : gh = g_j\} dg = \int_{g \in \mathcal{F}} \#\{h \in G_0 : x = gh \cdot x_L\} dg.$$

Therefore,

$$N(S; X) = \frac{1}{C_{G_0}^{(i)}} \sum_{\substack{x \in S^{\mathrm{irr}} \\ H(x) < X}} \int_{g \in \mathcal{F}} \#\{h \in G_0 : x = gh \cdot x_L\} dg \quad (13)$$

$$= \frac{1}{C_{G_0}^{(i)}} \int_{g \in \mathcal{F}} \#\{x \in S^{\mathrm{irr}} \cap gG_0 \cdot L : H(x) < X\} dg \quad (14)$$

$$= \frac{1}{C_{G_0}^{(i)}} \int_{g \in N'(t)A'\Lambda K} \#\{x \in S^{\mathrm{irr}} \cap n(\begin{smallmatrix} t^{-1} & \\ & t \end{smallmatrix})\lambda k G_0 \cdot L : H(x) < X\} t^{-2} dn d^\times t d^\times \lambda dk. \quad (15)$$

Since $KG_0 = G_0$ and $\int_K dk = 1$, we obtain the following theorem which provides a key formula for $N(S, X)$:

Theorem 2.5 *For any subset $S \subset V_{\mathbb{Z}}^{(i)}$, we have*

$$N(S; X) = \frac{1}{C_{G_0}^{(i)}} \int_{g \in N'(t)A'\Lambda} \#\{x \in S^{\mathrm{irr}} \cap B(n, t, \lambda, X)\} t^{-2} dn d^\times t d^\times \lambda, \quad (16)$$

where $C_{G_0}^{(i)} = n_i \int_{h \in G_0} dh$ and

$$B(n, t, \lambda, X) := n(\begin{smallmatrix} t^{-1} & \\ & t \end{smallmatrix})\lambda G_0 \cdot L \cap \{x \in V_{\mathbb{R}}^{(i)} : H(x) < X\}. \quad (17)$$

To estimate the number of lattice points in the (bounded) region $B(n, t, \lambda, X)$ defined by (17), we have the following proposition due to Davenport [17].

Proposition 2.6 *Let \mathcal{R} be a bounded, semialgebraic multiset in \mathbb{R}^n having maximum multiplicity m , and that is defined by at most k polynomial inequalities each having degree at most ℓ . Then the number of integral lattice points (counted with multiplicity) contained in the region \mathcal{R} is*

$$\text{Vol}(\mathcal{R}) + O(\max\{\text{Vol}(\bar{\mathcal{R}}), 1\}),$$

where $\text{Vol}(\bar{\mathcal{R}})$ denotes the greatest d -dimensional volume of any projection of \mathcal{R} onto a coordinate subspace obtained by equating $n - d$ coordinates to zero, where d takes all values from 1 to $n - 1$. The implied constant in the second summand depends only on n , m , k , and ℓ .

Davenport states the above proposition only for the number of lattice points in compact semialgebraic sets $\mathcal{R} \subset \mathbb{R}^n$. However, his result immediately implies Proposition 2.6 for a general bounded semialgebraic multiset $\mathcal{R} \subset \mathbb{R}^n$, via partitioning the multiset \mathcal{R} into semialgebraic sets having constant multiplicity and then applying the result to the closure and boundary of each such set.

By our construction of the $L^{(i)}$, the coefficients of the binary quartic forms in $G_0 \cdot L$ are all uniformly bounded. Let C be a constant such that C^4 bounds the absolute values of all the coefficients of all the forms in $G_0 \cdot L$. We then have the following lemma on the number of lattice points in $B(n, t, \lambda, X)$ having nonzero leading coefficient:

Proposition 2.7 *The number of lattice points (a, b, c, d, e) in $B(n, t, \lambda, X)$ with $a \neq 0$ is*

$$\begin{cases} 0 & \text{if } C\lambda < t; \\ \text{Vol}(B(n, t, \lambda, X)) + O(t^4 \lambda^{16}) & \text{otherwise.} \end{cases}$$

Proof: If $ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 \in B(n, t, \lambda, X)$ is a binary quartic form, then $|a|$, $|b|$, $|c|$, $|d|$, and $|e|$ are at most $C^4 \lambda^4 / t^4$, $C^4 \lambda^4 / t^2$, $C^4 \lambda^4$, $C^4 \lambda^4 t^2$, and $C^4 \lambda^4 t^4$, respectively. If $C\lambda / t < 1$, then $a = 0$ is the only possibility for such an integral binary quartic form.

Now assume $C\lambda / t \geq 1$. This implies that λ , like t , is bounded below by a positive constant. Then each of the upper limits $C^4 \lambda^4 / t^4$, $C^4 \lambda^4 / t^2$, $C^4 \lambda^4$, $C^4 \lambda^4 t^2$, and $C^4 \lambda^4 t^4$ for $|a|$, $|b|$, $|c|$, $|d|$, and $|e|$, respectively, are also bounded below by a positive constant, and the upper limit for $|a|$ is the smallest of these upper limits up to a bounded constant. Therefore, the k -dimensional volume of any projection of $B(n, t, \lambda, X)$ onto a subspace defined by setting k coefficients equal to 0 (where $1 \leq k \leq 4$) is at most a bounded constant times the product of the last four upper limits, or $O(\lambda^4 / t^2 \cdot \lambda^4 \cdot \lambda^4 t^2 \cdot \lambda^4 t^4) = O(t^4 \lambda^{16})$. The result now follows from Proposition 2.6. \square

In (16), since L (and therefore also $G_0 \cdot L$) contains only points with height at least 1, we observe (by the definition of $B(n, t, \lambda, X)$) that the integrand will be nonzero only if $t \leq C\lambda$ and $\lambda < X^{1/24}$. Thus we may write

$$N(V_{\mathbb{Z}}^{(i)}; X) = \frac{1}{C_{G_0}^{(i)}} \int_{\lambda = \sqrt[4]{3}/(\sqrt{2}C)}^{X^{1/24}} \int_{t = \sqrt[4]{3}/\sqrt{2}}^{C\lambda} \int_{N'(t)} (\text{Vol}(B(n, t, \lambda, X)) + O(t^4 \lambda^{16})) t^{-2} dn d^\times t d^\times \lambda + O(X^{3/4+\epsilon}), \quad (18)$$

where the error term of $O(X^{3/4+\epsilon})$ arises due to the bound on reducible forms in Lemma 2.3 and the bound on forms having nontrivial $\text{GL}_2(\mathbb{Z})$ -stabilizer in Lemma 2.4. The integral of the second summand is immediately evaluated to be $O(X^{3/4})$. Meanwhile, the integral of the first summand is

$$\frac{1}{C_{G_0}^{(i)}} \int_{h \in G_0} \text{Vol}(\mathcal{R}_X(h \cdot L)) dh - \int_{\lambda = \sqrt[4]{3}/(\sqrt{2}C)}^{X^{1/24}} \int_{t = C\lambda}^{\infty} \int_{N'(t)} \text{Vol}(B(n, t, \lambda, X)) t^{-2} dn d^\times t d^\times \lambda. \quad (19)$$

However, $\text{Vol}(\mathcal{R}_X(h \cdot L))$ is independent of h ; also, since $\text{Vol}(B(n, t, \lambda, X)) = O(\lambda^{20})$, by carrying out the integration in the second term of (19), we see that that this term is also $O(X^{3/4})$. In other words, the volume of the cuspidal region, where $t > C\lambda$, is small. We conclude that

$$N(V_{\mathbb{Z}}^{(i)}; X) = \text{Vol}(\mathcal{R}_X(L)) / n_i + O(X^{3/4+\epsilon}). \quad (20)$$

To complete the proof of Theorem 2.1, it thus remains only to compute the volume $\text{Vol}(\mathcal{R}_X(L))$.

2.4 Computation of the volume

Let i be equal to 0, 1, 2+, or 2-. Our aim in this subsection is to compute the volume of $\mathcal{R}_X(L^{(i)}) = \{w \in \mathcal{F}h \cdot L^{(i)} : |H(w)| < X\}$. To this end, let $R^{(i)} := \Lambda \cdot L^{(i)}$. Then for each $(I, J) \in \mathbb{R} \times \mathbb{R}$ with $\Delta(I, J) > 0$, the sets $R^{(0)}$, $R^{(2+)}$, and $R^{(2-)}$ contain exactly one point having invariants I and J ; for each $(I, J) \in \mathbb{R} \times \mathbb{R}$ with $\Delta(I, J) < 0$, the set $R^{(1)}$ contains exactly one point having invariants I and J . Let $R^{(i)}(X)$ denote the set of all those points in $R^{(i)}$ having height less than X . We now consider a twisted action of $\mathrm{GL}_2(\mathbb{R})$ on $V_{\mathbb{R}}$ given by

$$\gamma \cdot f(x, y) := f((x, y) \cdot \gamma) / (\det \gamma)^2 \quad (21)$$

for $\gamma \in \mathrm{GL}_2(\mathbb{R})$ and $f \in V_{\mathbb{R}}$, which induces an action of $\mathrm{PGL}_2(\mathbb{R})$ on $V_{\mathbb{R}}$. Let $\mathcal{F}_{\mathrm{PGL}_2}$ be the image in $\mathrm{PGL}_2(\mathbb{R})$ of the fundamental domain \mathcal{F} for the action of $\mathrm{GL}_2(\mathbb{Z})$ on $\mathrm{GL}_2(\mathbb{R})$. Then $\mathcal{F}_{\mathrm{PGL}_2}$ is a fundamental domain for the action of $\mathrm{PGL}_2(\mathbb{Z})$ on $\mathrm{PGL}_2(\mathbb{R})$ by left multiplication. Furthermore, we have $\mathcal{R}_X(L^{(i)}) = \mathcal{F}_{\mathrm{PGL}_2} \cdot R^{(i)}(X)$.

The set $R^{(i)}$ is in canonical one-to-one correspondence with the set $\{(I, J) \in \mathbb{R} \times \mathbb{R} : I^3 - J^2/4 > 0\}$ if $i = 0, 2+, \text{ or } 2-$, and with $\{(I, J) \in \mathbb{R} \times \mathbb{R} : I^3 - J^2/4 < 0\}$ if $i = 1$. There is thus a natural measure on each of these sets $R^{(i)}$, given by $dr = dI dJ$. Let ω be a differential which generates the rank 1 module of top-degree differentials of PGL_2 over \mathbb{Z} . Then ω is well-defined up to sign. To compute the volume of the multiset $\mathcal{R}_X(L^{(i)}) = \mathcal{F}_{\mathrm{PGL}_2} \cdot R^{(i)}(X)$, we use the following proposition:

Proposition 2.8 *For any measurable function ϕ on $V_{\mathbb{R}}$, we have*

$$\int_{\mathcal{F}_{\mathrm{PGL}_2} \cdot R^{(i)}} \phi(v) dv = \frac{1}{27} \int_{R^{(i)}} \int_{\mathrm{PGL}_2(\mathbb{R})} \phi(g \cdot p_{I,J}^{(i)}) \omega(g) dI dJ, \quad (22)$$

where $p_{I,J}^{(i)} \in R^{(i)}$ is the point having invariants equal to I and J and we regard $\mathcal{F}_{\mathrm{PGL}_2} \cdot R^{(i)}$ as a multiset.

The proposition follows from a Jacobian computation and can be verified directly; for a more noncomputational proof of the above proposition, see Section 3.3.

Proposition 2.8 may now be used to compute the volume of the multiset $\mathcal{R}_X(L^{(i)})$; we have

$$\int_{\mathcal{R}_X(L^{(i)})} dv = \int_{\mathcal{F}_{\mathrm{PGL}_2} \cdot R^{(i)}(X)} dv = \frac{1}{27} \int_{R^{(i)}(X)} \int_{\mathrm{PGL}_2} dg dI dJ = \frac{2\zeta(2)}{27} \int_{R^{(i)}(X)} dI dJ, \quad (23)$$

where the final equality follows from the fact that $\mathrm{Vol}(\mathcal{F}_{\mathrm{PGL}_2}) = \mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z}) \backslash \mathrm{PGL}_2(\mathbb{R})) = 2\zeta(2)$ (see [33]). When $i = 0, 2+, \text{ or } 2-$, we compute $\int_{R^{(i)}(X)} dI dJ$ to be

$$\int_{I=0}^{X^{1/3}} \int_{J=-2I^{3/2}}^{2I^{3/2}} dJ dI = \frac{8}{5} X^{5/6}. \quad (24)$$

Meanwhile, $\int_{R^{(1)}(X)} dI dJ$ is equal to

$$\int_{I=-X^{1/3}}^{X^{1/3}} \int_{J=-2X^{1/2}}^{2X^{1/2}} dJ dI - \mathrm{Vol}(R^{(0)}(X)) = 8X^{5/6} - \frac{8}{5} X^{5/6} = \frac{32}{5} X^{5/6}. \quad (25)$$

We conclude that

$$\mathrm{Vol}(\mathcal{R}_X(L^{(i)})) = \begin{cases} \frac{16}{135} \cdot \zeta(2) X^{5/6} & \text{for } i = 0, 2+, \text{ and } 2-; \\ \frac{64}{135} \cdot \zeta(2) X^{5/6} & \text{for } i = 1. \end{cases} \quad (26)$$

As $n_0 = n_{2+} = n_{2-} = 4$ and $n_1 = 2$, Equations (20) and (26) now immediately imply Theorem 2.1.

To deduce Theorem 1.8 from Theorem 2.1, we require a count of the number of eligible pairs $(I, J) \in \mathbb{Z} \times \mathbb{Z}$ satisfying $H(I, J) < X$. The next lemma follows immediately from Theorem 1.7, which we prove in §2.8:

Lemma 2.9 *The set of eligible $(I, J) \in \mathbb{Z} \times \mathbb{Z}$ is a union of 9 distinct translates of $9\mathbb{Z} \times 27\mathbb{Z}$.*

The following proposition is now a simple application of Proposition 2.6 and Lemma 2.9.

Proposition 2.10 *Let $N_{I,J}^+(X)$ and $N_{I,J}^-(X)$ denote the number of eligible $(I, J) \in \mathbb{Z} \times \mathbb{Z}$ satisfying $H(I, J) < X$ that have positive discriminant and negative discriminant, respectively. Then we have*

$$(a) \quad N_{I,J}^+(X) = \frac{8}{135}X^{5/6} + O(X^{1/2});$$

$$(b) \quad N_{I,J}^-(X) = \frac{32}{135}X^{5/6} + O(X^{1/2}).$$

Proof: Let $R_{I,J}^\pm(X)$ denote the sets $\{(i, j) \in \mathbb{R}^2 : |i| < X^{1/3}, |j| < 2X^{1/2}, \pm(4i^3 - j^2) > 0\}$. The sizes of the projections of $R_{I,J}^\pm(X)$ onto smaller-dimensional coordinate hyperplanes are all bounded by $O(X^{1/2})$. Using Proposition 2.6 and Lemma 2.9 we then see that $N_{I,J}^\pm(X) = \frac{9}{243}\text{Vol}(R_{I,J}^\pm(X)) + O(X^{1/2})$. The volumes of $R_{I,J}^+(X)$ and $R_{I,J}^-(X)$ were computed in (24) and (25), respectively, and the proposition follows. \square

Theorem 1.8 now follows from Theorem 2.1 and Proposition 2.10.

2.5 Congruence conditions

In this subsection, we prove a version of Theorem 2.1 where we count integral binary quartic forms satisfying any specified finite set of congruence conditions.

Suppose S is a subset of $V_{\mathbb{Z}}$ defined by finitely many congruence conditions. We may assume that $S \subset V_{\mathbb{Z}}$ is defined by congruence conditions modulo some integer m . Then S may be viewed as the union of (say) k translates $\mathcal{L}_1, \dots, \mathcal{L}_k$ of the lattice $m \cdot V_{\mathbb{Z}}$. For each such lattice translate \mathcal{L}_j , we may use formula (16) and the discussion following that formula to compute $N(\mathcal{L}_j \cap V_{\mathbb{Z}}^{(i)}; X)$, where each d -dimensional volume is scaled by a factor of $1/m^d$ to reflect the fact that our new lattice has been scaled by a factor of m . With these scalings, the maximum volume of the projections of $B(n, t, \lambda, X)$ is seen to be at most $O(t^4 \lambda^{16})$. Analogous to Proposition 2.7, we see that the number of points (a, b, c, d, e) in $B(n, t, \lambda, X) \cap \mathcal{L}_j$ with $a \neq 0$ is

$$\begin{cases} 0 & \text{if } \frac{C\lambda}{t} < 1; \\ \frac{1}{m^5}\text{Vol}(B(n, t, \lambda, X)) + O(t^4 \lambda^{16}) & \text{otherwise.} \end{cases}$$

Carrying out the integral for $N(\mathcal{L}_j \cap V_{\mathbb{Z}}^{(i)}; X)$ as in (18)–(19), we obtain the following analogue of (20):

$$N(\mathcal{L}_j \cap V_{\mathbb{Z}}^{(i)}; X) = \frac{\text{Vol}(\mathcal{R}_X(L^{(i)}))}{n_i \cdot m^5} + O(X^{3/4+\epsilon}).$$

Summing over j , we thus obtain

$$N(S \cap V_{\mathbb{Z}}^{(i)}; X) = \frac{k\text{Vol}(\mathcal{R}_X(L^{(i)}))}{n_i \cdot m^5} + O(X^{3/4+\epsilon}). \quad (27)$$

For any set S in $V_{\mathbb{Z}}$ that is definable by congruence conditions, let us denote by $\mu_p(S)$ the p -adic density of the p -adic closure of S in $V_{\mathbb{Z}_p}$, where we normalize the additive measure μ_p on $V_{\mathbb{Z}_p}$ so that $\mu_p(V_{\mathbb{Z}_p}) = 1$. We then have the following theorem:

Theorem 2.11 *Suppose S is a subset of $V_{\mathbb{Z}}$ defined by congruence conditions modulo finitely many prime powers. Then we have*

$$N(S \cap V_{\mathbb{Z}}^{(i)}; X) = N(V_{\mathbb{Z}}^{(i)}; X) \prod_p \mu_p(S) + O(X^{3/4+\epsilon}), \quad (28)$$

where $\mu_p(S)$ denotes the p -adic density of S in $V_{\mathbb{Z}}$, and where the implied constant depends only on S and ϵ .

Theorem 2.11 follows from Equations (20) and (27), together with the identity $km^{-5} = \prod_p \mu_p(S)$.

We will also have occasion to use the following weighted version of Theorem 2.11; the proof is identical.

Theorem 2.12 *Let p_1, \dots, p_k be distinct prime numbers. For $j = 1, \dots, k$, let $\phi_{p_j} : V_{\mathbb{Z}} \rightarrow \mathbb{R}$ be a $\mathrm{GL}_2(\mathbb{Z})$ -invariant function on $V_{\mathbb{Z}}$ such that $\phi_{p_j}(f)$ depends only on the congruence class of f modulo some power $p_j^{a_j}$ of p_j . Let $N_{\phi}(V_{\mathbb{Z}}^{(i)}; X)$ denote the number of irreducible $\mathrm{GL}_2(\mathbb{Z})$ -orbits in $V_{\mathbb{Z}}^{(i)}$ having height bounded by X , where each orbit $\mathrm{GL}_2(\mathbb{Z}) \cdot f$ is counted with weight $\phi(f) := \prod_{j=1}^k \phi_{p_j}(f)$. Then we have*

$$N_{\phi}(V_{\mathbb{Z}}^{(i)}; X) = N(V_{\mathbb{Z}}^{(i)}; X) \prod_{j=1}^k \int_{f \in V_{\mathbb{Z}p_j}} \tilde{\phi}_{p_j}(f) df + O(X^{3/4+\epsilon}), \quad (29)$$

where $\tilde{\phi}_{p_j}$ is the natural extension of ϕ_{p_j} to $V_{\mathbb{Z}p_j}$, df denotes the additive measure on $V_{\mathbb{Z}p_j}$ normalized so that $\int_{f \in V_{\mathbb{Z}p_j}} df = 1$, and where the implied constant in the error term depends only on the local weight functions ϕ_{p_j} and ϵ .

2.6 Uniformity estimates

In order to prove Theorems 1.1 and 1.3, we require a sieve that allows us to count equivalence classes of integral binary quartic forms of bounded height satisfying certain infinite sets of congruence conditions. (In particular, this sieve will allow us to count equivalence classes of integral binary quartic forms having bounded height and *squarefree* discriminant.) A key ingredient for this sieve—and the purpose of this subsection—is an estimate that uniformly bounds the error terms in Theorems 2.11 and 2.12 as more and more congruence conditions are imposed.

Specifically, we prove the following theorem:

Theorem 2.13 *For a prime p , let $\mathcal{W}_p(V)$ denote the set of binary quartic forms $f \in V_{\mathbb{Z}}$ such that $p^2 \mid \Delta(f)$. Then, for any $M > 0$, we have:*

$$\lim_{X \rightarrow \infty} \frac{N(\cup_{p > M} \mathcal{W}_p(V); X)}{X^{5/6}} = O\left(\frac{1}{\log M}\right),$$

where the implied constant is independent of M .

Such uniformity estimates can in general be quite nontrivial. In the current case, to prove this estimate, we use the following trick. We embed the space of integral binary quartic forms into the space of pairs of integral ternary quadratic forms, where such an estimate has been proven previously [4, Proposition 23]. More precisely, let $W_{\mathbb{Z}}$ denote the space of pairs (A, B) of ternary quadratic forms having coefficients in \mathbb{Z} . We will always identify ternary quadratic forms over \mathbb{Z} with their Gram matrices whose coefficients lie in $\frac{1}{2}\mathbb{Z}$; we may thus express an element $(A, B) \in W_{\mathbb{Z}}$ as a pair of 3×3 symmetric matrices via

$$2 \cdot (A, B) = \left(\left[\begin{array}{ccc} 2a_{11} & a_{12} & a_{13} \\ a_{12} & 2a_{22} & a_{23} \\ a_{13} & a_{23} & 2a_{33} \end{array} \right], \left[\begin{array}{ccc} 2b_{11} & b_{12} & b_{13} \\ b_{12} & 2b_{22} & b_{23} \\ b_{13} & b_{23} & 2b_{33} \end{array} \right] \right),$$

where $a_{ij}, b_{ij} \in \mathbb{Z}$.

The group $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ acts naturally on the space $W_{\mathbb{Z}}$. Namely, an element $g_3 \in \mathrm{SL}_3(\mathbb{Z})$ acts on $W_{\mathbb{Z}}$ by $g_3 \cdot (A, B) = (g_3 A g_3^t, g_3 B g_3^t)$, while an element $g_2 = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ acts by $g_2 \cdot (A, B) = (pA + qB, rA + sB)$. The ring of polynomial invariants for the action of $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ on $W_{\mathbb{Z}}$ is generated by one element, which is called the *discriminant*. The discriminant $\Delta(A, B)$ of an element $(A, B) \in W_{\mathbb{Z}}$ is given by the discriminant of the binary cubic form $4 \mathrm{Det}(Ax - By)$ in x and y , and is thus an invariant of degree 12 in the entries of A and B .

The space $V_{\mathbb{Z}}$ of integral binary quartic forms embeds into $W_{\mathbb{Z}}$ via the map ϕ defined by

$$\phi : ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 \mapsto \left(\begin{bmatrix} & & 1/2 \\ & -1 & \\ 1/2 & & \end{bmatrix}, \begin{bmatrix} a & b/2 & 0 \\ b/2 & c & d/2 \\ 0 & d/2 & e \end{bmatrix} \right). \quad (30)$$

We denote the first matrix in (30) by A_1 , and the subset of all pairs (A_1, B) of ternary quadratic forms in $W_{\mathbb{Z}}$ by $W_{\mathbb{Z},1}$. The group $F_{\mathbb{Z},1} \times \mathrm{SO}(A_1) \subset \mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ preserves $W_{\mathbb{Z},1}$, where $F_{\mathbb{Z},1}$ is the group of all 2×2 lower triangular matrices over \mathbb{Z} with 1's on the diagonal. We also note that the map ϕ is *discriminant preserving*, i.e., the discriminant of an element of $V_{\mathbb{Z}}$ is equal to the discriminant of its image in $W_{\mathbb{Z}}$. For a binary quartic form f , if we write $\phi(f) = (A_1, B)$, then we call the binary form $\mathrm{Det}(Ax - By)$ the *cubic resolvent form* of f ; note that this form is *monic*, i.e., its leading coefficient as a polynomial in x is 1.

Next, we observe that every $F_{\mathbb{Z},1}$ -equivalence class of $W_{\mathbb{Z},1}$ contains a unique element (A_1, B) such that the top right entry of B is equal to 0. It follows that ϕ maps the space of binary quartic forms $V_{\mathbb{Z}}$ bijectively to the set of $F_{\mathbb{Z},1}$ -orbits on $W_{\mathbb{Z},1}$ via the composite map

$$V_{\mathbb{Z}} \rightarrow W_{\mathbb{Z},1} \rightarrow F_{\mathbb{Z},1} \backslash W_{\mathbb{Z},1}.$$

We may ask how the action of $\mathrm{GL}_2(\mathbb{Z})$ on $V_{\mathbb{Z}}$ manifests itself (via ϕ) as an action on $F_{\mathbb{Z},1} \backslash W_{\mathbb{Z},1}$. To answer this, note that the center of $\mathrm{GL}_2(\mathbb{Z})$ acts trivially on its representation on binary quadratic forms $px^2 - 2qxy + ry^2$ via $\gamma \cdot f(x, y) := f((x, y) \cdot \gamma) / (\det \gamma)$. This action of $\mathrm{GL}_2(\mathbb{Z})$ preserves the discriminant $4(q^2 - pr)$ of these binary quadratic forms, yielding the map

$$\begin{aligned} \rho : \mathrm{PGL}_2(\mathbb{Z}) &\rightarrow \mathrm{SL}_3(\mathbb{Z}), \text{ given explicitly by} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\mapsto \frac{1}{ad - bc} \begin{pmatrix} d^2 & cd & c^2 \\ 2bd & ad + bc & 2ac \\ b^2 & ab & a^2 \end{pmatrix}. \end{aligned} \quad (31)$$

Since A_1 is the Gram matrix of the ternary form $q^2 - pr$, we see that the image of $\mathrm{PGL}_2(\mathbb{Z})$ is contained in the orthogonal group $\mathrm{SO}(A_1, \mathbb{Z})$, and is in fact equal to it (see [43, Lemma 4.4.2]).

For any ring R , let V_R denote the space of binary quartic forms with coefficients in R . The center of $\mathrm{GL}_2(R)$ acts trivially under the “twisted action” of $\mathrm{GL}_2(R)$ on V_R defined by

$$\gamma \cdot f(x, y) := (\det \gamma)^{-2} f((x, y) \cdot \gamma), \quad (32)$$

yielding an action of $\mathrm{PGL}_2(R)$ on V_R . Note that the $\mathrm{PGL}_2(\mathbb{Z})$ -orbits on $V_{\mathbb{Z}}$ are the same as the $\mathrm{GL}_2(\mathbb{Z})$ -orbits on $V_{\mathbb{Z}}$, since $\begin{pmatrix} -1 & \\ & -1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ acts trivially on $V_{\mathbb{Z}}$.

It is now easily checked that $\phi(\gamma \cdot f)$ and $\rho(\gamma) \cdot \phi(f)$ are the same element in $F_{\mathbb{Z},1} \backslash W_{\mathbb{Z},1}$ for all $\gamma \in \mathrm{PGL}_2(\mathbb{Z})$ and $f \in V_{\mathbb{Z}}$. Therefore, we have the following theorem, which will be essential in proving the uniformity estimate of Theorem 2.13:

Theorem 2.14 *The map ϕ defined by (30) gives a canonical bijection between $\mathrm{PGL}_2(\mathbb{Z})$ -orbits on $V_{\mathbb{Z}}$ and $F_{\mathbb{Z},1} \times \mathrm{SO}(A_1, \mathbb{Z})$ -orbits on $W_{\mathbb{Z},1}$.*

We thus obtain a natural map

$$\psi : \mathrm{PGL}_2(\mathbb{Z}) \backslash V_{\mathbb{Z}} \rightarrow (\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})) \backslash W_{\mathbb{Z}} \quad (33)$$

given by the composite map

$$\mathrm{PGL}_2(\mathbb{Z}) \backslash V_{\mathbb{Z}} \rightarrow (F_{\mathbb{Z},1} \times \mathrm{SO}(A_1, \mathbb{Z})) \backslash W_{\mathbb{Z},1} \rightarrow (\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})) \backslash W_{\mathbb{Z}}. \quad (34)$$

Remark 2.15 It is proven in [3] that the orbit space $(\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})) \backslash W_{\mathbb{Z}}$ corresponds to isomorphism classes of pairs (Q, R) , where Q is a quartic ring and R is a cubic resolvent ring of Q . Meanwhile, using the map (30), Wood [44] proves that the orbit space $\mathrm{PGL}_2(\mathbb{Z}) \backslash V_{\mathbb{Z}}$ corresponds to isomorphism classes of triples

(Q, R, x) , where Q is a quartic ring, R is a monogenic cubic resolvent ring of Q , and x is a *monogenizer* of R , i.e., x generates R as a \mathbb{Z} -algebra (so that $R = \mathbb{Z}[x]$). It follows that the map ψ in (33) corresponds to the map

$$\{(Q, R, x)\} \rightarrow \{(Q, R)\},$$

which takes a quartic ring with a monogenized cubic resolvent ring and simply forgets its monogenizer (and the fact that R is monogenic).

Before we state and prove the desired uniformity estimate, we require the following key proposition:

Proposition 2.16 *An element of $(\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})) \backslash W_{\mathbb{Z}}$ with nonzero discriminant has at most 12 preimages in $\mathrm{PGL}_2(\mathbb{Z}) \backslash V_{\mathbb{Z}}$ under the map ψ .*

Proof: By Theorem 2.14, it suffices to prove that an element w of $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z}) \backslash W_{\mathbb{Z}}$ has at most 12 preimages in $F_{\mathbb{Z},1} \times \mathrm{SO}(A_1, \mathbb{Z}) \backslash W_{\mathbb{Z},1}$. Let $\{(A_1, B_\alpha)\}$ be a set of $F_{\mathbb{Z},1} \times \mathrm{SO}(A_1, \mathbb{Z})$ -inequivalent preimages of w in $W_{\mathbb{Z},1}$, where α ranges over some (possibly infinite) set \mathcal{A} . The integral binary cubic forms $g_\alpha(x, y) := 4\mathrm{Det}(A_1x - B_\alpha y)$ all have x^3 -coefficient equal to 1, i.e., $g_\alpha(1, 0) = 1$. Since the (A_1, B_α) are pairwise $F_{\mathbb{Z},1} \times \mathrm{SO}(A_1, \mathbb{Z})$ -inequivalent but are all $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ -equivalent, we see that the g_α are pairwise $F_{\mathbb{Z},1}$ -inequivalent but are all $\mathrm{GL}_2(\mathbb{Z})$ -equivalent.

The deep results in [22] and [25], which assert that $g(x, y) = 1$ has at most 12 solutions with $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ for an integral binary cubic form g of nonzero discriminant, now imply that the cardinality of \mathcal{A} is at most 12. \square

We may now proceed to the proof of Theorem 2.13. To this end, let $\mathcal{W}_p(V) \subset V_{\mathbb{Z}}$ denote the set of integral binary quartic forms f such that $p^2 \mid \Delta(f)$. We partition $\mathcal{W}_p(V)$ into two disjoint sets $\mathcal{W}_p^{(1)}(V)$ and $\mathcal{W}_p^{(2)}(V)$. Here, $\mathcal{W}_p^{(1)}(V)$ is the set of all binary quartic forms f whose discriminant is *strongly divisible* by p^2 , i.e., $p^2 \mid \Delta(f + pg)$ for all $g \in V_{\mathbb{Z}}$. The set $\mathcal{W}_p^{(2)}(V)$ is the set of all binary quartic forms $f \in V_{\mathbb{Z}}$ whose discriminant, in the terminology of [6], is *weakly divisible* by p^2 , i.e., there exists $g \in V_{\mathbb{Z}}$ such that $p^2 \nmid \Delta(f + pg)$.

Then an element $f \in \mathcal{W}_p^{(1)}(V)$ is either a multiple of p or the *splitting type* of f at p is $(1^3 1)$, $(1^2 1^2)$, (2^2) , or (1^4) , i.e., either $f \in pV_{\mathbb{Z}}$ or the reduction of f modulo p factors into irreducible factors over \mathbb{F}_p as $c(x - \alpha y)^3(x - \beta y)$, $c(x - \alpha y)^2(x - \beta y)^2$, $c(x^2 + \alpha xy + \beta y^2)^2$, or $c(x - \alpha y)^4$, respectively.

The desired uniformity estimate for $\mathcal{W}_p^{(1)}(V)$ follows by applying the following quantitative version of a result of Ekedahl [24], proven in [6, Theorem 3.3]:

Theorem 2.17 *Let B be a compact region in \mathbb{R}^n having finite measure, and let Y be any closed subscheme of $\mathbb{A}_{\mathbb{Z}}^n$ of codimension $k \geq 2$. Let r and M be positive real numbers. Then we have*

$$\#\{v \in rB \cap \mathbb{Z}^n \mid v \pmod{p} \in Y(\mathbb{F}_p) \text{ for some prime } p > M\} = O\left(\frac{r^n}{M^{k-1} \log M} + r^{n-k+1}\right), \quad (35)$$

where the implied constant depends only on B and on Y .

To apply this result, recall that we used $\mathcal{F}_{\mathrm{PGL}_2}$ to denote the fundamental domain $N'A'K$ for the left action of $\mathrm{PGL}_2(\mathbb{Z})$ on $\mathrm{PGL}_2(\mathbb{R})$. For $0 < \epsilon < 1$, we denote by $\mathcal{F}_{\mathrm{PGL}_2}^{(\epsilon)}$ the subset of elements $n(u)a(t)k \in \mathcal{F}_{\mathrm{PGL}_2}$ where t is bounded above by a suitable constant to ensure that

$$\mathrm{Vol}(\mathcal{F}_{\mathrm{PGL}_2}^{(\epsilon)}) = (1 - \epsilon)\mathrm{Vol}(\mathcal{F}_{\mathrm{PGL}_2}).$$

Then, for fixed $\epsilon > 0$, the set $\mathcal{F}_{\mathrm{PGL}_2}^{(\epsilon)} \cdot R^{(i)}(X)$ (with $R^{(i)}(X)$ as defined in §2.4) is a bounded region in $V_{\mathbb{R}}$ that expands homogeneously as X grows. We have the following theorem:

Theorem 2.18 *Let $0 < \epsilon < 1$ be fixed. For $i \in \{0, 1, 2+, 2-\}$, we have*

$$\#\left\{\mathcal{F}_{\mathrm{PGL}_2}^{(\epsilon)} \cdot R^{(i)}(X) \cap \left(\bigcup_{p > M} \mathcal{W}_p^{(1)}(V)\right)\right\} = O(X^{5/6}/(M \log M) + X^{2/3}), \quad (36)$$

where the implied constant depends only on ϵ .

Indeed, the discriminants of elements in $\mathcal{W}_p^{(1)}(V)$ are strongly divisible by p^2 . Theorem 2.18 thus follows from Theorem 2.17 (with $n = 5$, $k = 2$, and $r = X^{1/6}$) because, as noted in [6], if an element in $v \in V_{\mathbb{Z}}$ has discriminant Δ strongly divisible by p^2 , then it lies in $Y(\mathbb{F}_p)$, where Y is the codimension 2 subscheme of $V \cong \mathbb{A}^5$ defined by the vanishing of Δ and $\partial\Delta/\partial e$.

However, a uniformity estimate for $\mathcal{W}_p^{(2)}(V)$ —the set of elements in $V_{\mathbb{Z}}$ having discriminant divisible, but not strongly divisible, by p^2 —is more difficult to obtain. It is for this case that we consider the embedding (30) of $V_{\mathbb{Z}}$ into $W_{\mathbb{Z}}$, where we can then use previously obtained uniformity estimates for $W_{\mathbb{Z}}$. We state the relevant estimate for $W_{\mathbb{Z}}$ below:

Theorem 2.19 ([4, Proposition 23]) *Let $\mathcal{W}_p^{(2)}(W)$ denote the set of elements in $W_{\mathbb{Z}}$ whose discriminants are divisible, but not strongly divisible, by p^2 . Then the number of $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ -orbits on $\mathcal{W}_p^{(2)}(W)$ having discriminant bounded by X is $O(X/p^2)$, where the implied constant is independent of p .*

We may use this uniformity estimate for $\mathcal{W}_p^{(2)}(W)$ to obtain one for $\mathcal{W}_p^{(2)}(V)$. Specifically, in conjunction with Proposition 2.16, we obtain the estimate

$$N(\mathcal{W}_p^{(2)}(V); X) = O(X/p^2), \quad (37)$$

where the implied constant is independent of X and p .

Theorem 2.20 *Let $0 < \epsilon < 1$ be fixed. For $i \in \{0, 1, 2+, 2-\}$, we have*

$$\#\left\{\mathcal{F}_{\mathrm{PGL}_2}^{(\epsilon)} \cdot R^{(i)}(X) \cap (\cup_{p>M} \mathcal{W}_p^{(2)}(V))\right\} = O(X^{5/6}/\log M), \quad (38)$$

where the implied constant is independent of X and M .

Proof: We define $R_X^{(\epsilon)} := \mathcal{F}_{\mathrm{PGL}_2}^{(\epsilon)} \cdot R^{(i)}(X)$ and obtain an individual bound on $\#\{R_X^{(\epsilon)} \cap \mathcal{W}_p^{(2)}(V)\}$ for each prime p . When viewed as a polynomial in e , the derivative of Δ with respect to e is a nonzero cubic polynomial $\partial\Delta/\partial e$ in e . If a binary quartic form $f(x, y) = a_0x^4 + b_0x^3y + c_0x^2y^2 + d_0xy^3 + e_0y^4$ belongs to $\mathcal{W}_p^{(2)}$, then for this form f we must have $p^2 \mid \Delta$ and $p \nmid \partial\Delta/\partial e$ (for otherwise f would belong to $\mathcal{W}_p^{(1)}$). Since $R_X^{(\epsilon)}$ is a homogeneously expanding region in $V_{\mathbb{R}} = \mathbb{R}^5$ with each side growing at the order of $X^{1/6}$, there are $O(X^{4/6})$ possibilities for a quadruple (a_0, b_0, c_0, d_0) such that $f(x, y) \in R_X^{(\epsilon)} \cap V_{\mathbb{Z}}$ for some e_0 . Given fixed values of $a_0, b_0, c_0,$ and d_0 , there are at most 3 choices for the residue of $e_0 \pmod{p}$ such that $p \mid \Delta$. Since $p \nmid \partial\Delta/\partial e$, each such residue modulo p has a unique lift modulo p^2 such that $p^2 \mid \Delta$. Hence, we have

$$\#\{R_X^{(\epsilon)} \cap \mathcal{W}_p^{(2)}(V)\} = O(\max\{X^{5/6}/p^2, X^{4/6}\}), \quad (39)$$

where we may use the first estimate for $p \leq X^{1/12}$ and the second estimate for $p > X^{1/12}$. Since there are $O(X^{1/6}/\log X)$ primes in the range $[1, X^{1/6}]$, and since $\sum_{p>X^{1/6}} 1/p^2 = O(1/(X^{1/6} \log X))$, we obtain

$$\#\left\{R_X^{(\epsilon)} \cap (\cup_{p>M} \mathcal{W}_p^{(2)}(V))\right\} = O\left(\sum_{p>M} \#\{R_X^{(\epsilon)} \cap \mathcal{W}_p^{(2)}(V)\}\right) = O(X^{5/6}/\log M)$$

by using (39) to estimate $\#\{R_X^{(\epsilon)} \cap \mathcal{W}_p^{(2)}(V)\}$ when $p < X^{1/6}$, and using (37) when $p \geq X^{1/6}$. \square

Using the above two uniformity estimates, we obtain a proof of Theorem 2.13:

Proof of Theorem 2.13: Let $R(X)$ denote $\cup_i R^{(i)}(X)$. By the results of §2.1, we have:

$$\begin{aligned} N(\cup_{p>M} \mathcal{W}_p(V), X) &\leq \#\{\mathcal{F}_{\mathrm{PGL}_2} \cdot R(X) \cap (\cup_{p>M} \mathcal{W}_p(V)) \cap V_{\mathbb{Z}}^{\mathrm{irr}}\} \\ &\leq \#\{\mathcal{F}_{\mathrm{PGL}_2}^{(\epsilon)} \cdot R(X) \cap (\cup_{p>M} \mathcal{W}_p(V))\} + \#\{(\mathcal{F}_{\mathrm{PGL}_2} \setminus \mathcal{F}_{\mathrm{PGL}_2}^{(\epsilon)}) \cdot R(X) \cap V_{\mathbb{Z}}^{\mathrm{irr}}\}. \end{aligned} \quad (40)$$

By Theorems 2.18 and 2.20, the first term in the second line of (40) is bounded by $O(X^{5/6}/\log M + X^{2/3})$. The results of §2.3 and §2.4 imply that the second term is bounded by $\mathrm{Vol}((\mathcal{F}_{\mathrm{PGL}_2} - \mathcal{F}_{\mathrm{PGL}_2}^{(\epsilon)}) \cdot R(X)) = O(\epsilon X^{5/6})$. Since this holds for all $\epsilon > 0$, the theorem follows. \square

2.7 A squarefree sieve

For the applications, we require a more general congruence version of our counting theorem for binary quartic forms, namely, one which allows appropriate infinite sets of congruence conditions to be imposed and which also allows weighted counts of lattice points (where weights are also assigned by congruence conditions). More precisely, we say that a function $\phi : V_{\mathbb{Z}} \rightarrow [0, 1] \subset \mathbb{R}$ is *defined by congruence conditions* if, for all primes p , there exist functions $\phi_p : V_{\mathbb{Z}_p} \rightarrow [0, 1]$ satisfying the following conditions:

- (1) For all $f \in V_{\mathbb{Z}}$, the product $\prod_p \phi_p(f)$ converges to $\phi(f)$.
- (2) For each prime p , the function ϕ_p is locally constant outside some closed set $S_p \subset V_{\mathbb{Z}_p}$ of measure zero.

Such a function ϕ is called *acceptable* if, for sufficiently large primes p , we have $\phi_p(f) = 1$ whenever $p^2 \nmid \Delta(f)$. For example, the characteristic function of the set of integral binary quartic forms having squarefree discriminant is an acceptable function.

We then have the following version of Theorem 2.12, in which we allow weights to be defined by certain infinite sets of congruence conditions:

Theorem 2.21 *Let $\phi : V_{\mathbb{Z}} \rightarrow [0, 1]$ be an acceptable function that is defined by congruence conditions via the local functions $\phi_p : V_{\mathbb{Z}_p} \rightarrow [0, 1]$. Then, with notation as in Theorem 2.12, we have:*

$$N_{\phi}(V_{\mathbb{Z}}^{(i)}; X) = N(V_{\mathbb{Z}}^{(i)}; X) \prod_p \int_{f \in V_{\mathbb{Z}_p}} \phi_p(f) df + o(X^{5/6}). \quad (41)$$

Proof: Since ϕ_p is locally constant outside some set of measure zero, there exists an increasing sequence of functions $\psi_{p,1} \leq \psi_{p,2} \leq \dots$ that are bounded above by and converge pointwise to ϕ_p , and a decreasing sequence of functions $1 = \psi'_{p,0} \geq \psi'_{p,1} \geq \psi'_{p,2} \geq \dots$ that are bounded below by and converge pointwise to ϕ_p , such that $\psi_{p,n}$ and $\psi'_{p,n}$ are defined on $V_{\mathbb{Z}_p}$ by congruence conditions modulo p^n . It will also be convenient in the formulas that follow to define $\psi_{p,0}$ to equal the constant function 1 on $V_{\mathbb{Z}_p}$.

By the dominated convergence theorem, we have

$$\lim_{n \rightarrow \infty} \int_{V_{\mathbb{Z}_p}} \psi_{p,n}(f) df = \lim_{n \rightarrow \infty} \int_{V_{\mathbb{Z}_p}} \psi'_{p,n}(f) df = \int_{V_{\mathbb{Z}_p}} \phi_p(f) df. \quad (42)$$

Furthermore, since ϕ is acceptable we have

$$1 - \int_{V_{\mathbb{Z}_p}} \phi_p(f) df \leq \int_{\substack{f \in V_{\mathbb{Z}_p} \\ p^2 \mid \Delta(f)}} df \ll p^{-2} \quad (43)$$

for sufficiently large p (see, for example, [36, Proof of Theorem 3.2]).

For a fixed integer Y , let $N_{\psi}^Y(V_{\mathbb{Z}}^{(i)}; X)$ (resp. $N_{\psi'}^Y(V_{\mathbb{Z}}^{(i)}; X)$) denote the number of irreducible $\mathrm{GL}_2(\mathbb{Z})$ -orbits in $V_{\mathbb{Z}}^{(i)}$ having height bounded by X , where each orbit $\mathrm{GL}_2(\mathbb{Z}) \cdot f$ is counted with weight

$$\prod_p \psi_{p, \lfloor Y/p \rfloor}(f) \quad \left(\text{resp. } \prod_p \psi'_{p, \lfloor Y/p \rfloor}(f) \right).$$

The function $\lfloor Y/p \rfloor$ is chosen to take nonzero values only for finitely many primes p for any fixed Y . Therefore, it follows from Theorem 2.12 that, for any fixed Y , we have

$$\limsup_{X \rightarrow \infty} \frac{N_{\phi}(V_{\mathbb{Z}}^{(i)}; X)}{X^{5/6}} \leq \limsup_{X \rightarrow \infty} \frac{N_{\psi'}^Y(V_{\mathbb{Z}}^{(i)}; X)}{X^{5/6}} = \lim_{X \rightarrow \infty} \frac{N(V_{\mathbb{Z}}^{(i)}; X)}{X^{5/6}} \prod_p \int_{f \in V_{\mathbb{Z}_p}} \psi'_{p, \lfloor Y/p \rfloor}(f) df.$$

Equation (43) implies that the product $\prod_p \int_{V_{\mathbb{Z}_p}} \phi_p(f) df$ converges. Letting Y tend to infinity, we have by (42) that

$$\limsup_{X \rightarrow \infty} \frac{N_{\phi}(V_{\mathbb{Z}}^{(i)}; X)}{X^{5/6}} \leq \lim_{X \rightarrow \infty} \frac{N(V_{\mathbb{Z}}^{(i)}; X)}{X^{5/6}} \prod_p \int_{f \in V_{\mathbb{Z}_p}} \phi_p(f) df. \quad (44)$$

We now obtain a lower bound using Theorem 2.13. For sufficiently large p and $n \geq 1$, we have $\psi_{p,n}(f) = \phi_p(f) = 1$ unless $p^2 \mid \Delta(f)$. Thus, for sufficiently large Y , we have

$$\begin{aligned} \liminf_{X \rightarrow \infty} \frac{N_\phi(V_{\mathbb{Z}}^{(i)}; X)}{X^{5/6}} &\geq \liminf_{X \rightarrow \infty} \left[\frac{N_\psi(V_{\mathbb{Z}}^{(i)}; X)}{X^{5/6}} - \frac{O(N(\cup_{p>Y} \mathcal{W}_p(V); X))}{X^{5/6}} \right] \\ &= \lim_{X \rightarrow \infty} \frac{N(V_{\mathbb{Z}}^{(i)}; X)}{X^{5/6}} \cdot \prod_p \int_{f \in V_{\mathbb{Z}_p}} \psi_{p, \lfloor Y/p \rfloor}(f) df - O(1/\log Y), \end{aligned}$$

where the first inequality follows because ϕ is an upper bound for $\psi_{p,n}$ unless $n = 0$, and the last equality follows from Theorems 2.12 and 2.13. Taking the limit as Y tends to infinity then yields

$$\liminf_{X \rightarrow \infty} \frac{N_\phi(V_{\mathbb{Z}}^{(i)}; X)}{X^{5/6}} = \lim_{X \rightarrow \infty} \frac{N(V_{\mathbb{Z}}^{(i)}; X)}{X^{5/6}} \cdot \prod_p \int_{f \in V_{\mathbb{Z}_p}} \phi_p(f) df \quad (45)$$

where we use (43) to exchange the limit (in Y) and product, and (42) to exchange the limit (in Y) and integral. The theorem now follows from (44) and (45). \square

2.8 Proofs of auxiliary results (Lemma 2.2, Lemma 2.4, and Theorem 1.7)

The proofs of the auxiliary results referred to in the title all turn out to have natural interpretations in terms of the monic cubic resolvent forms of binary quartic forms, as discussed in §2.6. More precisely, a *monic binary cubic form* $g(x, y)$ is defined as a binary cubic form $g(x, y)$ whose leading coefficient as a polynomial in x is equal to 1, i.e., it is of the form $x^3 + rx^2y + sxy^2 + ty^3$. We denote the space of binary cubic forms over \mathbb{Z} by $U_{\mathbb{Z}}$, and the subset of monic binary cubic forms over \mathbb{Z} by $U_{\mathbb{Z},1} \subset U_{\mathbb{Z}}$. Note that if $(A, B) \in W_{\mathbb{Z}}$, then $4 \text{Det}(Ax - By) \in U_{\mathbb{Z}}$, and that if $(A_1, B) \in W_{\mathbb{Z},1}$, then $4 \text{Det}(A_1x - By) \in U_{\mathbb{Z},1}$.

The group $F_{\mathbb{Z},1}$ acts naturally on $U_{\mathbb{Z},1}$ via $\gamma \cdot g(x, y) = g((x, y) \cdot \gamma)$. If $g(x, y) = x^3 + rx^2y + sxy^2 + ty^3$, then one easily sees that the quantities

$$\begin{aligned} I(g) &:= r^2 - 3s, \\ J(g) &:= -2r^3 + 9rs - 27t \end{aligned} \quad (46)$$

are invariant under the action of $F_{\mathbb{Z},1}$. The discriminant $\Delta(g)$ of the binary cubic form g can be expressed in terms of these basic invariants $I(g)$ and $J(g)$, namely, $\Delta(g) = (4I(g)^3 - J(g)^2)/27$. We again define the *height* of g by

$$H(g) := H(I, J) = \max\{|I(g)^3|, J(g)^2/4\}.$$

If $F_{\mathbb{Q},1}$ denotes the group of lower triangular matrices in $\text{SL}_2(\mathbb{Q})$ with 1's on the diagonal, then by using an $F_{\mathbb{Q},1}$ -transformation to clear out the x^2y -coefficient, we see that $g(x, y)$ is $F_{\mathbb{Q},1}$ -equivalent to the monic binary cubic form $h(x, y) = x^3 - \frac{I(f)}{3}xy^2 - \frac{J(f)}{27}y^3$.

If $f \in V_{\mathbb{Z}}$ is an integral binary quartic form, then as in §2.6 we define the *monic cubic resolvent form* of f by $g(x, y) = 4 \text{Det}(A_1x - B_fy)$, where (A_1, B_f) is the image of f under the map ϕ defined in (30). It is easy to check that $I(f) = I(g)$ and $J(f) = J(g)$. The elliptic curve $E_f : z^2 = g(x, 1)$ (which we may also write as $z^2 = x^3 - \frac{I(f)}{3}x - \frac{J(f)}{27}$) turns out to be the Jacobian of the genus one curve C_f in weighted projective space $\mathbb{P}(1, 1, 2)$ determined by the equation $z^2 = f(x, y)$; furthermore, the stabilizer of f in $\text{PGL}_2(\mathbb{Q})$ is isomorphic to $E_f(\mathbb{Q})[2]$ (see Theorem 32). This connection between f and E_f will be of key importance in the next section.

We first use this connection to prove Lemma 2.4, which states that the stabilizer in $\text{GL}_2(\mathbb{R})$ of $f \in V_{\mathbb{R}}$ is 8 or 4 in accordance with whether the discriminant of f is positive or negative, respectively.

Proof of Lemma 2.2: Consider the action of $\text{PGL}_2(\mathbb{R})$ on $V_{\mathbb{R}}$ defined by (32). If $f \in V_{\mathbb{R}}$ has nonzero discriminant, then Theorem 3.2 in Section 3 (which does not rely on the results of this section) asserts that

$\text{Stab}_{\text{PGL}_2(\mathbb{R})}(f)$ is isomorphic to $E(\mathbb{R})[2]$, where E is the elliptic curve given by $y^2 = x^3 - \frac{I(f)}{3}x - \frac{J(f)}{27}$. Therefore, $\#\text{Stab}_{\text{PGL}_2(\mathbb{R})}(f)$ is equal to 2 if $\Delta(f) < 0$ and equal to 4 if $\Delta(f) > 0$.

Now if $\gamma \in \text{GL}_2(\mathbb{R})$ stabilizes $f \in V_{\mathbb{R}}$ under the usual action (defined in (3)), then since $I(\gamma \cdot f) = (\det \gamma)^4 I(f)$ and $J(\gamma \cdot f) = (\det \gamma)^6 J(f)$, we see that $\det \gamma = \pm 1$. Hence the image of γ in $\text{PGL}_2(\mathbb{R})$ also stabilizes f . Since there are two elements in the center of $\text{GL}_2(\mathbb{R})$ that stabilize f , the size of the stabilizer in $\text{GL}_2(\mathbb{R})$ of an element $f \in V_{\mathbb{R}}^{(i)}$ is 4 when $i = 1$ (equivalently $\Delta(f) < 0$) and 8 when $i = 0$ or 2 (equivalently $\Delta(f) > 0$), as desired. \square

To prove Lemma 2.4, which states that the number of $\text{GL}_2(\mathbb{Z})$ -orbits on binary quartic forms having bounded height and a nontrivial stabilizer in $\text{PGL}_2(\mathbb{Q})$ is negligible, we use the following lemma:

Lemma 2.22 *The number of $F_{\mathbb{Z},1}$ -orbits on monic integral binary cubic forms g such that g is reducible over \mathbb{Q} and $H(g) < X$ is $O(X^{1/2+\epsilon})$.*

Proof: First, we note that if $g(x, y) = x^3 + rx^2y + sxy^2 + ty^3 \in U_{\mathbb{Z},1}$, then by replacing g with an $F_{\mathbb{Z},1}$ -translate if necessary we may assume that $r \in \{-1, 0, 1\}$. Throughout the rest of this proof, we will assume that this is the case. If g is such that $H(g) < X$, then since $|I(g)|^3 = |r^2 - 3s|^3 \leq H(g) < X$, we see that $s = O(X^{1/3})$. Since $J(g)^2/4 = (2r^3 + 9rs - 27t)^2/4 \leq H(g) < X$, this in turn implies that $t = O(X^{1/2})$.

Let us now count such forms g that are reducible. If $g(x, y) = x^3 + rx^2y + sxy^2 + ty^3$ satisfies $t = 0$ (and $r \in \{-1, 0, 1\}$), then g is reducible, and the number of such forms g with $H(g) < X$ is the number of possible values for r and s , namely $3 \cdot O(X^{1/3}) = O(X^{1/3})$.

Next, we consider those reducible forms $g(x, y) = x^3 + rx^2y + sxy^2 + ty^3$ satisfying $H(g) < X$, $r \in \{-1, 0, 1\}$ and $t \neq 0$. If $x - my$ is a factor of g , then $m \mid t$. Therefore, if we fix $t \neq 0$, then there are at most $t^\epsilon = O(X^\epsilon)$ choices for m . Moreover, once r , t , and m are fixed, then setting $g(m, 1)$ equal to 0 determines s . Since $t = O(X^{1/2})$, and there are at most 3 possible values for r , it follows that there are at most $O(X^{1/2+\epsilon})$ such reducible forms g with height less than X . \square

Proof of Lemma 2.4: Suppose an integral binary quartic form f has a stabilizer of size at least 2 in $\text{PGL}_2(\mathbb{Q})$. Then Theorem 3.2 asserts that $E(\mathbb{Q})[2]$ is nontrivial, where E is given by $y^2 = x^3 - \frac{I(f)}{3}x - \frac{J(f)}{27}$. This implies that the cubic resolvent form g of f is reducible over \mathbb{Q} . If we further assume that $H(f) < X$, then Lemma 2.22 implies that there are at most $O(X^{1/2+\epsilon})$ choices for the $F_{\mathbb{Z},1}$ -orbit of g .

Now, if the $\text{GL}_2(\mathbb{Z})$ -orbit of a reducible integral binary cubic form g having height X is fixed, then [4, Proof of Lemma 12] implies that the number of $\text{GL}_2(\mathbb{Z}) \times \text{SL}_3(\mathbb{Z})$ -orbits on $W_{\mathbb{Z}}$ having g as a cubic resolvent form is bounded by $O(X^{1/4})$. In conjunction with Proposition 2.16, this implies that the number of $\text{PGL}_2(\mathbb{Z})$ -orbits on $V_{\mathbb{Z}}$ having g as a cubic resolvent form is also at most $O(X^{1/4})$. Therefore, the number of $\text{PGL}_2(\mathbb{Z})$ -orbits on $V_{\mathbb{Z}}$ having a nontrivial stabilizer in $\text{PGL}_2(\mathbb{Q})$ and height less than X is bounded by $O(X^{1/4} X^{1/2+\epsilon}) = O(X^{3/4+\epsilon})$. This concludes the proof of Lemma 2.4. \square

Finally, we determine when a pair of invariants $(I, J) \in \mathbb{Z} \times \mathbb{Z}$ is eligible, thus proving Theorem 1.7.

Proof of Theorem 1.7: If an integral binary quartic form has invariants equal to I and J , then its cubic resolvent form also has invariants equal to I and J . Conversely, suppose an integral pair (I, J) occurs as the invariants of an integral monic binary cubic form $g(x, y) = x^3 + rx^2y + sxy^2 + ty^3$. Then one checks that the cubic resolvent form of the binary quartic form $f(x, y) = x^3y + rx^2y^2 + sxy^3 + ty^4$ is equal to g , and so f has invariants equal to I and J . Therefore the pair (I, J) is eligible. Hence, to prove Theorem 1.7, it suffices to answer the simpler question: which integral pairs (I, J) occur as invariants of integral monic binary cubic forms?

Suppose the integral monic binary cubic form $g(x, y) = x^3 + rx^2y + sxy^2 + ty^3 \in U_{\mathbb{Z},1}$ has invariants I and J . By replacing g with an $F_{\mathbb{Z},1}$ -translate if necessary, we may assume that $r \in \{-1, 0, 1\}$. This does not change the invariants I and J . If $I \equiv 0 \pmod{3}$ then $r = 0$, implying that $27 \mid J$. This is condition (a) in Theorem 1.7.

If I is not divisible by 3, then r equals 1 or -1 and we have $I \equiv 1 \pmod{3}$. Thus I must be congruent to 1, 4, or 7 $\pmod{9}$, which happens exactly when s is congruent to 0, 2, or 1 $\pmod{3}$, respectively. Because

$r^2 = 1$, we see that $J \equiv r(9s - 2) \pmod{27}$. It follows that $I \equiv 1, 4, 7 \pmod{9}$ corresponds to $J \equiv \pm 2, \pm 16, \pm 7 \pmod{27}$, respectively, yielding conditions (b), (c), and (d).

Therefore, if a pair (I, J) occurs as the invariants of an integral monic binary cubic form, then it must satisfy one of the conditions of Theorem 1.7. The converse also follows easily by reversing the above arguments. This concludes the proof of Theorem 1.7. \square

3 The average size of the 2-Selmer groups of elliptic curves

Recall that every elliptic curve E over \mathbb{Q} can be written in the form

$$E_{A,B} : y^2 = x^3 + Ax + B, \quad (47)$$

where $A, B \in \mathbb{Z}$ and $p^4 \nmid A$ if $p^6 \mid B$. For any elliptic curve $E = E_{A,B}$ over \mathbb{Q} written in the form (47), we define the quantities $I = I(E)$ and $J = J(E)$ by

$$\begin{aligned} I(E) &:= -3A, \\ J(E) &:= -27B, \end{aligned} \quad (48)$$

and denote the curve $E_{A,B}$ also by $E^{I,J}$. The height of $E_{A,B} = E^{I,J}$ is then defined by

$$H(E_{A,B}) = \max\{4|A^3|, 27B^2\} = \frac{4}{27} \max\{I(E)^3, J(E)^2/4\}.$$

In this section, we shall work with the slightly different height $H'(E)$ defined by

$$H'(E) := H(I(E), J(E)) = \max\{|I(E)|^3, J(E)^2/4\}, \quad (49)$$

so that the height agrees with the height defined for binary quartic forms in (6). Note that H and H' only differ by a constant factor; namely, for every elliptic curve E over \mathbb{Q} we have $27H(E) = 4H'(E)$.

Our purpose in this section is to prove Theorem 1.3 by computing the average size of the 2-Selmer group of elliptic curves E/\mathbb{Q} when these curves are ordered by their heights (note that the two heights H and H' give the same ordering on every set of elliptic curves). Theorem 1.1, being a special case of Theorem 1.3, will then follow.

In fact, we prove a statement stronger than Theorem 1.3. To state this result, we need some notation. For each prime p , let Σ_p be a closed subset of $\mathbb{Z}_p^2 \setminus \{\Delta \neq 0\}$ whose boundary has measure 0. To such a collection $(\Sigma_p)_p$, we associate the set F_Σ of elliptic curves over \mathbb{Q} , where $E^{I,J} \in F_\Sigma$ if and only if $(I, J) \in \Sigma_p$ for all p . We then say that F_Σ is a family of elliptic curves over \mathbb{Q} that is *defined by congruence conditions*. We can also impose ‘‘congruence conditions at infinity’’ on F_Σ by insisting that an elliptic curve $E^{I,J}$ belongs to F_Σ if and only if (I, J) belongs to Σ_∞ , where Σ_∞ is equal to $\{(I, J) \in \mathbb{R}^2 : \Delta(I, J) > 0\}$, $\{(I, J) \in \mathbb{R}^2 : \Delta(I, J) < 0\}$, or $\{(I, J) \in \mathbb{R}^2 : \Delta(I, J) \neq 0\}$.

If F is any nonempty family of elliptic curves over \mathbb{Q} defined by congruence conditions, then let $\text{Inv}(F)$ denote the set $\{(I(E), J(E)) : E \in F\}$. We define $\text{Inv}_p(F)$ to be the set of those elements (I, J) in the p -adic closure of $\text{Inv}(F) \subset \mathbb{Z}_p^2$ such that $\Delta(I, J) := (4I^3 - J^2)/27 \neq 0$. Also, we define $\text{Inv}_\infty(F)$ by $\{(I, J) \in \mathbb{R}^2 : \Delta(I, J) > 0\}$, $\{(I, J) \in \mathbb{R}^2 : \Delta(I, J) < 0\}$, or $\{(I, J) \in \mathbb{R}^2 : \Delta(I, J) \neq 0\}$ in accordance with whether F contains only curves of positive discriminant, negative discriminant, or both. A family F of elliptic curves defined by congruence conditions is then said to be *large* if, for all but finitely many primes p , the set $\text{Inv}_p(F)$ contains all pairs $(I, J) \in \mathbb{Z}_p \times \mathbb{Z}_p$ such that $p^2 \nmid \Delta(I, J)$. In this section, we prove the following strengthening of Theorem 1.3.

Theorem 3.1 *When all elliptic curves E in any large family are ordered by height, the average size of the 2-Selmer group $S_2(E)$ is 3.*

Note that the family of all elliptic curves is large. So too is the family of elliptic curves $E : y^2 = g(x)$ defined by finitely many congruence conditions on the coefficients of g . Thus Theorems 1.1 and 1.3 indeed follow from Theorem 3.1. Finally, we note that the family of all semistable elliptic curves is also large.

3.1 Preliminaries on binary quartic forms and 2-coverings of elliptic curves

The key to proving Theorem 3.1 is the use of a classical correspondence between elements in the 2-Selmer group of an elliptic curve $E^{I,J}$ over \mathbb{Q} and locally soluble integral binary quartic forms having invariants 2^4I and 2^6J . This correspondence was originally introduced by Birch and Swinnerton-Dyer [9], and was developed further by Cremona [13] (see also [16], [15], and [7]). We collect here the results that we will need on this correspondence. Throughout this section, we use the action of PGL_2 on V as defined by (32).

We say that a binary quartic form over a field K is K -soluble if the equation $z^2 = f(x, y)$ has a solution with $x, y, z \in K$ and $(x, y) \neq (0, 0)$. The first paragraph of the following theorem is contained in [16, Proposition 2.2], while the second follows from [15, §3–5 and Remark 1]. (For more details, see [7, §4.1].)

Theorem 3.2 *Let K be a field having characteristic not 2 or 3. Let $E : y^2 = x^3 - \frac{I}{3}x - \frac{J}{27}$ be an elliptic curve over K . Then there exists a bijection between elements in $E(K)/2E(K)$ and $\mathrm{PGL}_2(K)$ -orbits of K -soluble binary quartic forms having invariants I and J , given by*

$$(\xi, \eta) + 2E(K) \mapsto \mathrm{PGL}_2(K) \cdot \left(\frac{1}{4}x^4 - \frac{3}{2}\xi x^2y^2 + 2\eta xy^3 + \left(\frac{I}{3} - \frac{3}{4}\xi^2 \right) y^4 \right).$$

Under this bijection, the identity element in $E(K)/2E(K)$ corresponds to the $\mathrm{PGL}_2(K)$ -orbit of binary quartic forms having a linear factor over K .

Furthermore, the stabilizer in $\mathrm{PGL}_2(K)$ of any (not necessarily K -soluble) binary quartic form f in V_K , having nonzero discriminant and invariants I and J , is isomorphic to $E(K)[2]$, where E is the elliptic curve defined by $y^2 = x^3 - \frac{I}{3}x - \frac{J}{27}$.

Next, recall that a binary quartic form $f \in V_{\mathbb{Q}}$ is called *locally soluble* if f is \mathbb{R} -soluble and \mathbb{Q}_p -soluble for all primes p . We then have the following proposition (see [9, Lemma 2] and the discussion following it).

Proposition 3.3 *Let $E : y^2 = x^3 - \frac{I}{3}x - \frac{J}{27}$ be an elliptic curve over \mathbb{Q} . Then there exists a bijection between isomorphism classes of locally soluble 2-coverings of E and $\mathrm{PGL}_2(\mathbb{Q})$ -orbits of locally soluble binary quartic forms in $V_{\mathbb{Q}}$ having invariants I and J .*

Furthermore, the set of rational binary quartic forms having a rational linear factor and invariants equal to I and J lie in a single $\mathrm{PGL}_2(\mathbb{Q})$ -orbit, and this orbit corresponds to the identity element in the 2-Selmer group of E .

In order to prove Theorem 3.1, we will also require the following lemma, which follows from Lemmas 3, 4, and 5 of [9].

Lemma 3.4 *Let $f \in V_{\mathbb{Q}}$ be a locally soluble binary quartic form having integral invariants I and J such that $(2^4 \cdot 3) \mid I$ and $(2^6 \cdot 3^3) \mid J$. Then f is $\mathrm{PGL}_2(\mathbb{Q})$ -equivalent to an integral binary quartic form.*

Since $E = E^{I,J}$ is also isomorphic to the elliptic curve defined by $y^2 = x^3 - \frac{2^4I(E)}{3}x - \frac{2^6J(E)}{27}$, Proposition 3.3 and Lemma 3.4 now imply the following theorem:

Theorem 3.5 *Let $E = E^{I,J}$ be an elliptic curve over \mathbb{Q} . Then the elements of the 2-Selmer group of E are in one-to-one correspondence with $\mathrm{PGL}_2(\mathbb{Q})$ -equivalence classes of locally soluble integral binary quartic forms having invariants equal to 2^4I and 2^6J .*

Furthermore, the set of integral binary quartic forms that have a rational linear factor and invariants equal to 2^4I and 2^6J lie in one $\mathrm{PGL}_2(\mathbb{Q})$ -equivalence class, and this class corresponds to the identity element in the 2-Selmer group of E .

3.2 A weighted set $S(F)$ of integral binary quartic forms associated to a large family F of elliptic curves

Theorem 3.5 asserts that nonidentity elements in the 2-Selmer group of an elliptic curve $E^{I,J}$ over \mathbb{Q} are in bijective correspondence with $\mathrm{PGL}_2(\mathbb{Q})$ -equivalence classes of locally soluble integral binary quartic forms

having invariants 2^4I and 2^6J that do not possess a rational linear factor. In §2, we computed the asymptotic number of $\mathrm{GL}_2(\mathbb{Z})$ -orbits of irreducible integral binary quartic forms having bounded height. By Lemma 2.3, the number of $\mathrm{GL}_2(\mathbb{Z})$ -orbits of binary quartic forms of bounded height that are the product of two irreducible integral binary quadratic forms is negligible. Furthermore, $\mathrm{GL}_2(\mathbb{Z})$ -orbits on $V_{\mathbb{Z}}$ are exactly the same as $\mathrm{PGL}_2(\mathbb{Z})$ -orbits on $V_{\mathbb{Z}}$. Therefore, the same asymptotic formula in Theorem 3.5 holds also for the number of $\mathrm{PGL}_2(\mathbb{Z})$ -orbits of integral binary quartic forms having bounded height and no rational linear factor.

In order to adapt the latter results to compute the number of $\mathrm{PGL}_2(\mathbb{Q})$ -equivalence classes of locally soluble integral binary quartic forms having bounded height and no rational linear factor, we need to count each $\mathrm{PGL}_2(\mathbb{Z})$ orbit, $\mathrm{PGL}_2(\mathbb{Z}) \cdot f$, weighted by $1/n(f)$, where $n(f)$ is equal to the number of $\mathrm{PGL}_2(\mathbb{Z})$ -orbits inside the $\mathrm{PGL}_2(\mathbb{Q})$ -equivalence class of f in $V_{\mathbb{Z}}$. For this purpose, it suffices to count the number of $\mathrm{PGL}_2(\mathbb{Z})$ -orbits of locally soluble integral binary quartic forms having bounded height and no rational linear factor where each orbit $\mathrm{PGL}_2(\mathbb{Z}) \cdot f$ is weighted by $1/m(f)$, where

$$m(f) := \sum_{f' \in B(f)} \frac{\#\mathrm{Aut}_{\mathbb{Q}}(f')}{\#\mathrm{Aut}_{\mathbb{Z}}(f')} = \sum_{f' \in B(f)} \frac{\#\mathrm{Aut}_{\mathbb{Q}}(f)}{\#\mathrm{Aut}_{\mathbb{Z}}(f')},$$

here $B(f)$ denotes a set of representatives for the action of $\mathrm{PGL}_2(\mathbb{Z})$ on the $\mathrm{PGL}_2(\mathbb{Q})$ -equivalence class of f in $V_{\mathbb{Z}}$, and $\mathrm{Aut}_{\mathbb{Q}}(f)$ (resp. $\mathrm{Aut}_{\mathbb{Z}}(f)$) denotes the stabilizer of f in $\mathrm{PGL}_2(\mathbb{Q})$ (resp. $\mathrm{PGL}_2(\mathbb{Z})$). The reason it suffices to weight by $1/m(f)$ instead of $1/n(f)$ is that, by Lemma 2.4, all but a negligible number of $\mathrm{PGL}_2(\mathbb{Z})$ -orbits of integral binary quartic forms with nonzero discriminant and bounded height have trivial stabilizer in $\mathrm{PGL}_2(\mathbb{Q})$; thus all but a negligible number of $\mathrm{PGL}_2(\mathbb{Z})$ -equivalence classes of integral binary quartic forms with nonzero discriminant and bounded height satisfy $m(f) = n(f)$.

Let us use $S(F)$ to denote the set of all locally soluble integral binary quartic forms having invariants 2^4I and 2^6J , where $(I, J) \in \mathrm{Inv}(F)$. Assign to each element $f \in S(F)$ the weight $1/m(f)$. Then we conclude that the weighted number of irreducible $\mathrm{PGL}_2(\mathbb{Z})$ -orbits of height less than X in $S(F)$ is asymptotically equal to the number of nonidentity 2-Selmer elements of all elliptic curves of height less than X in F . In the remainder of this section, our goal is therefore to count the weighted number of irreducible orbits in $S(F)$ having bounded height.

The global weights $m(f)$ (as opposed to $n(f)$) are useful for the following reason. For a prime p and a binary quartic form $f \in V_{\mathbb{Z}_p}$, define $m_p(f)$ by

$$m_p(f) := \sum_{f' \in B_p(f)} \frac{\#\mathrm{Aut}_{\mathbb{Q}_p}(f')}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f')} = \sum_{f' \in B_p(f)} \frac{\#\mathrm{Aut}_{\mathbb{Q}_p}(f)}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f')},$$

where $B_p(f)$ denotes a set of representatives for the action of $\mathrm{PGL}_2(\mathbb{Z}_p)$ on the $\mathrm{PGL}_2(\mathbb{Q}_p)$ -equivalence class of f in $V_{\mathbb{Z}_p}$, and $\mathrm{Aut}_{\mathbb{Q}_p}(f)$ (resp. $\mathrm{Aut}_{\mathbb{Z}_p}(f)$) denotes the stabilizer of f in $\mathrm{PGL}_2(\mathbb{Q}_p)$ (resp. $\mathrm{PGL}_2(\mathbb{Z}_p)$).

Then we have the following proposition:

Proposition 3.6 *Suppose $f \in V_{\mathbb{Z}}$ has nonzero discriminant. Then $m(f) = \prod_p m_p(f)$.*

Proof: Let $\mathrm{PGL}_2(\mathbb{Q})_f$ (resp. $\mathrm{PGL}_2(\mathbb{Q}_p)_f$) denote the set of elements $\gamma \in \mathrm{PGL}_2(\mathbb{Q})$ (resp. $\mathrm{PGL}_2(\mathbb{Q}_p)$) such that $\gamma \cdot f \in V_{\mathbb{Z}}$ (resp. $V_{\mathbb{Z}_p}$). Then we have a natural map from $\mathrm{PGL}_2(\mathbb{Q})_f$ to the set of $\mathrm{PGL}_2(\mathbb{Z})$ -orbits on the $\mathrm{PGL}_2(\mathbb{Q})$ -equivalence class of f in $V_{\mathbb{Z}}$ via $\gamma \mapsto \mathrm{PGL}_2(\mathbb{Z})\gamma \cdot f$. Two elements in $\mathrm{PGL}_2(\mathbb{Q})_f$ map to the same orbit if and only if they map to the same element in the double coset space

$$\mathrm{PGL}_2(\mathbb{Z}) \backslash \mathrm{PGL}_2(\mathbb{Q})_f / \mathrm{Aut}_{\mathbb{Q}}(f).$$

Thus, the number of elements in $\mathrm{PGL}_2(\mathbb{Z}) \backslash \mathrm{PGL}_2(\mathbb{Q})_f$ that map to a fixed orbit $\mathrm{PGL}_2(\mathbb{Z}) \cdot f'$ is equal to $\#\mathrm{Aut}_{\mathbb{Q}}(f) / \#\mathrm{Aut}_{\mathbb{Z}}(f')$, implying that

$$\#[\mathrm{PGL}_2(\mathbb{Z}) \backslash \mathrm{PGL}_2(\mathbb{Q})_f] = \sum_{f' \in B(f)} \frac{\#\mathrm{Aut}_{\mathbb{Q}}(f)}{\#\mathrm{Aut}_{\mathbb{Z}}(f')} = m(f).$$

Similarly, we have that

$$\#[\mathrm{PGL}_2(\mathbb{Z}_p)\backslash\mathrm{PGL}_2(\mathbb{Q}_p)_f] = \sum_{f' \in B_p(f)} \frac{\#\mathrm{Aut}_{\mathbb{Q}_p}(f)}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f')} = m_p(f).$$

Now we consider the map

$$\tau : \mathrm{PGL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2(\mathbb{Q})_f \rightarrow \prod_p \mathrm{PGL}_2(\mathbb{Z}_p)\backslash\mathrm{PGL}_2(\mathbb{Q}_p)_f$$

given by the diagonal embedding. Since $\mathrm{PGL}_2(\mathbb{Q}_p)_f = \mathrm{PGL}_2(\mathbb{Z}_p)$ for all primes p not dividing the discriminant of f (see the proof of Proposition 3.18 for a stronger result), the product $\prod_p \mathrm{PGL}_2(\mathbb{Z}_p)\backslash\mathrm{PGL}_2(\mathbb{Q}_p)_f$ is in fact a finite product. It is easy to see that τ is well-defined and injective. (For injectivity, note that if γ_1 and γ_2 are elements in $\mathrm{PGL}_2(\mathbb{Q})_f$ that map to the same element under τ , then $\gamma_1\gamma_2^{-1}$ is an element of $\mathrm{PGL}_2(\mathbb{Q})$ and of $\mathrm{PGL}_2(\mathbb{Z}_p)$ for all p . This implies that $\gamma_1\gamma_2^{-1} \in \mathrm{PGL}_2(\mathbb{Z})$, as desired.)

The group $\mathrm{PGL}_2(\mathbb{Q})$ has class number 1 (see [35, Chapter 8]). Hence if $\sigma \in \prod_p \mathrm{PGL}_2(\mathbb{Z}_p)\backslash\mathrm{PGL}_2(\mathbb{Q}_p)_f$, then there exists an element $\gamma \in \mathrm{PGL}_2(\mathbb{Q})$ such that γ maps to σ under the diagonal embedding. Since $\gamma \cdot f \in V_{\mathbb{Z}_p}$ for all p , we see that $\gamma \cdot f \in V_{\mathbb{Z}}$, implying $\gamma \in \mathrm{PGL}_2(\mathbb{Q})_f$. Thus τ is surjective, completing the proof of the proposition. \square

Thus the global weights of elements in $S(F)$ are products of local weights, and so we may express the global weighted density of the set $S(F)$ in $V_{\mathbb{Z}}$ as a product of local weighted densities of the closures of $S(F)$ in $V_{\mathbb{Z}_p}$. We compute these local densities next, in terms of local masses of 2-coverings of elliptic curves.

3.3 Local densities of the weighted set $S(F)$ in terms of local masses of 2-coverings of elliptic curves in F

Let F be a large family of elliptic curves. Let $S(F)$ again denote the set of all locally soluble integral binary quartic forms having invariants 2^4I and 2^6J where $(I, J) \in \mathrm{Inv}(F)$, and let $S_p(F)$ denote the p -adic closure of $S(F)$ in $V_{\mathbb{Z}_p}$. We now determine the p -adic density of $S_p(F)$, where each element $f \in S_p(F)$ is weighted by $1/m_p(f)$, in terms of a *local (p -adic) mass* $M_p(V, F)$ involving all isomorphism classes of soluble 2-coverings of elliptic curves over \mathbb{Q}_p whose invariants lie in $\mathrm{Inv}_p(F)$. To do so we need the following proposition, which is a reformulation of the change-of-measure assertion of Proposition 2.8 with \mathbb{Z}_p in place of \mathbb{R} ; we postpone the proof to §3.4.

Proposition 3.7 *Let p be a prime, and let ϕ be a continuous function on $V_{\mathbb{Z}_p}$. Then*

$$\int_{V_{\mathbb{Z}_p}} \phi(f)df = \left| \frac{1}{27} \right|_p \int_{\substack{(I, J) \in \mathbb{Z}_p^2 \\ \Delta(I, J) \neq 0}} \left(\sum_{\substack{f \in \frac{V_{\mathbb{Z}_p}(I, J)}{\mathrm{PGL}_2(\mathbb{Z}_p)}}} \frac{1}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f)} \int_{g \in \mathrm{PGL}_2(\mathbb{Z}_p)} \phi(g \cdot f)\omega(g) \right) dIdJ, \quad (50)$$

where $\frac{V_{\mathbb{Z}_p}(I, J)}{\mathrm{PGL}_2(\mathbb{Z}_p)}$ denotes a set of representatives for the action of $\mathrm{PGL}_2(\mathbb{Z}_p)$ on elements in $V_{\mathbb{Z}_p}$ having invariants I and J .

In certain special cases where $\phi(f)$ is additionally weighted by $1/m_p(f)$, Equation (50) takes on a particularly nice form:

Corollary 3.8 *Let p be a prime and let ϕ be a continuous $\mathrm{PGL}_2(\mathbb{Q}_p)$ -invariant function on $V_{\mathbb{Z}_p}$ such that every element $f \in V_{\mathbb{Z}_p}$ in the support of ϕ has nonzero discriminant, is soluble, and satisfies $2^4 \cdot 3 \mid I(f)$ and $2^6 \cdot 3^3 \mid J(f)$. Then*

$$\int_{V_{\mathbb{Z}_p}} \frac{\phi(f)}{m_p(f)} df = \left| \frac{1}{27} \right|_p \mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z}_p)) \int_{\substack{(I, J) \in \mathbb{Z}_p^2 \\ \Delta(I, J) \neq 0}} \frac{1}{\#E[2](\mathbb{Q}_p)} \left(\sum_{\sigma \in E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)} \phi(f_\sigma) \right) dIdJ, \quad (51)$$

where f_σ is any element in $V_{\mathbb{Z}_p}$ that corresponds to σ under the correspondence of Theorem 3.2. (The existence of such an $f_\sigma \in V_{\mathbb{Z}_p}$ is the content of Lemma 3.4.)

Proof: Proposition 3.7 implies that we have

$$\begin{aligned} \int_{V_{\mathbb{Z}_p}} \frac{\phi(f)}{m_p(f)} df &= \left| \frac{1}{27} \right|_p \int_{\substack{(I,J) \in \mathbb{Z}_p^2 \\ \Delta(I,J) \neq 0}} \left(\sum_{\substack{f \in \frac{V_{\mathbb{Z}_p}(I,J)}{\mathrm{PGL}_2(\mathbb{Z}_p)}}} \frac{1}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f)} \int_{g \in \mathrm{PGL}_2(\mathbb{Z}_p)} \frac{\phi(g \cdot f)}{m_p(g \cdot f)} dg \right) dIdJ \\ &= \left| \frac{1}{27} \right|_p \mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z}_p)) \int_{\substack{(I,J) \in \mathbb{Z}_p^2 \\ \Delta(I,J) \neq 0}} \left(\sum_{\substack{f \in \frac{V_{\mathbb{Z}_p}(I,J)}{\mathrm{PGL}_2(\mathbb{Z}_p)}}} \frac{\phi(f)}{m_p(f) \#\mathrm{Aut}_{\mathbb{Z}_p}(f)} \right) dIdJ, \end{aligned} \quad (52)$$

since both ϕ and m_p are $\mathrm{PGL}_2(\mathbb{Z}_p)$ -invariant. We now evaluate the sum within the integral in the second line of (52). For $f \in V_{\mathbb{Z}_p}$, let $f = f_1, f_2, \dots, f_k$ be the set of all elements in $\frac{V_{\mathbb{Z}_p}(I,J)}{\mathrm{PGL}_2(\mathbb{Z}_p)}$ that are $\mathrm{PGL}_2(\mathbb{Q}_p)$ -equivalent to f . Then since ϕ and m_p are $\mathrm{PGL}_2(\mathbb{Q}_p)$ -invariant, we have

$$\begin{aligned} \sum_{i=1}^k \frac{\phi(f_i)}{m_p(f_i) \#\mathrm{Aut}_{\mathbb{Z}_p}(f_i)} &= \frac{\phi(f)}{m_p(f)} \sum_{i=1}^k \frac{1}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f_i)} = \phi(f) \left(\sum_{i=1}^k \frac{\#\mathrm{Aut}_{\mathbb{Q}_p}(f)}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f_i)} \right)^{-1} \sum_{i=1}^k \frac{1}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f_i)} \\ &= \frac{\phi(f)}{\#\mathrm{Aut}_{\mathbb{Q}_p}(f)}. \end{aligned}$$

Therefore, we obtain

$$\int_{V_{\mathbb{Z}_p}} \frac{\phi(f)}{m_p(f)} df = \left| \frac{1}{27} \right|_p \mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z}_p)) \int_{\substack{(I,J) \in \mathbb{Z}_p^2 \\ \Delta(I,J) \neq 0}} \left(\sum_{\substack{f \in \frac{V_{\mathbb{Z}_p}(I,J)}{\mathrm{PGL}_2(\mathbb{Q}_p)}}} \frac{\phi(f)}{\#\mathrm{Aut}_{\mathbb{Q}_p}(f)} \right) dIdJ, \quad (53)$$

where $\frac{V_{\mathbb{Z}_p}(I,J)}{\mathrm{PGL}_2(\mathbb{Q}_p)}$ analogously denotes a set consisting of one element from each $\mathrm{PGL}_2(\mathbb{Q})$ -equivalence class in $V_{\mathbb{Z}_p}$ having invariants I and J . Theorem 3.2 and Lemma 3.4 imply that soluble elements in $\frac{V_{\mathbb{Z}_p}(I,J)}{\mathrm{PGL}_2(\mathbb{Q}_p)}$ are in bijective correspondence with elements in $E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)$. Theorem 3.2 further states that $\mathrm{Aut}_{\mathbb{Q}_p}(f)$ is isomorphic to $E^{I(f),J(f)}[2](\mathbb{Q}_p)$. Therefore, Corollary 3.8 follows from (53). \square

We now have the following proposition which determines the necessary local p -adic masses.

Proposition 3.9 *We have*

$$\int_{S_p(F)} \frac{1}{m_p(f)} df = |2^{10}/27|_p \cdot \mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z}_p)) \cdot M_p(V, F),$$

where

$$M_p(V, F) := \int_{(I,J) \in \mathrm{Inv}_p(F)} \frac{\#(E^{I,J}(\mathbb{Q}_p)/2E^{I,J}(\mathbb{Q}_p))}{\#E^{I,J}(\mathbb{Q}_p)[2]} dIdJ. \quad (54)$$

Proof: The set $S_p(F)$ consists of all \mathbb{Q}_p -soluble binary quartic forms having invariants 2^4I and 2^6J with $(I, J) \in \mathrm{Inv}_p(F)$. Proposition 3.9 thus follows directly from Corollary 3.8 since $E^{I,J}(\mathbb{Q}_p)$ is isomorphic to $E^{2^4I, 2^6J}(\mathbb{Q}_p)$ and the volume of $\{(2^4I, 2^6J) | (I, J) \in \mathrm{Inv}_p(F)\} = |2^{10}|_p \cdot \mathrm{Vol}(\mathrm{Inv}_p(F))$. \square

3.4 A change-of-measure formula

In this subsection, our aim is to prove the change-of-variables formula that is contained in Proposition 2.8 and Proposition 3.7 over \mathbb{R} and over \mathbb{Q}_p , respectively. We begin by proving first the following result over \mathbb{C} :

Proposition 3.10 *Let ω , dv , and $dIdJ$ be as in Proposition 2.8. Let $R \subset \mathbb{C}^2$ be an open set and $s : R \rightarrow V_{\mathbb{C}}$ be a continuous function such that the binary quartic form $s_{I,J} := s(I, J)$ has invariants equal to I and J*

for each $(I, J) \in R$. Then there exists a nonzero rational number \mathcal{J} such that for any measurable function $\phi : V_{\mathbb{C}} \rightarrow \mathbb{R}$, we have

$$\int_{v \in \mathrm{PGL}_2(\mathbb{C}) \cdot s(R)} \phi(v) dv = |\mathcal{J}| \int_R \int_{\mathrm{PGL}_2(\mathbb{C})} \phi(g \cdot s_{I,J}) \omega(g) dIdJ,$$

where we regard $\mathrm{PGL}_2(\mathbb{C}) \cdot s(R)$ as a multiset.

Proof: Let us begin with the special case when the function s is locally analytic. Then we know that

$$\int_{v \in \mathrm{PGL}_2(\mathbb{C}) \cdot s(R)} \phi(v) dv = \int_{(I,J) \in \mathbb{C}^2} \int_{\mathrm{PGL}_2(\mathbb{C})} \mathcal{J}_s(g, I, J) \phi(g \cdot s_{I,J}) \omega(g) dIdJ, \quad (55)$$

where $\mathcal{J}_s(g, I, J)$ is the Jacobian change of variables of the map

$$\begin{aligned} \psi_s : \mathrm{PGL}_2(\mathbb{C}) \times R &\rightarrow V_{\mathbb{C}} \\ (g, (I, J)) &\mapsto g \cdot s_{I,J}. \end{aligned} \quad (56)$$

Note that $\mathcal{J}_s(g, I, J)$ is continuous in g, I , and J . In what follows, we prove that $\mathcal{J}_s(g, I, J)$ is independent of g, I, J , and s .

Step 1: $\mathcal{J}_s(g, I, J)$ is independent of $g \in \mathrm{PGL}_2(\mathbb{C})$.

Suppose there exists $(I, J) \in R$ and $g_1, g_2 \in \mathrm{PGL}_2(\mathbb{C})$ such that $\mathcal{J}_s(g_1, I, J) \neq \mathcal{J}_s(g_2, I, J)$. Then, by continuity and the fact that $\omega(g)$ is $\mathrm{PGL}_2(\mathbb{C})$ -invariant, there exists an open set $B_1 \subset \mathrm{PGL}_2(\mathbb{C})$ containing g_1 such that $\int_{B_1} \mathcal{J}_s(g, I, J) \omega(g) \neq \int_{g_2 g_1^{-1} B_1} \mathcal{J}_s(g, I, J) \omega(g)$. By continuity, there then exists an open set $N \subset R$ containing (I, J) such that

$$\int_{(I,J) \in N} \int_{B_1} \mathcal{J}_s(g, I, J) \omega(g) dIdJ \neq \int_{(I,J) \in N} \int_{g_2 g_1^{-1} B_1} \mathcal{J}_s(g, I, J) \omega(g) dIdJ. \quad (57)$$

From (55) it follows that the left hand side of (57) is equal to the volume of $B_1 \cdot N$ while the right hand side of (57) is equal to the volume of $g_2 g_1^{-1} B_1 \cdot N$. Since the map $g_2 g_1^{-1} : V_{\mathbb{C}} \rightarrow V_{\mathbb{C}}$ is via an element in $\mathrm{SL}(V_{\mathbb{C}})$, we obtain the desired contradiction.

Step 2: $\mathcal{J}_s(I, J) := \mathcal{J}_s(g, I, J)$ is independent of s .

Let $s' : R \rightarrow V_{\mathbb{C}}$ be another locally analytic function such that the invariants of $s'_{I,J} := s'(I, J)$ are I and J for each $(I, J) \in R$. Since $\mathrm{PGL}_2(\mathbb{C}) \cdot s(R)$ and $\mathrm{PGL}_2(\mathbb{C}) \cdot s'(R)$ are the same multisets, we have

$$\int_{v \in \mathrm{PGL}_2(\mathbb{C}) \cdot s'(R)} \phi(v) dv = \int_{v \in \mathrm{PGL}_2(\mathbb{C}) \cdot s(R)} \phi(v) dv = \int_{(I,J) \in \mathbb{C}^2} \int_{\mathrm{PGL}_2(\mathbb{C})} \mathcal{J}_s(I, J) \phi(g \cdot s_{I,J}) \omega(g) dIdJ.$$

For each $(I, J) \in \mathbb{C}^2$ let $g_{I,J} \in \mathrm{PGL}_2(\mathbb{C})$ be such that $g_{I,J} \cdot s_{I,J} = s'_{I,J}$. Then, because $\omega(g)$ is both a left and a right Haar-measure, we obtain

$$\begin{aligned} \int_{(I,J) \in \mathbb{C}^2} \int_{g \in \mathrm{PGL}_2(\mathbb{C})} \mathcal{J}_s(I, J) \phi(g \cdot s_{I,J}) \omega(g) dIdJ &= \int_{\mathbb{C}^2} \int_{\mathrm{PGL}_2(\mathbb{C})} \mathcal{J}_s(I, J) \phi(g g_{I,J} \cdot s_{I,J}) \omega(g) dIdJ \\ &= \int_{\mathbb{C}^2} \int_{\mathrm{PGL}_2(\mathbb{C})} \mathcal{J}_s(g, I, J) \phi(g \cdot s'_{I,J}) \omega(g) dIdJ. \end{aligned}$$

Hence it follows that

$$\int_{v \in \mathrm{PGL}_2(\mathbb{C}) \cdot s'(R)} \phi(v) dv = \int_{(I,J) \in \mathbb{C}^2} \int_{\mathrm{PGL}_2(\mathbb{C})} \mathcal{J}_s(I, J) \phi(g \cdot s'_{I,J}) \omega(g) dIdJ.$$

Thus $\mathcal{J}_{s'}(I, J) = \mathcal{J}_s(I, J)$ as desired.

Step 3: $\mathcal{J}(I, J) := \mathcal{J}_s(I, J)$ is a nonzero polynomial in I and J with rational coefficients.

We can choose s such that the coefficients of $s_{I,J}$ are rational polynomials in I and J ; for example, let $s_{I,J} := x^3y - \frac{I}{3}xy^3 - \frac{J}{27}y^4$. Since $\mathcal{J}(I, J)$ is the determinant of a 5×5 matrix whose entries are polynomials in the coefficients of $s_{I,J}$, it follows that $\mathcal{J}(I, J)$ is a rational polynomial in I and J . Because $\psi_s(\mathrm{PGL}_2(\mathbb{C}), \mathbb{C}^2)$ is a full measure set in $V_{\mathbb{C}}$, we obtain that $\mathcal{J}(I, J)$ is nonzero.

Step 4: $\mathcal{J} := \mathcal{J}(I, J)$ is a nonzero rational constant.

Let $G_0 \subset \mathrm{PGL}_2(\mathbb{C})$ be a bounded subset having volume 1 and let R_0 be any bounded measurable set in \mathbb{C}^2 . We denote the set of all elements $s_{I,J}$ with $(I, J) \in R_0$ by $B = B(R_0)$. Then

$$\int_{G_0 \cdot B} dv = \int_{(I,J) \in R_0} \mathcal{J}(I, J) dIdJ, \quad (58)$$

where we view $G_0 \cdot B$ as a multiset. Now for any $c \in \mathbb{C}$, we have by (58) that

$$\int_{cG_0 \cdot B} dv = |c|^5 \int_{G_0 \cdot B} dv = |c|^5 \int_{(I,J) \in R_0} \mathcal{J}(I, J) dIdJ \quad (59)$$

because $V_{\mathbb{C}}$ has dimension 5. On the other hand, we may evaluate the left hand side of (59) in another way; namely, using (58) with cB in place of B , we obtain

$$\int_{cG_0 \cdot B} dv = \int_{G_0 \cdot cB} dv = \int_{(c^{-2}I, c^{-3}J) \in R_0} \mathcal{J}(I, J) dIdJ = \int_{(I', J') \in R_0} \mathcal{J}(c^2I', c^3J') |c^2| dI' |c^3| dJ' \quad (60)$$

because I and J are homogeneous polynomials of degree 2 and 3, respectively. Comparing the right hand sides of (59) and (60), we obtain

$$\int_{(I,J) \in R_0} \mathcal{J}(I, J) dIdJ = \int_{(I,J) \in R_0} \mathcal{J}(c^2I, c^3J) dIdJ. \quad (61)$$

Since, by Step 3, $\mathcal{J}(I, J)$ is a nonzero polynomial in I and J having rational coefficients, and since the equality (61) is true for all R_0 and all c , we conclude that $\mathcal{J}(I, J)$ must be a nonzero rational constant.

Finally, as every continuous function can be locally uniformly approximated as closely as desired by locally analytic functions (by the Stone–Weierstrass theorem), the proposition follows. \square

Proposition 2.8, with $1/27$ replaced by \mathcal{J} , now follows from Proposition 3.10 and the principle of permanence of identities. More generally, we have obtained the following result:

Proposition 3.11 *Let K be \mathbb{R} , \mathbb{C} , or \mathbb{Z}_p for some prime p . Let dv be the standard additive measure on V_K , the space of all binary quartic forms with coefficients in K . Let R be an open subset of $K \times K$ and let $s : R \rightarrow V_K$ be a continuous function such that the invariants of $s_{I,J} := s(I, J)$ are I and J . Then there exists a rational nonzero constant \mathcal{J} such that for any measurable function ϕ on V_K , we have*

$$\int_{v \in \mathrm{PGL}_2(K) \cdot s(R)} \phi(v) dv = |\mathcal{J}| \int_R \int_{\mathrm{PGL}_2(K)} \phi(g \cdot s_{I,J}) \omega(g) dIdJ, \quad (62)$$

where we regard $\mathrm{PGL}_2(K) \cdot s(R)$ as a multiset, ω is as defined in Section 2.4, and $|\mathcal{J}|$ denotes the usual absolute value of \mathcal{J} as an element of K .

We next wish to prove the statement of Proposition 3.7, with $1/27$ replaced by \mathcal{J} . To do this, because every continuous function on $V_{\mathbb{Z}_p}$ is locally constant outside a set of arbitrarily small measure, we may assume that ϕ is locally constant. Also, it suffices to prove the statement locally; i.e., for every element $f \in V_{\mathbb{Z}_p}$ (we may also assume that $\Delta(f) \neq 0$) there exists a neighborhood B_f of f such that (50), with $1/27$ replaced by \mathcal{J} , is true when ϕ is the characteristic function of B_f .

Given $f \in V_{\mathbb{Z}_p} \setminus \{\Delta = 0\}$, we now construct such a neighborhood B_f . Let $P \subset V_{\mathbb{Z}_p}$ be a generic 2-dimensional plane passing through f defined by linear equations over \mathbb{Q} ; then there exists a neighborhood $P_0 \subset P$ of f such that the invariants of any two elements in P_0 are distinct in \mathbb{Z}_p^2 and the size of the stabilizers in $\mathrm{PGL}_2(\mathbb{Z}_p)$ of any two elements in P_0 are equal. The first claim in the previous statement follows from the inverse function theorem for local fields (see [38, Proposition 4.3]) used on the usual map from $\mathrm{PGL}_2(\mathbb{Z}_p) \times P$ to $V_{\mathbb{Z}_p}$. Then we define B_f to be $\mathrm{PGL}_2(\mathbb{Z}_p) \cdot P_0$ (regarded as a set, not a multiset). Since the plane P was defined by linear equations over \mathbb{Q} , Proposition 3.10 and the principle of permanence of identities implies that

$$\#\mathrm{Aut}_{\mathbb{Z}_p}(f) \cdot \mathrm{Vol}(B_f) = |\mathcal{J}|_p \cdot \mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z}_p)) \cdot \int_{\mathrm{Inv}_p(P_0)} dIdJ,$$

where $\mathrm{Inv}_p(P_0)$ denotes the set of all $(I, J) \in \mathbb{Z}_p^2$ that occur as invariants of some element in P_0 . We have thus proven Proposition 3.7, with $1/27$ replaced by \mathcal{J} . In fact, our argument yields the following result:

Proposition 3.12 *Let K be \mathbb{R} , \mathbb{C} , or \mathbb{Z}_p for some prime p , and let ϕ be a measurable function on V_K . Then there exists a rational constant \mathcal{J} , independent of K and ϕ , such that*

$$\int_{V_K} \phi(f) df = |\mathcal{J}| \int_{\substack{(I,J) \in K^2 \\ \Delta(I,J) \neq 0}} \left(\sum_{\substack{f \in V_K(I,J) \\ f \in \mathrm{PGL}_2(K)}} \frac{1}{\#\mathrm{Aut}_K(f)} \int_{g \in \mathrm{PGL}_2(K)} \phi(g \cdot f) \omega(g) \right) dIdJ, \quad (63)$$

where $\frac{V_K(I,J)}{\mathrm{PGL}_2(K)}$ denotes a set of representatives for the action of $\mathrm{PGL}_2(K)$ on elements in V_K having invariants I and J .

To complete the proof of Proposition 3.7, it only remains to show that the absolute value of \mathcal{J} is equal to $1/27$. We accomplish this by computing the value of $|\mathcal{J}|_p$ for each prime p . Namely, for each prime p , we pick an appropriate set $S \subset V_{\mathbb{Z}_p}$, and then use (62) to express $|\mathcal{J}|_p$ in terms of the volume of S . We then consider \bar{S} , the reduction of S modulo p , and determine its cardinality to explicitly compute the volume of S , and thereby determine the value of $|\mathcal{J}|_p$.

To this end, we have the following proposition.

Proposition 3.13 *Let p be a fixed prime number. Let $S \subset V_{\mathbb{Z}_p}$ be a set defined by congruence conditions modulo p , and let $\bar{S} \subset V_{\mathbb{F}_p}$ denote the reduction of S modulo p . Assume that $S = \pi^{-1}(\pi(S))$, where π is given by taking invariants. Then*

$$|\mathcal{J}|_p = \frac{\#\mathrm{PGL}_2(\mathbb{F}_p) \cdot \left(\sum_{f \in \mathrm{PGL}_2(\mathbb{F}_p) \setminus \bar{S}} \frac{1}{\#\mathrm{Aut}_{\mathbb{F}_p}(f)} \right)}{p^{\dim V} \cdot \mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z}_p)) \cdot \left(\int_{(I,J) \in \pi(S)} \sum_{\substack{f \in V_{\mathbb{Z}_p}(I,J) \\ f \in \mathrm{PGL}_2(\mathbb{Z}_p)}} \frac{1}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f)} dIdJ \right)}. \quad (64)$$

Proof: Using Proposition 3.12 with ϕ replaced by the characteristic function of S , we obtain

$$\mathrm{Vol}(S) = |\mathcal{J}|_p \mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z}_p)) \int_{(I,J) \in \pi(S)} \left(\sum_{\substack{f \in V_{\mathbb{Z}_p}(I,J) \\ f \in \mathrm{PGL}_2(\mathbb{Z}_p)}} \frac{1}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f)} \right) dIdJ. \quad (65)$$

Since S is defined by congruence conditions modulo p , and since \bar{S} is $\mathrm{PGL}_2(\mathbb{F}_p)$ invariant (a consequence of the $\mathrm{PGL}_2(\mathbb{Z}_p)$ -invariance of S), we have

$$\mathrm{Vol}(S) = \frac{\#\bar{S}}{p^{\dim V}} = \frac{1}{p^{\dim V}} \#\mathrm{PGL}_2(\mathbb{F}_p) \cdot \left(\sum_{f \in \mathrm{PGL}_2(\mathbb{F}_p) \setminus \bar{S}} \frac{1}{\#\mathrm{Aut}_{\mathbb{F}_p}(f)} \right), \quad (66)$$

where the final equality follows from the orbit-stabilizer formula. Equating the right hand sides of (65) and (66) yields the proposition. \square

Remark 3.14 Thus far, we have not used anything specific about binary quartic forms, and the analogues of the statements and proofs of Propositions 3.11–3.13 continue to hold if we replace the pair (PGL_2, V) with any representation (G, W) defined over \mathbb{Z} , as long as the following conditions hold:

1. G is a semisimple group and W is a *coregular* representation of G , i.e., the ring of invariants for the action of $G_{\mathbb{C}}$ on $W_{\mathbb{C}}$ is freely generated, say, by the polynomials I_1, \dots, I_k (which we may take to be integral polynomials).
2. The stabilizer in $G_{\mathbb{C}}$ of any element $v \in W_{\mathbb{C}}$ outside a measure 0 set of $W_{\mathbb{C}}$ is finite and absolutely bounded.
3. The sum of the degrees of the I_j 's is equal to the dimension of W (in the case of binary quartic forms, we had $2 + 3 = 5$). This condition is necessary to prove that the relevant Jacobian change of variables \mathcal{J} is independent of the values of I_1, \dots, I_k in Step 4.
4. There exists a rational polynomial map $\phi : \mathbb{C}^k \rightarrow W_{\mathbb{C}}$ such that $\phi(i_1, \dots, i_k)$ has invariants (i_1, \dots, i_k) for each k -tuple in \mathbb{C}^k .

In our case of binary quartic forms, to apply Proposition 3.13 we may choose S , e.g., to be the set of binary quartic forms in $V_{\mathbb{Z}_p}$ having some fixed invariants (I, J) modulo p . The following lemma is then useful in evaluating the right hand side of (64).

Lemma 3.15 *Let p be a fixed prime, and let $(I, J) \in \mathbb{Z}_p^2$ be an element in the image of π such that $p^2 \nmid \Delta(I, J)$. Then*

$$\sum_{f \in \frac{V_{\mathbb{Z}_p}(I, J)}{\mathrm{PGL}_2(\mathbb{Z}_p)}} \frac{1}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f)} = 1.$$

Let $p \neq 3$ be a prime, and let $(I, J) \in \mathbb{F}_p^2$ be an element such that $\Delta(I, J) \neq 0$. Then

$$\sum_{f \in \frac{V_{\mathbb{F}_p}(I, J)}{\mathrm{PGL}_2(\mathbb{F}_p)}} \frac{1}{\#\mathrm{Aut}_{\mathbb{F}_p}(f)} = 1.$$

Proof: Since $p^2 \nmid \Delta(I, J)$, Theorem 3.2 and Proposition 3.18 imply that

$$\mathrm{Aut}_{\mathbb{Z}_p}(f) = \mathrm{Aut}_{\mathbb{Q}_p}(f) = E^{I, J}(\mathbb{Q}_p)[2]. \quad (67)$$

For odd primes p , Theorem 3.2 and [9, Lemmas 3, 4] show that the number of $\mathrm{PGL}_2(\mathbb{Q}_p)$ -equivalence class in $V_{\mathbb{Z}_p}$ having invariants I and J is equal to $\#(E^{I, J}(\mathbb{Q}_p)/2E^{I, J}(\mathbb{Q}_p))$, while the results in [16, Section 6] show that the number of $\mathrm{PGL}_2(\mathbb{Q}_2)$ -equivalence class in $V_{\mathbb{Z}_2}$ having invariants I and J is equal to $\frac{1}{2}\#(E^{I, J}(\mathbb{Q}_2)/2E^{I, J}(\mathbb{Q}_2))$. The first assertion of Lemma 3.15 now follows from Lemma 3.20, which states that the value of $\#(E^{I, J}(\mathbb{Q}_p)/2E^{I, J}(\mathbb{Q}_p))/\#E^{I, J}(\mathbb{Q}_p)[2]$ is 1 if $p \neq 2$, and 2 if $p = 2$.

For $p \geq 5$, the second assertion of Lemma 3.15 follows from Theorem 3.2 with K replaced by \mathbb{F}_p , and the fact that $\#(E^{I, J}(\mathbb{F}_p)/2E^{I, J}(\mathbb{F}_p))/\#E^{I, J}(\mathbb{F}_p)[2]$ is 1. For $p = 2$, the lemma follows from a finite computation. \square

Let us now choose some specific sets $S \subset V_{\mathbb{Z}_p}$ for each prime p . If $p \neq 3$, let $(I_0, J_0) \in \mathbb{F}_p^2$ be a fixed element such that $\Delta(I_0, J_0) \neq 0$. We then define S to be the set of all $f \in V_{\mathbb{Z}_p}$ such that the reduction of $(I(f), J(f))$ modulo p is equal to (I_0, J_0) . Then Proposition 3.13 in conjunction with Lemma 3.15 implies that

$$|\mathcal{J}|_p = \frac{\#\mathrm{PGL}_2(\mathbb{F}_p)}{p^5 \mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z}_p))(1/p^2)} = 1.$$

Because the definition of Δ in terms of I and J requires division by 27, specifying a given value of (I, J) modulo 3 cannot alone guarantee that $3 \nmid \Delta(I, J)$ (this is indeed the reason for excluding the case

$p = 3$ in Lemma 3.15). Hence, in the case $p = 3$, we choose instead a set S defined by conditions on the invariants (I, J) modulo a higher power of 3. For example, let S be the set of all $f \in V_{\mathbb{Z}_3}$ such that $I(f) \equiv 3 \pmod{9}$. The proof of Theorem 1.7 immediately implies that if $f \in V_{\mathbb{Z}_3}$ and $I(f) \equiv 0 \pmod{3}$, then the only condition on J is that $J(f) \equiv 0 \pmod{27}$. Thus, if $f(x, y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 \in S$, then $\Delta(f) \not\equiv 0 \pmod{3}$, and we may use the first statement of Lemma 3.15. Next, note that $I(f) \equiv 3 \pmod{9}$ precisely when $c \equiv 0 \pmod{3}$ and $ae - bd \equiv 1 \pmod{3}$. Let $\bar{a}, \bar{b}, \bar{c}, \bar{d}$, and \bar{e} denote the reductions modulo 3 of a, b, c, d , and e , respectively. Then $f \in S$ if and only if $\bar{c} = 0$ and $\bar{a}\bar{e} - \bar{b}\bar{d} = 1$. There are 24 values of $(\bar{a}, \bar{b}, \bar{c}, \bar{d}, \bar{e}) \in \mathbb{F}_p^5$ satisfying these two conditions. Therefore,

$$|\mathcal{J}|_3 = \frac{24}{3^5 \text{Vol}(\text{PGL}_2(\mathbb{Z}_p)) \text{Vol}(\pi(S))} = \frac{24}{3^5(1 - 1/3^2)(1/3^5)} = 27.$$

This completes the proof of Proposition 3.7.

Alternatively, we could choose S to be the set of $f \in V_{\mathbb{Z}_p}$ such that $p \nmid \Delta(f)$. Then \bar{S} , the reduction of S modulo p , is the set of all $f \in V_{\mathbb{F}_p}$ such that $\Delta(f) \neq 0$. An element of \bar{S} is determined, up to scaling by elements in \mathbb{F}_p^\times , by its roots in $\mathbb{P}_{\mathbb{F}_p}^1$. For example, the number of elements in \bar{S} having four distinct roots in $\mathbb{P}^1(\mathbb{F}_p)$ is $(p-1)\frac{1}{24}(p+1)p(p-1)(p-2)$. An elementary computation then yields the following equality:

$$\#\bar{S} = p^2(p+1)(p-1)^2.$$

Therefore, (65) and Lemma 3.15 imply that we have

$$|\mathcal{J}|_p = \frac{\text{Vol}(S)}{\text{Vol}(\text{PGL}_2(\mathbb{Z}_p)) \text{Vol}(\pi(S))} = \frac{\#\bar{S}}{p^5 \text{Vol}(\text{PGL}_2(\mathbb{Z}_p)) \text{Vol}(\pi(S))} = \frac{p-1}{p \text{Vol}(\pi(S))}.$$

The set $\pi(S)$ consists of eligible pairs $(I, J) \in \mathbb{Z}_p^2$ such that $p \nmid \Delta(I, J)$. (A pair $(I, J) \in \mathbb{Z}_p^2$ is said to be *eligible* if it occurs as the invariants of some $f \in V_{\mathbb{Z}_p}$.) We may thus use Theorem 1.7 and compute the volume of $\pi(S)$ to be $(p-1)/p$ when $p \neq 3$ and $2/81$ when $p = 3$. We thus again obtain $|\mathcal{J}|_p = 1$ for $p \neq 3$ and $|\mathcal{J}|_3 = 27$, yielding Proposition 3.7.

3.5 The number of elliptic curves of bounded height in a large family

Suppose F is a large family of elliptic curves. To prove Theorem 3.1 we need to estimate the number of elliptic curves in F that have height bounded by X . In this section, we determine exact asymptotics for the number of elliptic curves having bounded height in any large family F of elliptic curves.

As an elliptic curve is determined by its invariants I and J , we estimate the number of pairs (I, J) that belong to $\text{Inv}(F)$ and have height less than X . It follows from an easy application of Proposition 2.6 that the number of pairs $(I, J) \in \mathbb{Z} \times \mathbb{Z}$ satisfying $H(I, J) < X$ and $4I^3 - J^2 > 0$ (resp. $H(I, J) < X$ and $4I^3 - J^2 < 0$) is equal to the volume of R_X^+ (resp. R_X^-) up to an error of $O(X^{1/2})$, where the sets R_X^\pm were defined in the proof of Proposition 2.10. For any set $S \subset \mathbb{Z} \times \mathbb{Z}$, let $N(S; X)$ denote the number of pairs $(I, J) \in S$, having height bounded by X , satisfying $\Delta(I, J) \neq 0$.

Now, the set $\text{Inv}(F) \subset \mathbb{Z} \times \mathbb{Z}$ is defined by (perhaps infinitely many) congruence conditions. To determine the asymptotics of $N(\text{Inv}(F); X)$ as X goes to infinity, we need the following uniformity estimate:

Proposition 3.16 *The number of elliptic curves E over \mathbb{Q} having height less than X such that p^2 divides the discriminant of E is $O(X^{5/6}/p^{3/2})$, where the implied constant is independent of p .*

Proof: This proof is very similar to (but much easier than) the proof of the uniformity estimate for binary quartic forms in Theorem 2.13. We start with embedding the set $\{x^3 + Ax + B : A, B \in \mathbb{Z}\}$ into the bigger space of all integral binary cubic forms. Let $U_{\mathbb{Z}}$ denote the space of all integral binary cubic forms. The group $\text{GL}_2(\mathbb{Z})$ acts on $U_{\mathbb{Z}}$ by linear substitution of variables. Consider the composite map $\psi = \psi_2 \circ \psi_1$ given by

$$\psi : \{x^3 + Ax + B : A, B \in \mathbb{Z}\} \rightarrow U_{\mathbb{Z}} \rightarrow \text{GL}_2(\mathbb{Z}) \backslash U_{\mathbb{Z}},$$

where the first map ψ_1 sends $x^3 + Ax + B$ to the integral binary cubic form $x^3 + Axy^2 + By^3$. As in the proof of Proposition 2.16, an element in $\mathrm{GL}_2(\mathbb{Z}) \backslash U_{\mathbb{Z}}$ has at most 12 preimages under ψ . This can be seen as follows: if f is in the preimage of the $\mathrm{GL}_2(\mathbb{Z})$ -orbit of $v \in U_{\mathbb{Z}}$, then there exists an element $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ such that $\gamma \cdot v = \psi_1(f)$. Then $v((1,0) \cdot \gamma) = 1$ since $\psi_1(f)$ has x^3 -coefficient equal to 1. The results in [22] and [25] assert that there are at most 12 solutions $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ to the equation $v(a, b) = 1$. This implies that v has at most 12 preimages under ψ because each preimage yields a different solution to $v(a, b) = 1$. From [19, Proposition 1], it follows that the number of $\mathrm{GL}_2(\mathbb{Z})$ -orbits on $U_{\mathbb{Z}}$ having discriminant divisible by p^2 is bounded by $O(X/p^2)$. Therefore, the number of elliptic curves having discriminant divisible p^2 is bounded by $O(X/p^2)$ as well.

To complete the proof of the above proposition, we partition the set of elliptic curves having discriminant divisible by p^2 into two subsets. First, consider elliptic curves $E_{A,B} : y^2 = x^3 + Ax + B$ having additive reduction at a prime $p > 3$. This happens if and only if $p \mid A$ and $p \mid B$. The number of such pairs $(A, B) \in \mathbb{Z} \times \mathbb{Z}$ having height less than X is clearly bounded by $O(X^{5/6}/p^2 + X^{1/2}/p + 1)$. Therefore, the number of elliptic curves having additive reduction at p and height less than X is bounded both by $O(X/p^2)$ and by $O(X^{5/6}/p^2 + X^{1/2}/p + 1)$. These combined estimates yield a bound of $O(X^{5/6}/p^{5/3})$ which is sufficient.

Now consider those elliptic curves $E_{A,B}$ such that $p^2 \mid \Delta(E_{A,B})$, $E_{A,B}$ has multiplicative reduction at p , and $H'(E_{A,B}) < X$. Assuming that $p > 3$, we now have $p \nmid A$. Since $E_{A,B}$ has height bounded by X , there are $O(X^{1/3})$ possible choices for A and $O(X^{1/2})$ possible choices for B . With A fixed, there are then $O(1)$ possible choices for the reduction of B modulo p^2 . Therefore, the number of such elliptic curves is bounded by $O(X^{1/3} \cdot (X^{1/2}/p^2 + 1))$. Combined with the previously obtained bound of $O(X/p^2)$, we see that the number of such elliptic curves $E_{A,B}$ is bounded by $O(X^{5/6}/p^{3/2})$. This concludes the proof. \square

Analogously to $M_p(V, F)$, we define the local mass $M_p(F)$ by

$$M_p(F) = \int_{(I,J) \in \mathrm{Inv}_p(F)} dIdJ. \quad (68)$$

We also define the following analogues at infinity of $M_p(F)$ and $M_p(V, F)$, respectively.

$$\begin{aligned} M_{\infty}(F; X) &:= \int_{\substack{(I,J) \in \mathrm{Inv}_{\infty}(F) \\ H(I,J) < X}} dIdJ, \\ M_{\infty}(V, F; X) &:= \int_{\substack{(I,J) \in \mathrm{Inv}_{\infty}(F) \\ H(I,J) < X}} \frac{\#(E^{I,J}(\mathbb{R})/2E^{I,J}(\mathbb{R}))}{\#E^{I,J}(\mathbb{R})[2]} dIdJ. \end{aligned} \quad (69)$$

We now have the following theorem, which follows from Proposition 3.16 just as Theorem 2.21 followed from Theorem 2.13:

Theorem 3.17 *Let F be a large family of elliptic curves and let $N(F; X)$ denote the number of elliptic curves $E \in F$ such that $H'(E) < X$. Then*

$$N(F; X) = M_{\infty}(F; X) \prod_p M_p(F) + o(X^{5/6}). \quad (70)$$

3.6 Proofs of the main theorems (Theorems 1.1, 1.3, and 3.1)

Let us say that an element $f \in V_{\mathbb{Z}}$ is *bad at p* if either f is not \mathbb{Q}_p -soluble or $m_p(f) \neq 1$. To deduce Theorem 3.1 from Theorem 2.21, we need the following result:

Proposition 3.18 *If an integral binary quartic form f is bad at a prime $p > 2$, then $p^2 \mid \Delta(f)$.*

Proof: If $m_p(f) \neq 1$, then there exists $\gamma \in \mathrm{PGL}_2(\mathbb{Q}_p) \backslash \mathrm{PGL}_2(\mathbb{Z}_p)$ such that $\gamma \cdot f \in V_{\mathbb{Z}_p}$. By replacing f with a $\mathrm{PGL}_2(\mathbb{Z}_p)$ -translate if necessary, we may assume that $\gamma = \begin{pmatrix} p^a & \\ & p^b \end{pmatrix}$, with $a > b = 0$. It then follows that the x^4 -coefficient of f is divisible by p^2 and the x^3y -coefficient of f is divisible by p , implying that $p^2 \mid \Delta(f)$.

We now show that if $f \in V_{\mathbb{Z}}$ is not \mathbb{Q}_p -soluble, then f has splitting type (1^21^2) , (2^2) , or (1^4) at p , implying that $p^2 \mid \Delta(f)$. First, if the discriminant of $f \in V_{\mathbb{Z}_p}$ is prime to p , then f is \mathbb{Q}_p -soluble (see [13, Chapter 3.6]). Also, if the splitting type of f at p is (1^211) or (1^31) , then the reduction of f modulo p has a simple root in $\mathbb{P}^1(\mathbb{F}_p)$, which then lifts to a root in $\mathbb{P}^1(\mathbb{Q}_p)$ by Hensel's Lemma. Thus f is \mathbb{Q}_p -soluble.

It remains to prove that if the splitting type of f at p is (1^22) , then f is \mathbb{Q}_p -soluble. If $f \in V_{\mathbb{Z}_p}$ has splitting type (1^22) , then the reduction of f modulo p can be assumed to be of the form $\bar{a}x^2(x^2 - \bar{n}y^2)$, where \bar{n} is a nonresidue modulo p . Hence we may assume that $f = a(x^2 - kpy^2)(x^2 - ny^2)$, where $a, n, k \in \mathbb{Z}_p$, the element $n \in \mathbb{Z}_p$ is a nonresidue when reduced modulo p , and $p \nmid a$. If a is a square in \mathbb{Q}_p , then $f(1, 0)$ is a square in \mathbb{Q}_p and we are done. So we may assume that a is a nonsquare. Now if $p \nmid x_0$, then $x_0^2 - kp$ is a square in \mathbb{Q}_p ; so it suffices to prove the existence of $\bar{x}_0 \in \mathbb{F}_p^\times$ such that $\bar{x}_0^2 - \bar{n}$ is a quadratic nonresidue modulo p . Consider the first quadratic residue $\bar{x}_0^2 = (c+1)\bar{n}$ appearing in the sequence $\bar{n}, 2\bar{n}, \dots, (p-1)\bar{n}$. Then $\bar{x}_0^2 - \bar{n} = (c+1)\bar{n} - \bar{n} = c\bar{n}$ is a nonresidue, as was desired. \square

Analogously to the sets $S_p(F)$, we define $S_\infty(F)$ to be the set of all \mathbb{R} -soluble binary quartic forms in $V_{\mathbb{R}}$ whose invariants belong to $\text{Inv}_\infty(F)$. Since $\#(E^{I,J}(\mathbb{R})/2E^{I,J}(\mathbb{R}))/\#E^{I,J}(\mathbb{R})[2]$ is always equal to $1/2$, the computation of the volume of the sets $\mathcal{R}_X(L^{(i)})$ in Section 2.4 and the definition of $M_\infty(F; X)$ implies that

$$N(V_{\mathbb{Z}} \cap S_\infty(F); X) = \frac{1}{27} \text{Vol}(\text{PGL}_2(\mathbb{Z}) \backslash \text{PGL}_2(\mathbb{R})) M_\infty(V, F; X) + O(X^{3/4+\epsilon}).$$

We now prove the following theorem, from which Theorem 3.1 will be seen to follow.

Theorem 3.19 *Let F be a large family of elliptic curves. Then we have*

$$\lim_{X \rightarrow \infty} \frac{\sum_{\substack{E \in F \\ H'(E) < X}} (\#S_2(E) - 1)}{\sum_{\substack{E \in F \\ H'(E) < X}} 1} = \text{Vol}(\text{PGL}_2(\mathbb{Z}) \backslash \text{PGL}_2(\mathbb{R})) \frac{M_\infty(V, F; X)}{M_\infty(F; X)} \prod_p \left[\text{Vol}(\text{PGL}_2(\mathbb{Z}_p)) \frac{M_p(V, F)}{M_p(F)} \right]. \quad (71)$$

Proof: Note that by Theorem 3.5, the numerator of the left hand side of (71) is equal to the number of locally soluble $\text{PGL}_2(\mathbb{Z})$ -orbits on $S(F^{\text{inv}})$ having height bounded by $2^{12}X$ and no rational linear factor, where each orbit $\text{PGL}_2(\mathbb{Z}) \cdot f$ is counted with weight $1/m(f)$. Thus, by Theorem 2.21 and Propositions 3.6, 3.9, and 3.18, we have

$$\begin{aligned} \sum_{\substack{E \in F \\ H'(E) < X}} (\#S_2(E) - 1) &= N(V_{\mathbb{Z}} \cap S_\infty(X); 2^{12}X) \prod_p \int_{S_p(F)} \frac{1}{m_p(f)} df + o(X^{5/6}) \\ &= \frac{2^{10}}{27} \text{Vol}(\text{PGL}_2(\mathbb{Z}) \backslash \text{PGL}_2(\mathbb{R})) M_\infty(V, F; X) \prod_p \left| \frac{2^{10}}{27} \right|_p \text{Vol}(\text{PGL}_2(\mathbb{Z}_p)) M_p(V, F) + o(X^{5/6}) \\ &= \text{Vol}(\text{PGL}_2(\mathbb{Z}) \backslash \text{PGL}_2(\mathbb{R})) M_\infty(V, F; X) \prod_p \text{Vol}(\text{PGL}_2(\mathbb{Z}_p)) M_p(V, F) + o(X^{5/6}). \end{aligned} \quad (72)$$

Meanwhile, Theorem 3.17 implies that we have

$$\sum_{\substack{E \in F \\ H'(E) < X}} 1 = M_\infty(F; X) \prod_p M_p(F) + o(X^{5/6}). \quad (73)$$

Taking the ratio of (72) and (73) now yields Theorem 3.19. \square

To evaluate the right hand side of (71), we require the following fact (see [12, Lemma 3.1]):

Lemma 3.20 *Let E be an elliptic curve over \mathbb{Q}_p . Then*

$$\#(E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)) = \begin{cases} \#E(\mathbb{Q}_p)[2] & \text{if } p \neq 2; \\ 2 \cdot \#E(\mathbb{Q}_p)[2] & \text{if } p = 2. \end{cases}$$

Combining Lemma 3.20 with (54) and (68), we obtain that

$$\frac{M_p(V, F)}{M_p(F)} = \frac{\int_{(I, J) \in \text{Inv}_p(F)} \frac{\#(E^{I, J}(\mathbb{Q}_p)/2E^{I, J}(\mathbb{Q}_p))}{\#E^{I, J}(\mathbb{Q}_p)[2]} dIdJ}{\int_{(I, J) \in \text{Inv}_p(F)} dIdJ} = \begin{cases} 1 & \text{if } p \neq 2; \\ 2 & \text{if } p = 2. \end{cases} \quad (74)$$

Since we also know that $M_\infty(V, F; X)/M_\infty(F; X) = 1/2$, Theorem 3.19 implies that

$$\frac{\sum_{\substack{E \in F \\ H'(E) < X}} (\#S_2(E) - 1)}{\sum_{\substack{E \in F \\ H'(E) < X}} 1} = \text{Vol}(\text{PGL}_2(\mathbb{Z}) \backslash \text{PGL}_2(\mathbb{R})) \prod_p \text{Vol}(\text{PGL}_2(\mathbb{Z}_p))$$

which is then equal to $2\zeta(2) \prod_p (1 - p^{-2}) = 2$, the Tamagawa number of $\text{PGL}_2(\mathbb{Q})$. We have proven Theorem 3.1 (and thus also Theorems 1.1 and 1.3).

Acknowledgments

We are very grateful to John Cremona, Dick Gross, Tom Fisher, Florian Herzig, Wei Ho, Jennifer Park, Bjorn Poonen, Jerry Wang, and the anonymous referee for their many helpful comments on an earlier version of this manuscript. The first author was partially supported by NSF Grant DMS-1001828.

References

- [1] S. Y. An, S. Y. Kim, D. C. Marshall, S. H. Marshall, W. G. McCallum, and A. R. Perlis, Jacobians of genus one curves, *J. Number Theory* **90** (2001), no. 2, 304–315.
- [2] B. Bektemirov, B. Mazur, W. Stein, M. Watkins, Average ranks of elliptic curves: tension between data and conjecture, *Bull. Amer. Math. Soc. (N.S.)* **44** (2007), no. 2, 233–254 (electronic).
- [3] M. Bhargava, Higher composition laws III: The parametrization of quartic rings, *Ann. of Math.* **159** (2004) 1329–1360.
- [4] M. Bhargava, The density of discriminants of quartic rings and fields, *Ann. of Math.* **162**, 1031–1063.
- [5] M. Bhargava, The density of discriminants of quintic rings and fields, *Ann. of Math. (2)*, **172** (2010), no. 3, 1559–1591.
- [6] M. Bhargava, The geometric sieve and squarefree values of polynomial discriminants and other invariant polynomials, preprint.
- [7] M. Bhargava and W. Ho, Coregular spaces and genus one curves, <http://arxiv.org/abs/1306.4424v1>.
- [8] B. J. Birch and J. R. Merriman, Finiteness theorems for binary forms with given discriminant, *Proc. London Math. Soc. (3)* **24** (1972), 385–394.
- [9] B. J. Birch and H. P. F. Swinnerton-Dyer, Notes on elliptic curves I, *J. Reine Angew. Math.* **212** (1963), 7–25.

- [10] A. Borel and Harish-Chandra, Arithmetic subgroups of algebraic groups, *Ann. of Math.* **75** (1962), 485–535.
- [11] A. Brumer, The average rank of elliptic curves I, *Invent. Math.* **109** (1992), no. 3, 445–472.
- [12] A. Brumer and K. Kramer, The rank of elliptic curves, *Duke Math. J.* **44** (1977), no. 4, 715–743.
- [13] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd edn., Cambridge University Press, 1997.
- [14] J. E. Cremona, Reduction of binary cubic and quartic forms, *LMS J. Comput. Math.* **2** (1999), 64–94.
- [15] J. E. Cremona and T. Fisher, On the equivalence of binary quartics, *Journal of Symbolic Computation* **44** (2009), 673–682.
- [16] J. E. Cremona and M. Stoll, Minimal models for 2-coverings of elliptic curves, *LMS J. Comput. Math.* **5** (2002), 220–243 (electronic).
- [17] H. Davenport, On a principle of Lipschitz, *J. London Math. Soc.* **26** (1951), 179–183. Corrigendum: “On a principle of Lipschitz”, *J. London Math. Soc.* **39** (1964), 580.
- [18] H. Davenport, On the class-number of binary cubic forms I and II, *J. London Math. Soc.* **26** (1951), 183–198.
- [19] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields II, *Proc. Roy. Soc. London Ser. A* **322** (1971), no. 1551, 405–420.
- [20] A. J. de Jong, Counting elliptic surfaces over finite fields, *Mosc. Math. J.* **2** (2002), no. 2, 281–311.
- [21] C. Delaunay, Heuristics on class groups and on Tate-Shafarevich groups: the magic of the Cohen-Lenstra heuristics, *Ranks of elliptic curves and random matrix theory*, London Math. Soc. Lecture Note Ser. **341**, Cambridge Univ. Press, Cambridge, 2007, 323–340.
- [22] B. N. Delone, Über die Darstellung der Zahlen durch die binäre kubischen Formen von negativer Diskriminante, *Math. Z.* **31** (1930), 1–26.
- [23] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, AMS Translations of Mathematical Monographs **10**, 1964.
- [24] T. Ekedahl, An infinite version of the Chinese remainder theorem, *Comment. Math. Univ. St. Paul.* **40** (1991), 53–59.
- [25] J. H. Evertse, On the representation of integers by binary cubic forms of positive discriminant, *Invent. Math.* **73** (1983), no. 1, 117–138.
- [26] É. Fouvry, Sur le comportement en moyenne du rang des courbes $y^2 = x^3 + k$, *Séminaire de Théorie des Nombres, Paris, 1990–91, Progr. Math.* **108**, Birkhäuser Boston, Boston, MA, 1993.
- [27] C. F. Gauss, *Disquisitiones Arithmeticae*, 1801.
- [28] D. Goldfeld, Conjectures on elliptic curves over quadratic fields, *Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979)*, pp. 108–118, Lecture Notes in Math. **751**, Springer, Berlin, 1979.
- [29] D. R. Heath-Brown, The size of Selmer groups for the congruent number problem, *Invent. Math.* **111** (1993), no. 1, 171–195.
- [30] D. R. Heath-Brown, The average analytic rank of elliptic curves, *Duke Math. J.* **122** (2004), no. 3, 591–623.

- [31] D. Kane, On the ranks of the 2-Selmer groups of twists of a given elliptic curve, *Algebra & Number Theory* **7** (2013), no. 5, 1253–1279.
- [32] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications **45**, American Mathematical Society, Providence, RI, 1999.
- [33] R. P. Langlands, The volume of the fundamental domain for some arithmetical subgroups of Chevalley groups, *Algebraic Groups and Discontinuous Subgroups*, pp. 143–148, Proc. Sympos. Pure Math. **9**, Boulder, CO, 1966.
- [34] F. Mertens, Ueber einige asymptotische Gesetze der Zahlentheorie, *J. reine angew. Math.* **77** (1874), 289–338.
- [35] V. Platonov and A. Rapinchuk, *Algebraic groups and number theory*, Translated from the 1991 Russian original by Rachel Rowen, Pure and Applied Mathematics **139**, Academic Press, Inc., Boston, MA, 1994.
- [36] B. Poonen, Squarefree values of multivariable polynomials, *Duke Math. J.* **118** (2003), no. 2, 353–373.
- [37] B. Poonen and E. Rains, Random maximal isotropic subspaces and Selmer groups, *J. Amer. Math. Soc.* **25** (2012), no. 1, 245–269.
- [38] P. Schneider, *p-adic Lie groups*, Springer, 2011.
- [39] J-P. Serre, *A course in arithmetic*, Translated from the French, Graduate Texts in Mathematics **7**, Springer-Verlag, New York-Heidelberg, 1973.
- [40] C. L. Siegel, The average measure of quadratic forms with given determinant and signature, *Ann. of Math. (2)* **45** (1944), 667–685.
- [41] J. H. Silverman, *The arithmetic of elliptic curves*, Second edition, Graduate Texts in Mathematics **106**, Springer, Dordrecht, 2009.
- [42] H. P. F. Swinnerton-Dyer, The effect of twisting on the 2-Selmer group, *Math. Proc. Cambridge Philos. Soc.* **145** (2008), no. 3, 513–526.
- [43] M. Wood, *Moduli spaces for rings and ideals*, Ph.D. Thesis, Princeton University, June 2009.
- [44] M. Wood, Quartic rings associated to binary quartic forms, *Int. Math. Res. Not.* **2012** (2012), no. 6, 1300–1320.
- [45] M. P. Young, Low-lying zeros of families of elliptic curves. *J. Amer. Math. Soc.* **19** (2006), no. 1, 205–250.