

Families of elliptic curves ordered by conductor

Ananth N. Shankar and Arul Shankar and Xiaoheng Wang

May 12, 2019

Abstract

In this article, we study the family of elliptic curves E/\mathbb{Q} , having good reduction at 2 and 3, and whose j -invariants are small. Within this set of elliptic curves, we consider the following two subfamilies: first, the set of elliptic curves E such that the quotient $\Delta(E)/C(E)$ is squarefree; and second, the set of elliptic curves E such that the *Szpiro quotient* $\beta_E := \log |\Delta(E)|/\log(C(E))$ is less than $7/4$. Both these families are conjectured to contain a positive proportion of elliptic curves, when ordered by conductor.

Our main results determine asymptotics for both these families, when ordered by conductor. Moreover, we prove that the average size of the 2-Selmer groups of elliptic curves in the first family, again when these curves are ordered by their conductors, is 3. This implies that the average rank of these elliptic curves is finite, and bounded by 1.5.

1 Introduction

Every elliptic curve over \mathbb{Q} can be uniquely represented as $E_{AB} : y^2 = x^3 + Ax + B$, where A and B are integers such that there is no prime p with $p^4 \mid A$ and $p^6 \mid B$, and such that $\Delta(A, B) := -4A^3 - 27B^2 \neq 0$. Given an elliptic curve E over \mathbb{Q} , we denote its algebraic rank by $r(E)$ and its analytic rank by $r_{\text{an}}(E)$. The Birch and Swinnerton-Dyer conjecture asserts that these two quantities are equal, i.e., we have $r(E) = r_{\text{an}}(E)$.

Foundational conjectures of Goldfeld [24] (in the case of families of quadratic twists of elliptic curves) and Katz–Sarnak [27] (for the full family of elliptic curves) assert that a density of 50% of elliptic curves have rank 0, and that 50% have rank 1, and that the average rank of elliptic curves is $1/2$. Both these conjectures are formulated through a study of the associated family of the L -functions $L_E(s)$ attached to the elliptic curves E . The behaviour of $L_E(s)$ at and near the critical point is used to control the distribution of analytic ranks, which, assuming the BSD conjecture, can be used to give heuristics for the distribution of the algebraic ranks.

The most natural way to order a family of L -functions is by their *conductors*, which, in this case of L -functions of elliptic curves, is equal to the levels of the associated modular forms. Thus in the conjectures of Goldfeld and Katz–Sarnak, it is implicitly assumed that elliptic curves are ordered by their conductors. However, when studying two-parameter families of elliptic curves, the curves E_{AB} are usually ordered by their (naive) *height* $H(E_{AB}) = \max\{4|A|^3, 27B^2\}$.¹ Assuming the generalized Riemann hypothesis, Brumer [14], Heath-Brown [25], and Young [32], proved the successively better bounds of 2.3, 2, and $25/14$, on the average analytic ranks of elliptic curves when ordered by height. On the algebraic side, Bhargava and the second named author [7] proved that the average rank of elliptic curves, when ordered by height, is bounded by 0.885.

If elliptic curves are instead ordered by conductor, even asymptotics for the number of curves are not known. The *discriminant* $\Delta(E_{AB})$ of E_{AB} is (up to absolutely bounded factors of 2 and 3) $-4A^3 - 27B^2$. The *conductor* $C(E_{AB})$ of E_{AB} is (again, up to bounded factors of 2 and 3) the product over all primes p dividing $\Delta(E_{AB})$ of either p or p^2 depending on if E_{AB} has multiplicative or additive reduction at p . Building on the work of Brumer–McGuinness [16] on the family of elliptic curves ordered by discriminant, Watkins [31] gives heuristics suggesting that the number of elliptic curves with conductor bounded by X

¹See, however, work of Hortsch [26] obtaining asymptotics for the number of elliptic curves with bounded Faltings height.

grows as $\sim cX^{5/6}$ for an explicit constant c . Lower bounds of this magnitude are easy to obtain, but the best known upper bound is $O(X^{1+\epsilon})$ due to work of Duke–Kowalski [21].

The difficulties in determining precise upper bounds are twofold. First, it is difficult to rule out the possibility of many elliptic curves with large height but small discriminant. Second, it is difficult to rule out the possibility of many elliptic curves with large discriminant but small conductor. It is interesting to note here that the second difficulty is exactly a nonarchimedean version of the first. Indeed, curves E_{AB} with large height and small discriminant correspond to pairs (A, B) of integers, where $4A^3$ and $-27B^2$ are unusually close as real numbers. On the other hand, curves E_{AB} with large discriminant and small conductor correspond to pairs of integers (A, B) such that $4A^3$ and $-27B^2$ are unusually close as p -adic numbers.

In this article, we focus on studying the second difficulty while entirely sidestepping the first. To this end, we let \mathcal{E} denote the set of elliptic curves E over \mathbb{Q} that satisfy the following properties.

1. The j -invariant $j(E)$ of E satisfies $j(E) < \log \Delta(E)$.
2. E has good reduction at 2 and 3.

The first of the above three properties excludes all elliptic curves E with $\Delta(E) \ll H(E)^{1-\epsilon}$ and is absolutely critical for our results. According to the Brumer–McGuinness heuristics [16], only a negligible number of elliptic curves are being excluded by the assumption of this property, but this is unproven. The second property is a technical assumption made to simplify local computations at the 2-adic and 3-adic places. We will in fact have to further restrict our families of elliptic curves. We define the families

$$\begin{aligned} \mathcal{E}_{\text{sf}} &:= \left\{ E \in \mathcal{E} : \frac{\Delta(E)}{C(E)} \text{ is squarefree} \right\}, \\ \mathcal{E}_\kappa &:= \left\{ E \in \mathcal{E} : \beta_E \leq \kappa \right\}, \end{aligned}$$

for every $\kappa > 1$, where the *Szpiro constant* β_E is defined to be $\log |\Delta(E)| / \log(C(E))$. When ordered by conductor, the family \mathcal{E}_κ conjecturally contains 100% of elliptic curves with good reduction at 2 and 3, and \mathcal{E}_{sf} conjecturally contains a positive proportion of elliptic curves. We prove the following result determining asymptotics for these families of elliptic curves, ordered by their conductors.

Theorem 1.1 *Let $1 < \kappa < 7/4$ be a positive constant. Then we have*

$$\begin{aligned} \#\{E \in \mathcal{E}_{\text{sf}} : C(E) < X\} &\sim \frac{1 + \sqrt{3}}{60\sqrt{3}} \frac{\Gamma(1/2)\Gamma(1/6)}{\Gamma(2/3)} \cdot \prod_{p \geq 5} \left(1 + \frac{1}{p^{7/6}} - \frac{1}{p^2} - \frac{1}{p^{13/6}} \right) \cdot X^{5/6}; \\ \#\{E \in \mathcal{E}_\kappa : C(E) < X\} &\sim \frac{1 + \sqrt{3}}{60\sqrt{3}} \frac{\Gamma(1/2)\Gamma(1/6)}{\Gamma(2/3)} \cdot \prod_{p \geq 5} \left[\left(1 - \frac{1}{p} \right) \left(1 + \frac{1}{p^{5/3}} + \frac{1}{p^{11/6}} + \frac{1}{p^{17/6}} \right) \right. \\ &\quad \left. + \frac{1}{p} \left(1 - \frac{1}{p} \right) \left(1 - \frac{1}{p^{1/6}} \right)^{-1} \left(1 + \frac{2}{p} - \frac{2}{p^{3/2}} \right) \right] \cdot X^{5/6}. \end{aligned} \quad (1)$$

We expect Theorem 1.1 to hold for all κ . Furthermore, since the abc conjecture implies that for $\kappa > 6$, we have $\mathcal{E}_\kappa = \mathcal{E}$, we expect these asymptotics to also hold for the family \mathcal{E} . We note that the Euler factors appearing in Theorem 1.1 arise naturally from the densities of elliptic curves over \mathbb{Q}_p with fixed Kodaira symbol. These densities are computed in Theorem 1.6.

Our next main result is on the distribution of ranks of elliptic curves in \mathcal{E}_{sf} . As in [7], we study the ranks of these elliptic curves via their 2-Selmer groups. Recall that the 2-Selmer group $\text{Sel}_2(E)$ of an elliptic curve E over \mathbb{Q} is a finite 2-torsion group which fits into the exact sequence

$$0 \rightarrow E(\mathbb{Q})/2E(\mathbb{Q}) \rightarrow \text{Sel}_2(E) \rightarrow \text{III}_E[2] \rightarrow 0, \quad (2)$$

where III_E denotes the Tate–Shafarevich group of E . Our result regarding the 2-Selmer groups of elliptic curves in \mathcal{E}_{sf} is as follows.

Theorem 1.2 *When elliptic curves in \mathcal{E}_{sf} are ordered by their conductors, the average size of their 2-Selmer groups is 3.*

Theorem 1.2 has the following immediate corollary.

Corollary 1.3 *When elliptic curves in $E \in \mathcal{E}_{\text{sf}}$ are ordered by their conductors, their average 2-Selmer rank is at most 1.5; thus, their average rank is at most 1.5 and the average rank of $\text{III}_E[2]$ is also at most 1.5.*

Corollary 1.3 provides evidence for the widely held belief that the distribution of the ranks of elliptic curves are the same regardless of whether the curves are ordered by height or conductor. Moreover, as expected, the average size of the 2-Selmer groups of curves in \mathcal{E}_{sf} are the same as the average over all elliptic curve ordered by height obtained in [7, Theorem 1.1]. We remark that our methods are flexible enough to recover verions of Theorems 1.1 and 1.2 where the families \mathcal{E}_{sf} and \mathcal{E}_κ are restricted so that the curves in them satisfy any finite set of local conditions. This result is stated as Theorem 7.1.

The key ingredient for proving the main results are “uniformity estimates” or “tail estimates”. These are upper bounds on the number of elliptic curves in our families whose discriminants are large compared to their conductors. For the proof of Theorem 1.2, we additionally need bounds on the sum of the sizes of the 2-Selmer groups of elliptic curves in \mathcal{E}_{sf} with large discriminant and small conductor. To this end, we prove the following result for the family \mathcal{E}_{sf} .

Theorem 1.4 *For positive real numbers X and M , we have*

$$\#\left\{(E, \sigma) : E \in \mathcal{E}_{\text{sf}}, C(E) < X, \frac{\Delta(E)}{C(E)} > M, \sigma \in \text{Sel}_2(E)\right\} \ll_\epsilon \frac{X^{5/6+\epsilon}}{M^{1/6}}.$$

We note that up to the power of X^ϵ , this is expected to be the optimal bound.

For the family \mathcal{E}_κ , we prove the following result.

Theorem 1.5 *Let $\kappa < 7/4$ and $\delta > 1$ be positive constants. Then there exists a positive constant θ , depending only on δ and κ , such that for every $X > 0$, we have*

$$\#\left\{E \in \mathcal{E}_\kappa : C(E) < X, \beta_E \geq \delta\right\} \ll_{\epsilon, \delta} X^{5/6-\theta+\epsilon}.$$

Complementary versions of these uniformity estimates have been obtained previously. In [7, Theorem 2.13], the authors bound the average number of 2-Selmer elements in elliptic curves E , where the height $H(E)$ is bounded and $\Delta(E)$ is divisible by the square of a large prime. These estimates were used to obtain asymptotics on the number of elliptic curves with bounded height and squarefree discriminant, as well as to compute the average size of the 2-Selmer groups of these elliptic curves. In a different direction, Fouvry–Nair–Tenenbaum [22] prove bounds on the number of elliptic curves E with large Szpiro constant β_E , when these curves are ordered by height or discriminant. Strikingly, they do not require any assumption bounding β_E from above! However, neither of these results in [7] or [22] allow for the elliptic curves in question to be ordered by conductor.

The main difficulty we face in proving Theorems 1.4 and 1.5 is that the heights and discriminants of curves with bounded conductor can grow very rapidly. Indeed, the height (and discriminant) of $E \in \mathcal{E}_{\text{sf}}$ with $C(E) = X$ can be as large as X^2 . As a consequence, the error term arising from the use of the Ekedahl sieve, a key input in the uniformity estimates of [7], is $O(X^{4/3})$, which is much too large. Subsequent improvements to the Ekedahl sieve by Taniguchi–Thorne [30], in which the sieve is combined with equidistribution methods, are also insufficient for our purposes.

We now describe the proofs of our main theorems. We study the ratios $\Delta(E)/C(E)$ of elliptic curves $E : y^2 = f(x)$ in our families by considering the associated family of cubic rings $R_f := \mathbb{Z}[x]/f(x)$ and cubic algebras $K_f := \mathbb{Q}[x]/f(x)$ over \mathbb{Q} . Let \mathcal{O}_f denote the ring of integers of K_f . Then R_f is a suborder of K_f . Define the invariants

$$\begin{aligned} Q(E) &:= [\mathcal{O}_f : R_f] \\ D(E) &:= \text{Disc}(K_f) \end{aligned}$$

which satisfy the relation

$$\Delta(E) = \text{Disc}(R_f) = Q(E)^2 D(E).$$

For primes p , we let $C_p(E)$, $\Delta_p(E)$, $Q_p(E)$, and $D_p(E)$ denote the p -parts of $C(E)$, $\Delta(E)$, $Q(E)$, and $D(E)$, respectively. The local invariants $C_p(E)$, $\Delta_p(E)$, $Q_p(E)$, and $D_p(E)$ depend only on the Kodaira symbol of E . The starting point of our proof is a determination of these local invariants along with a computation of the density of elliptic curves over \mathbb{Q}_p with fixed Kodaira symbol.

Theorem 1.6 *Fix a prime $p \geq 5$ and a Kodaira symbol T . Let $E : y^2 = f(x)$ be an elliptic curve over \mathbb{Z}_p such that the Kodaira symbol of E is T . Then the local invariants of E are as given in Table 1. Furthermore, there exists an element $t \in \mathbb{Z}_p$ such that coefficients of $f(x+t) = x^3 + ax^2 + bx + c$ are as given in the second column of Table 1. Finally, the density of all elliptic curves with Kodaira symbol T is as given in the last column.*

Kodaira Symbol of E	Congruence Condition	$C_p(E)$	$\Delta_p(E)$	$Q_p(E)$	$D_p(E)$	Density
I_0	$p \nmid \Delta(f)$	1	1	1	1	$(p-1)/p$
I_n	$p \nmid a, \quad p^{\lceil n/2 \rceil} \mid b, \quad p^n \parallel c$	p	p^n	$p^{\lfloor n/2 \rfloor}$	$p^{n \pmod{2}}$	$(p-1)^2/p^{n+2}$
II	$p \mid a, \quad p \mid b, \quad p \parallel c$	p^2	p^2	1	p^2	$(p-1)/p^3$
III	$p \mid a, \quad p \parallel b, \quad p^2 \mid c$	p^2	p^3	p	p	$(p-1)/p^4$
IV	$p \mid a, \quad p^2 \mid b, \quad p^2 \parallel c$	p^2	p^4	p	p^2	$(p-1)/p^5$
I_0^*	$p \mid a, \quad p^2 \mid b, \quad p^3 \mid c, \quad p^7 \nmid \Delta(f)$	p^2	p^6	p^3	1	$(p-1)/p^6$
I_n^*	$p \parallel a, \quad p^{\lceil n/2 \rceil + 2} \mid b, \quad p^{n+3} \parallel c$	p^2	p^{n+6}	$p^{\lfloor n/2 \rfloor + 3}$	$p^{n \pmod{2}}$	$(p-1)^2/p^{n+7}$
IV*	$p^2 \mid a, \quad p^3 \mid b, \quad p^4 \parallel c$	p^2	p^8	p^3	p^2	$(p-1)/p^8$
III*	$p^2 \mid a, \quad p^3 \parallel b, \quad p^5 \mid c$	p^2	p^9	p^4	p	$(p-1)/p^9$
II*	$p^2 \mid a, \quad p^4 \mid b, \quad p^5 \parallel c$	p^2	p^{10}	p^4	p^2	$(p-1)/p^{10}$

Table 1: Local invariants of small elliptic curves

These density computations are straightforward, and indeed many of them are implicit in the work of Watkins [31, §3.2]. However we include a proof since our use of a \mathbb{G}_a -action on the space of monic cubic polynomials simplifies the computations.

We use three different techniques to prove the estimates of Theorems 1.4 and 1.5. First, we fix a prime $p \geq 5$ and a Kodaira symbol T . The set of elliptic curves that have Kodaira symbol T at p is cut out by certain congruence conditions S modulo q , some power of p . Working modulo q , we compute the Fourier transform of the characteristic function of S . An application of Poisson summation then yields baseline estimates for the number of elliptic curves with bounded height having Kodaira symbol T at p .

Our next two techniques average over primes p in a crucial way. Suppose that $E : y^2 = f(x)$ is an elliptic curve in \mathcal{E}_{sf} such that the ratio $\Delta(E)/C(E)$ is large. Then we prove that either the discriminant of the algebra K_f is small, or that the shape of the ring of integers \mathcal{O}_f of K_f is very skewed. The work of Bhargava and Harron [5] proves that the shapes of rings of integers are equidistributed in the family of cubic fields. Furthermore, the forthcoming thesis of Chiche-Lapierre [17] determines asymptotics for the number of cubic fields such that the shapes of their ring of integers are constrained to lie within 0-density sets. Using ideas from these works, we prove bounds on the number of possible cubic algebras K_f corresponding to elliptic curves in \mathcal{E}_{sf} with bounded conductor, along with bounds on the average sizes of the 2-torsion subgroups $\text{Cl}_2(K_f)$ of the class groups of K_f . In combination with the work of Brumer–Kramer [15], relating the size of $\text{Sel}_2(E)$ to $\#\text{Cl}_2(K_f)$, we deduce Theorem 1.4.

The above method exploits the following crucial fact. If $E : y^2 = f(x)$ is an elliptic curve such that the ratio $\Delta(E)/C(E)$ is large, then primes p such that the Kodaira symbol of E at p is $I_0, I_1, I_2, \text{II},$ or III impose archimedean constraints on the algebras K_f . However, primes p with Kodaira symbol IV or I_n with

$n \geq 3$ impose only p -adic conditions on $R_f \hookrightarrow K_f$. Namely, the prime p divides the gcd of $Q(E)$ and $D(E)$. To exploit this, we proceed as follows. The set of integer monic traceless cubic polynomials f with $p \mid Q(E_f)$ embeds into the space of binary quartic forms with a rational linear factor. This embedding σ is defined in (20). The group PGL_2 acts on the space of binary quartic forms, and the ring of invariants for this action is freely generated by two polynomials I and J . Restricted to the space of reducible binary quartic forms gives an additional invariant Q . Explicitly, if $g(x, y)$ is a binary quartic form with coefficients in \mathbb{Q} , and $g(\alpha, \beta) = 0$, then define

$$Q(g(x, y), [\alpha : \beta]) = \frac{g(x, y)}{\beta x - \alpha y}(\alpha, \beta).$$

This new invariant Q is an exact analogue of the Q -invariants used in [13],[11] to compute the density of polynomials with squarefree discriminants. As there, for every fixed root $[\alpha : \beta] \in \mathbb{P}^1(\mathbb{Z})$, the discriminant polynomial on the space of integer binary quartic forms g with $g(\alpha, \beta)$ is reducible, and in fact divisible by Q^2 . We also define

$$D(g(x, y), [\alpha : \beta]) := \Delta(g)/(Q(g(x, y), [\alpha : \beta]))^2.$$

Our embedding σ satisfies $Q(E) = Q(\sigma(E))$ and $D(E) = D(\sigma(E))$. Then the required estimates on elliptic curves $E \in \mathcal{E}_\kappa$ with large $\Delta(E)/C(E)$, translate to estimates on the number of $\mathrm{PGL}_2(\mathbb{Z})$ -orbits on integral reducible binary quartic forms with bounded height and large Q - and D -invariants. We prove the required estimates by fibering over roots, and then combining geometry of numbers methods with the Ekedahl sieve.

This paper is organized as follows. In §2 and §3, we work locally, one prime at a time. Theorem 1.6 is proved in §2, while the Fourier coefficients corresponding to a fixed Kodaira symbol are computed in §3. The computation of the Fourier coefficients are then used to obtain estimates (see Theorem 3.1) on curves with fixed Kodaira symbols at finitely many primes. We prove bounds on the number of cubic fields K , weighted by $|\mathrm{Cl}_2(K)|$, in §4, and obtain estimates on the number of reducible integer binary quartic forms with large Q - and D -invariants in §5. The results of §3, §4, and §5, are combined in §6 to prove the uniformity estimates Theorems 1.4 and 1.5. Finally, in §7, we prove the main results Theorems 1.1 and 1.2.

Acknowledgments

It is a pleasure to thank Manjul Bhargava, Étienne Fouvry, Benedict Gross, Hector Pasten, Peter Sarnak, and Jacob Tsimerman for many helpful conversations and comments. The second named author is supported an NSERC Discovery Grant and a Sloan Fellowship. The third named author is supported by an NSERC Discovery Grant.

2 Reduction types of elliptic curves

Throughout this section, we fix a prime $p \geq 5$. Let U denote the space of monic cubic polynomials. Then for any ring R , we have

$$U(R) = \{x^3 + ax^2 + bx + c : a, b, c \in R\}.$$

We denote the space of traceless elements of U (i.e., $a = 0$ in the above equation) by U_0 . The group \mathbb{G}_a acts on U via $(t \cdot f)(x) = f(x + t)$. Given any element $f \in U(\mathbb{Z}_p)$, there exists a unique element $\gamma \in \mathbb{Z}_p$ such that $f_0(x) = (\gamma \cdot f)(x)$ belongs to $U_0(\mathbb{Z}_p)$. Thus we may identify the quotient space $\mathbb{Z}_p \backslash U(\mathbb{Z}_p)$ with $U_0(\mathbb{Z}_p)$. We denote the Euclidean measures on $U(\mathbb{Z}_p)$ and $U_0(\mathbb{Z}_p)$ by $dg = da db dc$ and $df = db dc$, respectively, where da , db and dc are Haar measures on \mathbb{Z}_p normalized so that \mathbb{Z}_p has volume 1. Then the change of measure formula for the bijection

$$\begin{aligned} \mathbb{Z}_p \times U_0(\mathbb{Z}_p) &\rightarrow U(\mathbb{Z}_p) \\ (t, f(x)) &\mapsto g(x) = (t \cdot f)(x) = f(x + t) \end{aligned} \tag{3}$$

is $dt df = dg$, where dt is again the Haar measure on \mathbb{Z}_p normalized so that \mathbb{Z}_p has volume 1.

Given an element $f(x) \in U(\mathbb{Z}_p)$ such that the discriminant $\Delta(f)$ is nonzero, we consider the elliptic curve E_f over \mathbb{Q}_p with affine equation $y^2 = f(x)$. An element $f(x) \in U(\mathbb{Z}_p)$ with nonzero discriminant is said to be *minimal* if $\Delta(f) = \Delta(E_f)$. Equivalently, $f(x)$ is minimal if $f_0(x) = x^3 + Ax + B$, the unique

element in $U_0(\mathbb{Z}_p)$ in the \mathbb{Z}_p -orbit of f , does not satisfy $p^4 \mid A$ and $p^6 \mid B$. Another equivalent condition is that the roots of $f_0(x)$ are not all multiples of p^2 . We denote the set of minimal elements in $U(\mathbb{Z}_p)$ by $U(\mathbb{Z}_p)^{\min}$, and denote $U(\mathbb{Z}_p)^{\min} \cap U_0(\mathbb{Z}_p)$ by $U_0(\mathbb{Z}_p)^{\min}$. The map $f \mapsto E_f$ is then a natural surjective map from $\mathbb{Z}_p \setminus U(\mathbb{Z}_p)^{\min}$ (equivalently $U_0(\mathbb{Z}_p)^{\min}$) to the set of isomorphism classes of elliptic curves over \mathbb{Q}_p .

The twisting-by- p map is a natural involution on the set of isomorphism classes of elliptic curves over \mathbb{Q}_p . This yields a natural involution σ on $\mathbb{Z}_p \setminus U(\mathbb{Z}_p)^{\min}$. If $f \in U(\mathbb{Z}_p)^{\min}$ such that $f_0(x) = x^3 + Ax + B$ with $p^2 \nmid A$ or $p^3 \nmid B$, then we say f is *small* and in this case, $\sigma(f)_0(x) = \sigma(f_0)(x) = x^3 + p^2Ax + p^3B$. Otherwise, if $f_0(x) = x^3 + Ax + B$ with $p^2 \mid A$ and $p^3 \mid B$, then we say f is *large* and in this case, $\sigma(f)_0(x) = \sigma(f_0)(x) = x^3 + p^{-2}Ax + p^{-3}B$. We have $\Delta(E_{\sigma(f)}) = p^6\Delta(E_f)$ if f is small and $\Delta(E_{\sigma(f)}) = p^{-6}\Delta(E_f)$ otherwise. Let $U(\mathbb{Z}_p)^{\text{sm}}$ denote the set of small elements $f \in U(\mathbb{Z}_p)$.

Let E be an elliptic curve over \mathbb{Q}_p , and let \mathcal{X} be a minimal proper regular model of E over \mathbb{Z}_p . For brevity, we will say that T , the Kodaira symbol associated to the special fiber of \mathcal{X} , is the Kodaira symbol of E . Define the *index* of E by $\text{ind}(E) := \Delta(E)/C(E)$. Then the index of E is 1 if and only if the Kodaira symbol of E is I_0 (when E has good reduction), I_1 , or II . Given $f \in U(\mathbb{Z}_p)^{\min}$, we define the *index* of f to be $\text{ind}(f) := \text{ind}(E_f)$. We also define two other invariants associated to elements $f \in U(\mathbb{Z}_p)^{\min}$. Let K_f denote the cubic étalé algebra $K_f := \mathbb{Q}_p[x]/f(x)$, let \mathcal{O}_f denote the ring of integers of K_f , and let R_f denote the cubic ring $\mathbb{Z}[x]/f(x)$. We define

$$\begin{aligned} Q_p(f) &:= [\mathcal{O}_f : R_f]; \\ D_p(f) &:= \text{Disc}(K_f). \end{aligned}$$

These quantities are clearly invariant under the action of \mathbb{Z}_p on $U(\mathbb{Z}_p)$ and satisfy the equation

$$\Delta(f) = \Delta(R_f) = D_p(f)Q_p(f)^2.$$

The next result gives a criterion for $f \in U(\mathbb{Z}_p)$ to be small in terms of the Kodaira symbol of E_f .

Proposition 2.1 *Let $f(x) \in U(\mathbb{Z}_p)^{\min}$ be a monic cubic polynomial corresponding to the elliptic curve E_f . Then f is small if and only if the Kodaira symbol of E_f is I_n for $n \geq 1$, II , III , or IV .*

Proof: We first note that if the Kodaira symbol of E_f is II , III , or IV , then f is small since the discriminant is less than p^6 . If f is not small, then E_f has additive reduction. Hence if the Kodaira symbol of E_f is I_n , then f is small.

Conversely, we start with fixing an element $f \in U(\mathbb{Z}_p)^{\text{sm}}$. Let $\alpha_1, \alpha_2, \alpha_3$ denote the three roots of $f(x)$ over $\overline{\mathbb{Q}_p}$, the Galois closure of \mathbb{Q}_p , and let ν_p denote the p -adic valuation on $\overline{\mathbb{Q}_p}$. We now consider the following four cases: $f(x)$ is irreducible over \mathbb{Q}_p ; $f(x)$ factors as a product of a linear and a quadratic factor over \mathbb{Q}_p , and moreover E_f has additive reduction; $f(x)$ factors as a product of a linear and a quadratic polynomial over \mathbb{Q}_p , and moreover E_f has multiplicative reduction; $f(x)$ factors into the product of three distinct linear polynomials over \mathbb{Q}_p . In what follows, we will repeatedly use [29, Table 4.1] to determine the Kodaira symbol of E_f from its reduction type and discriminant.

First suppose $f(x)$ is irreducible over \mathbb{Q}_p . The absolute Galois group of \mathbb{Q}_p acts transitively on $\alpha_1, \alpha_2, \alpha_3$. Let σ be an element sending α_1 to α_2 . If $\sigma(\alpha_3) = \alpha_3$, then $\sigma(\alpha_1 - \alpha_3) = \alpha_2 - \alpha_3$. If $\sigma(\alpha_3) = \alpha_1$, then $\sigma(\alpha_2 - \alpha_3) = \alpha_3 - \alpha_1$. Hence in either case

$$\nu_p(\alpha_1 - \alpha_3) = \nu_p(\alpha_2 - \alpha_3).$$

Similarly, we have $\nu_p(\alpha_1 - \alpha_3) = \nu_p(\alpha_1 - \alpha_2)$. Let $m \in \frac{1}{3}\mathbb{Z}$ be their common value. Let $t = (\alpha_1 + \alpha_2 + \alpha_3)/3 \in \mathbb{Z}_p$. Then replacing α_i by $\alpha_i - t$, we may assume $\nu_p(\alpha_i) \geq m$ for $i = 1, 2, 3$. On the other hand, $\nu_p(\alpha_1 - \alpha_2) \geq \max\{\nu_p(\alpha_1), \nu_p(\alpha_2)\}$. Hence $\nu_p(\alpha_i) = m$ for $i = 1, 2, 3$. Since f is integral and small, we have $0 \leq m < 1$.

If $m = 0$, then E_f has good reduction at p , and the Kodaira symbol is I_0 . If $m = 1/3$, then E_f has additive reduction at p and $\nu_p(\Delta(E_f)) = 2$. This implies that the Kodaira symbol is II . Finally, if $m = 2/3$, then E_f has additive reduction and $\nu_p(\Delta(E_f)) = 4$. It follows that the Kodaira symbol is IV .

Next suppose that $f(x)$ factors as a product of a linear and a quadratic factor over \mathbb{Q}_p , and that E_f has additive reduction. Let α_1 denote the root of the linear factor and let α_2 and α_3 denote the conjugate

roots of the quadratic factor. Then $\alpha_1, \alpha_2, \alpha_3$ are congruent modulo $p^{1/2}$. Let $t = (\alpha_1 + \alpha_2 + \alpha_3)/3$ as above. Replacing α_i by $\alpha_i - t$, we may assume

$$\nu_p(\alpha_1) \geq 1, \quad \nu_p(\alpha_2) = \nu_p(\alpha_3) = \frac{1}{2}.$$

The latter equality holds because if $p \mid \alpha_2$, then f is not small. Since α_2 and α_3 are roots of a quadratic polynomial $q(x)$ with \mathbb{Z}_p coefficients, we have $\alpha_2 + \alpha_3 \in p\mathbb{Z}_p$. Hence

$$\nu_p(\alpha_2 - \alpha_3) = \frac{1}{2}.$$

Clearly, $\nu_p(\alpha_1 - \alpha_2) = \nu_p(\alpha_1 - \alpha_3) = 1/2$. Hence, E_f has additive reduction and $\nu_p(\Delta(E_f)) = 3$. This implies that the Kodaira symbol is III.

The third case follows immediately: since E_f is assumed to have multiplicative reduction, the Kodaira symbol is I_n for some $n \geq 1$, which is sufficient. Finally, for the fourth case, suppose that f factors into a product of three linear polynomials over \mathbb{Q}_p . If the α_i are all congruent modulo p , then replacing each α_i by $\alpha_i - \alpha_1$, we see that f is not small. Hence E_f does not have additive reduction, and the Kodaira symbol is again I_n for some $n \geq 0$. This concludes the proof of the proposition. \square

Next, we prove Theorem 1.6.

Proof of Theorem 1.6: We start by assuming that $E = E_f$ corresponds to $f \in U(\mathbb{Z}_p)^{\text{sm}}$. By Proposition 2.1, the associated Kodaira symbol is I_n , II, III, or IV. We will begin with verifying the second through sixth columns of the Table 1, leaving the density computation to Proposition 2.2. The result is clear if E_f has good reduction, which happens precisely when $\Delta_p(E_f) = 1$.

First assume that E_f has additive reduction, in which case $C_p(E) = p^2$. Then the Kodaira symbol of E_f is II, III, or IV, according to whether $\Delta_p(E_f)$ is p^2 , p^3 , or p^4 , respectively. Replacing $f(x)$ with a \mathbb{Z}_p -translate, if necessary, we may assume that $f(x) \equiv x^3 \pmod{p}$. Write $f(x) = x^3 + pa_1x^2 + pb_1x + pc_1$ with $a_1, b_1, c_1 \in \mathbb{Z}_p$. Then

$$\Delta(f) \equiv 4p^3b_1^3 - 27p^2c_1^2 + 18p^3a_1b_1c_1 \pmod{p^4}$$

and $p^2 \parallel \Delta(f)$ if and only if $p \nmid c_1$. In that case, the paragraph following Lemma 13 in [9] implies that R_f is the maximal order of K_f . This confirms the second through sixth columns in the case when the Kodaira symbol is II.

If $p^3 \mid \Delta(f)$, then $p \mid c_1$. We write $c_1 = pc_2$ for some $c_2 \in \mathbb{Z}_p$, and then $\Delta(f) \equiv 4p^3b_1^3 \pmod{p^4}$. Hence $p^3 \parallel \Delta(f)$ if and only if $p \nmid b_1$. Suppose $p \nmid b_1$. Then R_f is a suborder of index p in the cubic ring \mathcal{O} corresponding to the binary cubic form $px^3 + pa_1x^2y + b_1xy^2 + c_2y^3$. The ring \mathcal{O} is maximal (from [9] as before) with $\Delta_p(\mathcal{O}) = p$, confirming the values of Q_p and D_p when the Kodaira symbol is III. Finally, suppose that $p \mid b_1$ and write $b_1 = pb_2$. Then $f(x) = x^3 + pa_1x + p^2b_2 + p^2c_2$, and since f is small, we have $p \nmid c_2$. In this case, we see that $\Delta_p(f) = p^4$ and that R_f is a suborder of index p of the maximal order \mathcal{O} corresponding to the binary cubic form $px^3 + pa_1x^2y + pb_2xy^2 + c_2y^3$ with $\Delta_p(\mathcal{O}) = p^2$. This confirms the second through sixth columns of Table 1 in the case when E_f has additive reduction and $f \in U(\mathbb{Z}_p)^{\text{sm}}$.

Next, assume that E_f has multiplicative reduction. From the proof of Proposition 2.1, it follows that $f(x)$ is not irreducible over \mathbb{Q}_p . Suppose that $f(x)$ factors into a product of a quadratic $q(x)$ and a linear polynomial $\ell(x)$ over \mathbb{Q}_p and that $f(x)$ has splitting type (1^21) . Let α_1 denote the root of the linear factor and let α_2 and α_3 denote the conjugate roots of the quadratic factor. Let $t = (\alpha_2 + \alpha_3)/2 \in \mathbb{Z}_p$. Replacing α_i by $\alpha_i - t$, we may assume

$$\nu_p(\alpha_1) = 0, \quad \nu_p(\alpha_2) = \lambda, \quad \alpha_3 = -\alpha_2$$

for some positive $\lambda \in \frac{1}{2}\mathbb{Z}$. Then $\nu_p(\alpha_2 - \alpha_3) = \nu_p(2\alpha_2) = \lambda$. Clearly, $\nu_p(\alpha_1 - \alpha_2) = \nu_p(\alpha_1 - \alpha_3) = 0$. Thus, $\Delta_p = p^{2\lambda}$ and the Kodaira symbol of E_f is $I_{2\lambda}$. Moreover, the coefficients a, b , and c of f satisfy

$$\begin{aligned} \nu_p(a) &= \nu_p(\alpha_1 + \alpha_2 + \alpha_3) = \nu_p(\alpha_1) = 0, \\ \nu_p(b) &= \nu_p(\alpha_1(\alpha_2 + \alpha_3) + \alpha_2\alpha_3) = 2\lambda, \\ \nu_p(c) &= \nu_p(\alpha_1\alpha_2\alpha_3) = 2\lambda. \end{aligned}$$

The cubic order $\mathbb{Z}_p[x]/(f(x))$ is a suborder of index $p^{\lfloor \lambda \rfloor}$ of the cubic order associated to the binary cubic form

$$p^{\lfloor \lambda \rfloor} x^3 + ax^2y + (b/p^{\lfloor \lambda \rfloor})xy^2 + (c/p^{2\lfloor \lambda \rfloor})y^3,$$

which is maximal since its discriminant is 1 when λ is an integer and p when λ is a half integer. Hence we have $Q_p(E_f) = p^{\lfloor \lambda \rfloor}$ and $D_p = p^{2\lambda \pmod{2}}$ as necessary.

Suppose instead that $f(x)$ factors as a product of three linear polynomials over \mathbb{Q}_p . By assumption, the three roots α_1, α_2 , and α_3 of $f(x)$ in \mathbb{Z}_p are not all congruent modulo p . After renaming, suppose α_2 and α_3 are congruent modulo p and α_1 is not congruent to them. Let $t = 2\alpha_3 - \alpha_2 \in \mathbb{Z}_p$. Replacing α_i by $\alpha_i - t$, we may assume α_1 is a unit and $\alpha_2 = 2\alpha_3$. That is,

$$\nu_p(\alpha_1) = 0, \quad \nu_p(\alpha_2) = \nu_p(\alpha_3) = \lambda,$$

for some positive integer $\lambda \in \mathbb{Z}$. Thus, $\Delta_p(f) = p^{2\lambda}$, which implies that the Kodaira symbol of E_f is $I_{2\lambda}$. As a consequence, the coefficients a, b , and c of f satisfy

$$\begin{aligned} \nu_p(a) &= \nu_p(\alpha_1 + \alpha_2 + \alpha_3) = 0, \\ \nu_p(b) &= \nu_p(\alpha_1(\alpha_2 + \alpha_3) + \alpha_2\alpha_3) = \lambda, \\ \nu_p(c) &= \nu_p(\alpha_1\alpha_2\alpha_3) = 2\lambda. \end{aligned}$$

The cubic order $\mathbb{Z}_p[x]/(f(x))$ is a suborder of index p^λ of the cubic order associated to the binary cubic form $p^\lambda x^3 + ax^2y + (b/p^\lambda)xy^2 + (c/p^{2\lambda})y^3$, which is maximal since its discriminant is 1. Therefore, $Q_p(E_f) = p^\lambda$ and $D_p(E_f) = 1$ as required.

We now turn to large elliptic curves. Let E be a large elliptic curve over \mathbb{Z}_p . Let E' denote the twist of E by p . Then the Kodaira symbol of E' is I_n, II, III , or IV , depending on whether the Kodaira symbol of E is I_n^*, IV^*, III^* , or II^* , respectively. Let $y^2 = f(x)$ be a model for E' , where the coefficients of $f(x) = x^3 + ax^2 + bx + c$ satisfy the congruence conditions of Table 1. Then $y^2 = g(x) = x^3 + pa^2x^2 + p^2bx + p^3c$ is a model for E . It is then easy to check that the second column of Table 1 is correct for all ten rows. Furthermore, $K_g = K_f$ and R_g has index p^3 in R_f . It follows that the local invariants of E are as in Table 1. Theorem 1.6 follows the density computations in the following proposition. \square

Proposition 2.2 *The density of elliptic curves over \mathbb{Z}_p having a fixed Kodaira symbol is as in Table 1.*

Proof: Let T be a fixed Kodaira symbol. Let $U(\mathbb{Z}_p)^{(T)}$ (resp. $U_0(\mathbb{Z}_p)^{(T)}$) denote the set of elements $f \in U(\mathbb{Z}_p)^{\min}$ (resp. $f \in U_0(\mathbb{Z}_p)^{\min}$) such that E_f has Kodaira symbol T . Then the density of elliptic curves with Kodaira symbol T is $\text{Vol}(U_0(\mathbb{Z}_p)^{(T)}) = \text{Vol}(U(\mathbb{Z}_p)^{(T)})$, where the equality holds since $\mathbb{Z}_p \cdot U_0(\mathbb{Z}_p)^{(T)} = U(\mathbb{Z}_p)^{(T)}$ and the Jacobian change of variables of the map (3) is 1.

We start with Kodaira symbol I_0 . The set $U(\mathbb{Z}_p)^{(I_0)}$ consists of those $f \in U(\mathbb{Z}_p)$ such that $f(x) \pmod{p}$ has three distinct roots in $\overline{\mathbb{F}}_p$. Denote these roots by α_1, α_2 , and α_3 . Either the α_i all belong to \mathbb{F}_p , or $\alpha_1 \in \mathbb{F}_p$ and α_2, α_3 are a pair of conjugate elements in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$, or the α_i are conjugate elements in $\mathbb{F}_{p^3} \setminus \mathbb{F}_p$. Thus, we have

$$\begin{aligned} \text{Vol}(U(\mathbb{Z}_p)^{(I_0)}) &= \frac{p(p-1)(p-2)}{6p^3} + \frac{p(p^2-p)}{2p^3} + \frac{p^3-p}{3p^3} \\ &= 1 - \frac{1}{p}, \end{aligned}$$

as required.

Second, we consider the Kodaira symbol I_n for $n \geq 1$. Suppose $f(x) \in U(\mathbb{Z}_p)^{I_n}$. Then $f(x)$ has exactly one double root modulo p . We therefore have $f(x) = g(x)(x - \alpha)$, where $g(x)$ has a double root modulo p , and $p \nmid g(\alpha)$. Clearly, we have $\Delta_p(g) = \Delta_p(f) = p^n$, since $\Delta_p(E_f) = p^n$. We write the quadratic factor $g(x)$ in unique form as $g(x) = (x + \beta)^2 + \gamma$. The discriminant condition translates to $p^n \parallel \gamma$, and the condition that $p \nmid g(\alpha)$ translates to $p \nmid (\alpha + \beta)$. Therefore, every element of $U(\mathbb{Z}_p)^{I_n}$ can be expressed uniquely in the form

$$((x + \beta)^2 + \gamma)(x - \alpha) = x^3 + (2\beta - \alpha)x^2 + (\beta^2 - 2\alpha\beta + \gamma)x - \alpha\beta^2 - \alpha\gamma,$$

such that $p^n \parallel \gamma$ and $p \nmid (\alpha + \beta)$. The Jacobian change of variables for the map $(\alpha, \beta, \gamma) \mapsto (a, b, c)$ is $-2(\alpha + \beta)^2 - 2\gamma$ which is always a unit. Thus, we have

$$\begin{aligned} \text{Vol}(U(\mathbb{Z}_p)^{I_n}) &= \text{Vol}(p^n \mathbb{Z}_p \setminus p^{n+1} \mathbb{Z}_p) \text{Vol}(\{(\alpha, \beta) \in \mathbb{Z}_p^2 : p \nmid (\alpha + \beta)\}) \\ &= (p-1)^2 / p^{n+2}, \end{aligned}$$

as required.

Third, we consider the Kodaira symbols II, III, and IV. If $f \in U_0(\mathbb{Z}_p)$ is such that the Kodaira symbol of E_f is one of the three above, then $f(x) = x^3 + Ax + B$ has a triple root modulo p , which implies that p divides A and B . By examining the discriminant of f as in the proof of Proposition 2.1, we see that the Kodaira symbol of E_f is II if and only if $p \mid A$ and $p \parallel B$; III if and only if $p \parallel A$ and $p^2 \mid B$; and IV if and only if $p^2 \mid A$ and $p^2 \parallel B$. Hence the volumes of $U_0(\mathbb{Z}_p)^{(T)}$, for $T = \text{II}, \text{III}, \text{and IV}$, are $(p-1)/p^3$, $(p-1)/p^4$, and $(p-1)/p^5$, as required.

Finally, we turn to the large Kodaira symbols, i.e., those corresponding to large elliptic curves. Consider the following map

$$\begin{aligned} \sigma : U(\mathbb{Z}_p)^{\text{sm}} &\rightarrow U(\mathbb{Z}_p) \\ x^3 + ax^2 + bx + c &\mapsto x^3 + pax^2 + p^2bx + p^3c. \end{aligned}$$

Clearly, if $S \subset U(\mathbb{Z}_p)$ is any measurable set, then $\text{Vol}(\sigma(S)) = p^{-6} \text{Vol}(S)$. Furthermore, we set $\sigma(I_n) = I_n^*$, $\sigma(\text{II}) = \text{IV}^*$, $\sigma(\text{III}) = \text{III}^*$ and $\sigma(\text{IV}) = \text{II}^*$. Then σ sends f of Kodaira symbol T to $\sigma(f)$ of Kodaira symbol $\sigma(T)$. Moreover, we have $\sigma(t \cdot f) = (pt) \cdot \sigma(f)$. Hence we have

$$\sigma(U(\mathbb{Z}_p)^{(T)}) = \sigma(\mathbb{Z}_p \cdot U_0(\mathbb{Z}_p)^{(T)}) = (p\mathbb{Z}_p) \cdot \sigma(U_0(\mathbb{Z}_p)^{(T)}).$$

Fix any $g \in U_0(\mathbb{Z}_p)^{(\sigma(T))}$. There exists $t \in \mathbb{Z}_p$ such that the coefficients of $t \cdot g$ are as in the second column of Table 1. Hence there exists $f \in U(\mathbb{Z}_p)^{(T)}$ with $\sigma(f) = t \cdot g$. Then $\sigma(f_0)$ is \mathbb{Z}_p -equivalent to g . Since $\sigma(f_0)$ and g both belong to $U_0(\mathbb{Z}_p)$, we must have $\sigma(f_0) = g$. Hence we have $\sigma(U_0(\mathbb{Z}_p)^{(T)}) = U_0(\mathbb{Z}_p)^{(\sigma(T))}$. Therefore, we have

$$\begin{aligned} \text{Vol}(U(\mathbb{Z}_p)^{(\sigma(T))}) &= \text{Vol}(\mathbb{Z}_p \cdot U_0(\mathbb{Z}_p)^{(\sigma(T))}) \\ &= p \cdot \text{Vol}(p\mathbb{Z}_p \cdot U_0(\mathbb{Z}_p)^{(\sigma(T))}) \\ &= p \cdot \text{Vol}(\sigma(U(\mathbb{Z}_p)^{(T)})) \\ &= p^{-5} \text{Vol}(U(\mathbb{Z}_p)^{(T)}). \end{aligned}$$

This concludes the proof of Proposition 2.2, and thus of Theorem 1.6. \square

Theorem 1.6 has the following immediate corollary, which will be useful in what follows.

Corollary 2.3 *Let $p \geq 5$ be a prime. The density of elliptic curves E over \mathbb{Q}_p with good, multiplicative, or additive reduction, such that $\text{ind}(E) = \Delta_p(E)/C_p(E) = p^k$ is as given in Table 2.*

3 Fourier coefficients of polynomials with fixed Kodaira symbol

Let $p \geq 5$ be a prime, and let $U(\mathbb{Z}_p)^{\text{min}}$ and $U(\mathbb{Z}_p)^{\text{sm}}$ be as in §2. Recall that to each $f(x) \in U(\mathbb{Z}_p)^{\text{min}}$, we associate the Kodaira symbol of the elliptic curve E_f . By Proposition 2.1 and Theorem 1.6, an element $f(x) \in U(\mathbb{Z}_p)^{\text{min}}$ belongs to $U(\mathbb{Z}_p)^{\text{sm}}$ and satisfies $\Delta(f) \neq C(f)$ if and only if the Kodaira symbol of f is III, IV, or I_n for $n \geq 2$. Denote the set of polynomials $f(x) \in U(\mathbb{Z})$ such that $f \in U(\mathbb{Z}_p)^{\text{min}}$ for all primes p by

Index	Good Red.	Multiplicative Red.	Additive Red.	Total
1	$(p-1)/p$	$(p-1)^2/p^3$	$(p-1)/p^3$	$(p^2-1)/p^2$
p	0	$(p-1)^2/p^4$	$(p-1)/p^4$	$(p-1)/p^3$
p^2	0	$(p-1)^2/p^5$	$(p-1)/p^5$	$(p-1)/p^4$
p^3	0	$(p-1)^2/p^6$	0	$(p-1)^2/p^6$
p^4	0	$(p-1)^2/p^7$	$(p-1)/p^6$	$(2p-1)(p-1)/p^7$
$p^k, k = 6, 7, 8$	0	$(p-1)^2/p^{k+3}$	$(2p-1)(p-1)/p^{k+3}$	$(3p-2)(p-1)/p^{k+3}$
$p^k, k = 5 \text{ or } k \geq 9$	0	$(p-1)^2/p^{k+3}$	$(p-1)^2/p^{k+3}$	$2(p-1)^2/p^{k+3}$

Table 2: p -adic densities of elliptic curves with given index

$U(\mathbb{Z})^{\min}$. Given $f(x) \in U(\mathbb{Z})^{\min}$ and a prime p , we say that the *Kodaira symbol of f at p* is T , the Kodaira symbol of $f(x)$ considered as an element in $U(\mathbb{Z}_p)^{\min}$.

Let Σ be a set consisting of the following data: a finite set $\{p_1, \dots, p_k\}$ of primes $p_i \geq 5$ along with a Kodaira symbol $T(p_i)$ which is III, IV or $I_{n \geq 2}$ associated to each prime p_i in the set. We say $f \in U(\mathbb{Z})$ has splitting type Σ if f has Kodaira symbol $T(p_i)$ at each prime p_i in Σ . Let $U(\mathbb{Z})_\Sigma$ denote the set of elements $f \in U(\mathbb{Z})$ with splitting type Σ . Given such a collection Σ , we define the constant $Q(\Sigma)$ to be $\prod_{p_i} p_i^{a_i}$, where $a_i = 1$ if $T(p_i)$ is III or IV, and $a_i = \lfloor n/2 \rfloor$ if $T(p_i)$ is I_n . Note that if $f \in U(\mathbb{Z})_\Sigma$, then $Q(\Sigma) \mid Q(f)$. We define $m_T(\Sigma)$ to be the product of all primes p such that $T(p) = T$. We also define $m_{\text{odd}}(\Sigma)$ to be the product of all primes p in Σ such that $\sigma(p) = I_n$ for some *odd* integer n . Finally, we define $\nu(\Sigma)$ to be the product over the primes p in Σ of the density $\nu(T_p)$, i.e., the p -adic volume of the set of elements in $U(\mathbb{Z}_p)^{\min}$ having Kodaira symbol $T(p)$.

Define the height function H on $U(\mathbb{R})$ to be

$$H(x^3 + ax^2 + bx + c) := \max\{|a|^6, |b|^3, |c|^2\}.$$

The goal of this section is to obtain a bound on the number of elements in $U(\mathbb{Z})$ that have bounded height and specified Kodaira symbols III, IV or $I_{n \geq 2}$ at finitely many primes. We prove the following theorem.

Theorem 3.1 *Let Σ be as above and for every Kodaira symbol T , denote $Q(\Sigma)$, $m_{\text{odd}}(\Sigma)$, and $m_T(\Sigma)$ by Q , m_{odd} , and m_T , respectively. Then we have*

$$\#\{f \in U(\mathbb{Z})_\Sigma : H(f) < Y\} \ll_\epsilon \frac{Y}{Q^2 m_{\text{III}} m_{\text{IV}}^2 m_{\text{odd}}} + \frac{Q m_{\text{odd}}}{m_{\text{IV}}} Y^\epsilon,$$

where the implied constant is independent of Y and Σ .

This section is organized as follows. First, in §3.1, we recall some preliminary results from Fourier analysis. In particular, the ‘‘twisted Poisson summation’’ formula of Proposition 3.2 will be our main tool in proving Theorem 3.1. Also, in (6), we determine how the action of \mathbb{G}_a on U changes the Fourier coefficients of functions. Next, in §3.2, we compute the Fourier coefficients of a slightly modified version of the characteristic functions of the set of monic polynomials having Kodaira symbol T , for $T = \text{III}, \text{IV}$, and $I_{n \geq 2}$. Finally, in §3.3, we use these computations and the twisted Poisson summation formula to prove Theorem 3.1.

3.1 Preliminary results from Fourier analysis

We fix a positive integer N with $(N, 6) = 1$, and consider the space $U(\widehat{\mathbb{Z}/N\mathbb{Z}})$ dual to $U(\mathbb{Z}/N\mathbb{Z})$. We write elements $\chi \in U(\widehat{\mathbb{Z}/N\mathbb{Z}})$ as triples $\chi = (\check{a}, \check{b}, \check{c}) \in (\mathbb{Z}/N\mathbb{Z})^3$, and view χ as the character given by

$$\chi(x^3 + ax^2 + bx + c) = e\left(\frac{\check{a} \cdot a + \check{b} \cdot b + \check{c} \cdot c}{N}\right), \quad (4)$$

where $e(x) := \exp(2\pi i x)$. Given a function $\phi : U(\mathbb{Z}/N\mathbb{Z}) \rightarrow \mathbb{C}$, we have the Fourier dual $\hat{\phi} : U(\widehat{\mathbb{Z}/N\mathbb{Z}}) \rightarrow \mathbb{C}$ defined to be

$$\hat{\phi}(\chi) := \sum_{f \in U(\mathbb{Z}/N\mathbb{Z})} \phi(f) \chi(f),$$

and Fourier inversion yields the equality

$$\frac{1}{N^3} \sum_x \hat{\phi}(\chi) \overline{\chi(f)} = \phi(f).$$

The additive group $\mathbb{Z}/N\mathbb{Z}$ acts on the space $U(\mathbb{Z}/N\mathbb{Z})$ via the action $(r \cdot f)(x) = f(x+r)$. Identifying $U(\mathbb{Z}/N\mathbb{Z})$ with the coefficient space $(\mathbb{Z}/N\mathbb{Z})^3$, we write the action explicitly:

$$r \cdot (a, b, c) = ((a + 3r), (b + 2ra + 3r^2), (c + rb + r^2a + r^3)).$$

Given a function $\phi : U(\mathbb{Z}/N\mathbb{Z}) \rightarrow \mathbb{C}$ and an element $r \in \mathbb{Z}/N\mathbb{Z}$, we define $r \cdot \phi : U(\mathbb{Z}/N\mathbb{Z}) \rightarrow \mathbb{C}$ to be $(r \cdot \phi)(f) := \phi((-r) \cdot f)$. We also define an action of $\mathbb{Z}/N\mathbb{Z}$ on $U(\widehat{\mathbb{Z}/N\mathbb{Z}})$ by

$$r \cdot \chi := ((\check{a} + 2r\check{b} + r^2\check{c}), (\check{b} + r\check{c}), \check{c}), \quad (5)$$

for $\chi = (\check{a}, \check{b}, \check{c})$. Then we have

$$\begin{aligned} r \cdot \widehat{\phi}(\chi) &= \sum_f (r \cdot \phi)(f) \chi(f) = \sum_f \phi((-r) \cdot f) \chi(f) = \sum_f \phi(f) \chi(r \cdot f) \\ &= \sum_{f=(a,b,c)} \phi(f) e\left(\frac{\check{a}a + \check{b}(b + 2ra) + \check{c}(c + rb + r^2a)}{N}\right) e\left(\frac{3\check{a}r + 3\check{b}r^2 + \check{c}r^3}{N}\right) \\ &= e\left(\frac{3\check{a}r + 3\check{b}r^2 + \check{c}r^3}{N}\right) \sum_{f=(a,b,c)} \phi(f) e\left(\frac{(\check{a} + 2r\check{b} + r^2\check{c})a + (\check{b} + r\check{c})b + \check{c}c}{N}\right) \\ &= \Psi_r(\chi) \hat{\phi}(r \cdot \chi), \end{aligned} \quad (6)$$

where we set

$$\Psi_r(\chi) := e\left(\frac{3\check{a}r + 3\check{b}r^2 + \check{c}r^3}{N}\right).$$

Note that if we identify elements $\chi = (\check{a}, \check{b}, \check{c}) \in U(\widehat{\mathbb{Z}/N\mathbb{Z}})$ with binary quadratic forms

$$P_\chi(x, y) := \check{a}x^2 + 2\check{b}xy + \check{c}y^2,$$

then the action of $\mathbb{Z}/N\mathbb{Z}$ on $U(\widehat{\mathbb{Z}/N\mathbb{Z}})$ in (5) corresponds exactly to the natural action:

$$P_{r \cdot \chi}(x, y) = P_\chi(x, y + rx).$$

We define $\Delta_2(\chi) = \check{b}^2 - \check{a}\check{c}$. Then Δ_2 is invariant under the action of $\mathbb{Z}/N\mathbb{Z}$. Throughout the rest of §4, we will thus identify the space $U(\widehat{\mathbb{Z}/N\mathbb{Z}})$ with the space $V_2(\mathbb{Z}/N\mathbb{Z})$, where $V_2 = \text{Sym}_2(2)$ is the space of binary quadratic forms with middle coefficient a multiple of 2.

Finally, we recall the following result which follows from the use of Poisson summation combined with the unfolding technique.

Proposition 3.2 *Let $\psi : U(\mathbb{R}) \rightarrow \mathbb{R}$ denote a smooth function with bounded support. Let $\phi : U(\mathbb{Z}/N\mathbb{Z}) \rightarrow \mathbb{R}$ be any function. Then, for every positive real number Y , we have*

$$\sum_{(a,b,c) \in U(\mathbb{Z})} \psi\left(\frac{a}{Y^{1/6}}, \frac{b}{Y^{1/3}}, \frac{c}{Y^{1/2}}\right) \phi(a, b, c) = \frac{Y}{N^3} \sum_{\chi=(\check{a}, \check{b}, \check{c}) \in \widehat{U(\mathbb{Z})}} \hat{\psi}\left(\frac{Y^{1/6}\check{a}}{N}, \frac{Y^{1/3}\check{b}}{N}, \frac{Y^{1/2}\check{c}}{N}\right) \hat{\phi}(\check{a}, \check{b}, \check{c}).$$

The $\hat{\psi}$ on the right hand side is the usual Fourier transform over \mathbb{R} and so decays faster than any polynomial.

3.2 Bounds on Fourier coefficients

Let $p \geq 5$ be a fixed prime. The conditions imposed by the choice of Kodaira symbol T being equal to III, IV or $I_{n \geq 2}$ are defined via congruence conditions modulo $N = N_p(T)$, where N is p^2 , p^2 or p^n , respectively. Hence, when we refer to an element f having one of the above Kodaira symbols, we will be implicitly assuming that f belongs to $U(\mathbb{Z}/N\mathbb{Z})$, where N is the appropriate power of p . Naturally, in this context, we will also assume that elements χ belong to $U(\widehat{\mathbb{Z}/N\mathbb{Z}})$, and represent them as triplets $(\check{a}, \check{b}, \check{c}) \in (\mathbb{Z}/N\mathbb{Z})^3$.

For a Kodaira symbol $T \in \{\text{III}, \text{IV}, I_{\geq 2}\}$, we define the set $\mathcal{S}_0(T)$ to be

$$\begin{aligned} \{x^3 + ax^2 + bx + c : p \mid a; p \mid b, p^2 \mid c\} &\subset U(\mathbb{Z}/p^2\mathbb{Z}) & \text{if } T = \text{III}; \\ \{x^3 + ax^2 + bx + c : p \mid a; p^2 \mid b, p^2 \mid c\} &\subset U(\mathbb{Z}/p^2\mathbb{Z}) & \text{if } T = \text{IV}; \\ \{x^3 + ax^2 + bx + c : p^n \mid b, p^{2n} \mid c\} &\subset U(\mathbb{Z}/p^{2n}\mathbb{Z}) & \text{if } T = I_{2n}; \\ \{x^3 + ax^2 + bx + c : p^{n+1} \mid b, p^{2n+1} \mid c\} &\subset U(\mathbb{Z}/p^{2n+1}\mathbb{Z}) & \text{if } T = I_{2n+1}. \end{aligned}$$

From the second column of Table 1, it follows that every element having Kodaira symbol T is contained within some \mathbb{G}_a translate of $\mathcal{S}_0(T)$. Let $\Phi_{0,T}$ denote the characteristic function of $\mathcal{S}_0(T)$, and define the function Φ_T by

$$\Phi_T = \sum_{r \in \mathbb{Z}/M\mathbb{Z}} r \cdot \Phi_{0,T},$$

where $M = M_p(T)$ is p if $T = \text{III}, \text{IV}$, p^n if $T = I_{2n}$ and p^{n+1} if $T = I_{2n+1}$. The next lemma, determining the Fourier transforms of the sets $\Phi_{0,T}$, follows quickly from the definitions.

Lemma 3.3 *Let $p \geq 5$ be a prime number. Let T be one the three Kodaira symbols, and let $N = N_p(T)$ denote the appropriate power of p . For $\chi = (\check{a}, \check{b}, \check{c}) \in U(\widehat{\mathbb{Z}/N\mathbb{Z}})$, we have*

$$\begin{aligned} |\widehat{\Phi_{0,\text{III}}}(\chi)| &= \begin{cases} p^2 & \text{if } p \mid \check{a}, p \mid \check{b}; \\ 0 & \text{else;} \end{cases} & |\widehat{\Phi_{0,\text{IV}}}(\chi)| &= \begin{cases} p & \text{if } p \mid \check{a}; \\ 0 & \text{else;} \end{cases} \\ |\widehat{\Phi_{0,I_{2n}}}(\chi)| &= \begin{cases} p^{3n} & \text{if } p^{2n} \mid \check{a}, p^n \mid \check{b}; \\ 0 & \text{else;} \end{cases} & |\widehat{\Phi_{0,I_{2n+1}}}(\chi)| &= \begin{cases} p^{3n+1} & \text{if } p^{2n+1} \mid \check{a}, p^n \mid \check{b}; \\ 0 & \text{else.} \end{cases} \end{aligned}$$

As an immediate consequence, 6 yield the inequality

$$|\widehat{\Phi_T}(\chi)| \leq p^{k_T} r_T(\chi), \tag{7}$$

where k_T is 2, 1, $3n$, or $3n + 1$ depending on whether T is III, IV, I_{2n} , or I_{2n+1} , respectively, and $r_T(\chi)$ is the number of $r \in \{0, \dots, M - 1\}$ such that $(r \cdot \chi)$ belongs to the support of $\widehat{\Phi_{0,T}}$. To bound $\widehat{\Phi_T}(\chi)$, it then remains to bound $r_T(\chi)$.

Lemma 3.4 *We have*

1. *Let $T = \text{III}$. Then $r_T(\chi) = 0$ unless $p \mid \Delta_2(\chi)$. In that case, $r_T(\chi) = 1$ if $p \nmid \chi$ and $r_T(\chi) = p$ otherwise.*
2. *Let $T = \text{IV}$. Then $r_T(\chi) \leq 2$ if $p \nmid \chi$ and $r_T(\chi) = p$ otherwise.*
3. *Let $T = I_{2n}$. Then $r_T(\chi) = 0$ unless χ is \mathbb{G}_a -equivalent to some element $(0, p^{n+i}\check{b}, p^j\check{c})$, for i and j nonnegative integers and $p \nmid \check{b}\check{c}$. Then $r_T(\chi) \ll p^{\min(i, \lfloor j/2 \rfloor)}$.*
4. *Let $T = I_{2n+1}$. Then $r_T(\chi) = 0$ unless χ is \mathbb{G}_a -equivalent to some element $(0, p^{n+i}\check{b}, p^j\check{c})$, for i and j nonnegative integers and $p \nmid \check{b}\check{c}$. Then $r_T(\chi) \ll p^{\min(i, \lfloor j/2 \rfloor)}$.*

Proof: We prove the above lemma in the case when $T = I_{2n}$. Assume that χ is \mathbb{G}_a -equivalent to $(0, p^{n+i}\check{b}, p^j\check{c})$, for i and j nonnegative integers and $p \nmid \check{b}\check{c}$. Note that the entry $p^j\check{c}$ does not change under the \mathbb{G}_a -action. Then by definition, we have

$$r_T(\chi) = \#\{r \in \mathbb{Z}/p^n\mathbb{Z} : p^n \mid rp^j, p^{2n} \mid 2p^{n+i}r\check{b} + r^2p^j\check{c}\}.$$

Write $r \in \mathbb{Z}/p^n\mathbb{Z}$ as $r = sp^k + p^n\mathbb{Z}$ with $p \nmid s$. Then the condition on r translates to

$$p^n \mid p^{j+k}, \quad p^{2n} \mid (2\check{b}p^{n+i+k} + s\check{c}p^{j+2k}).$$

We consider two possible cases. First assume that p^{2n} divides both $2\check{b}p^{n+i+k}$ and $s\check{c}p^{j+2k}$. Then we have $k \geq \max(n-i, n - \lfloor j/2 \rfloor)$, which implies that there are $p^{\min(i, \lfloor j/2 \rfloor)}$ choices for r . Otherwise, we have $n+i+k = j+2k =: \ell < 2n$, and $p^{2n-\ell} \mid 2\check{b} + s\check{c}$. In this case, s is determined modulo $p^{2n-\ell}$, which implies that there are $p^{n-k-(2n-\ell)} = p^{\ell-n-k}$ choices for r . Note that $\ell - n - k = i$. Furthermore, we have $j+2k = \ell < 2n$, from which it follows that $2(\ell - n - k) = 2j + 2k - 2n < j$. This proves the lemma in the case when $T = I_{2n}$. The other three cases are similar, and we omit the proof. \square

3.3 Proof of Theorem 3.1

Let Σ be as before. That is, a finite set of primes $p \geq 5$, and a Kodaira symbol $T_p = \text{III, IV, or } I_{n \geq 2}$ for each prime p in this set. For each prime p of Σ , set $N_p := N_p(T_p)$ and set $m_{\text{odd},p}$ to be p if $T_p = I_{2n+1}$ and 1 otherwise. Set Q_p to be the Q -invariant associated to T_p in Table 1. We define the quantities $N = N(\Sigma)$, $Q = Q(\Sigma)$, and $m_{\text{odd}} = m_{\text{odd}}(\Sigma)$ to be the product over all primes p of Σ of N_p , Q_p , and m_p , respectively. Note that $N = Q^2 m_{\text{odd}}$. Since Q^2 divides $\Delta(f)$ for any f with splitting type Σ , we may assume that Q and also N are bounded above by some fixed power of Y .

Then elements with splitting type Σ are defined via congruence conditions modulo N . Let $\phi : U(\mathbb{Z}/N\mathbb{Z}) \rightarrow \mathbb{R}$ denote the characteristic function of elements with splitting type Σ . Let $\psi : U(\mathbb{R}) \rightarrow \mathbb{R}_{\geq 0}$ be a smooth compactly supported function such that $\psi(f) = 1$ for $H(f) \leq 1$. We have

$$\begin{aligned} \#\{f \in U(\mathbb{Z})_\Sigma : H(f) < Y\} &\leq \sum_{(a,b,c) \in U(\mathbb{Z})_\Sigma} \psi\left(\frac{a}{Y^{1/6}}, \frac{b}{Y^{1/3}}, \frac{c}{Y^{1/2}}\right) \phi(a, b, c) \\ &= \frac{Y}{N^3} \sum_{\chi = (\check{a}, \check{b}, \check{c}) \in \widehat{U(\mathbb{Z})}} \hat{\psi}\left(\frac{Y^{1/6}\check{a}}{N}, \frac{Y^{1/3}\check{b}}{N}, \frac{Y^{1/2}\check{c}}{N}\right) \hat{\phi}(\check{a}, \check{b}, \check{c}) \\ &= S_0 + S_{\check{a}\check{c}=0} + S_{\Delta_2=0} + S_{\neq 0}, \end{aligned} \tag{8}$$

where S_0 is the contribution of the term $\chi = 0$, $S_{\check{a}\check{c}=0}$ is the contribution from the nonzero terms χ with $\check{a}\check{c} = 0$, $S_{\Delta_2=0}$ is the contribution from nonzero terms χ with $\Delta_2(\chi) = 0$, and $S_{\neq 0}$ is the contribution from the terms χ with $\check{a}\check{c}\Delta_2(\chi) \neq 0$. We bound each of these quantities in turn.

To begin with, since $\hat{\phi}(0)/N^3 = \nu(\Sigma)$ and ψ is compactly supported, we have

$$S_0 = \frac{Y}{N^3} \hat{\psi}(0) \hat{\phi}(0) \ll \nu(\Sigma) Y \ll \frac{Y}{Q^2 m_{\text{III}} m_{\text{IV}}^2 m_{\text{odd}}}, \tag{9}$$

by Table 1. To bound $S_{\check{a}\check{c}=0}$, $S_{\Delta_2=0}$ and $S_{\neq 0}$, we have the following immediate consequence of (7) and Lemma 3.4.

Corollary 3.5 *With notations as above, let $\chi = (\check{a}, \check{b}, \check{c}) \in \widehat{U(\mathbb{Z})}$ with $\hat{\phi}(\chi) \neq 0$. Let A be the largest divisor of $m_{\text{III}} m_{\text{IV}}$ dividing \check{a} , \check{b} and \check{c} . For each prime p with $T_p = I_{2n}$ or $T_p = I_{2n+1}$ for some $n \geq 1$, let k_p be the nonnegative integer with $p^{2n+k_p} \parallel \Delta_2(\chi)$. Then*

$$\hat{\phi}(\chi) \ll A m_{\text{III}}^2 m_{\text{IV}} \prod_{T_p=I_{2n}} p^{3n+k_p/2} \prod_{T_p=I_{2n+1}} p^{3n+1+k_p/2}. \tag{10}$$

Since $\hat{\psi}$ decays faster than any polynomial, it suffices to consider characters $\chi = (\check{a}, \check{b}, \check{c})$ such that

$$\check{a} \ll N^{1+\epsilon}/Y^{1/6}, \quad \check{b} \ll N^{1+\epsilon}/Y^{1/3}, \quad \check{c} \ll N^{1+\epsilon}/Y^{1/2}.$$

We consider $S_{\check{a}\check{c}=0}$ first. Fix a divisor A of $m_{\text{III}}m_{\text{IV}}$ and a nonnegative integer k_p for every prime p with $T_p = I_{\geq 2}$. The number of characters $\chi = (0, \check{b}, \check{c})$ such that A is the largest divisor of $m_{\text{III}}m_{\text{IV}}$ dividing χ and $m_{\text{III}}m_{\text{IV}} \mid \Delta_2(\chi)$ and $p^{2n+k_p} \parallel \Delta_2(\chi)$ for every prime p with $T_p = I_{2n}$ or $T_p = I_{2n+1}$ is

$$\ll_{\epsilon} \frac{N^{1+\epsilon}}{m_{\text{III}}m_{\text{IV}}Y^{1/3}} \frac{N^{1+\epsilon}}{AY^{1/2}} \prod_{T_p=I_{2n} \text{ or } I_{2n+1}} p^{-n-k_p/2}.$$

The number of choices for A and the k_p 's is $\ll Y^{\epsilon}$. Combining with the bound (10), we have

$$\frac{Y}{N^3} \sum_{\substack{\check{b} \ll N^{1+\epsilon}/Y^{1/3} \\ \check{c} \ll N^{1+\epsilon}/Y^{1/2}}} \hat{\phi}(0, \check{b}, \check{c}) \ll_{\epsilon} \frac{Y^{1/6+\epsilon}}{N} m_{\text{III}} \prod_{T_p=I_{2n}} p^{2n} \prod_{T_p=I_{2n+1}} p^{2n+1} = \frac{Y^{1/6+\epsilon}}{m_{\text{III}}m_{\text{IV}}^2}.$$

To bound the sum of $\hat{\phi}(\check{a}, \check{b}, 0)$, we need a slight refinement. Fix again a divisor A of $m_{\text{III}}m_{\text{IV}}$ and a nonnegative integer ℓ_p for every prime p with $T_p = I_{\geq 2}$. Suppose $\chi = (\check{a}, \check{b}, 0)$ with $p^{n+\ell_p} \parallel \check{b}$ for every prime p with $T_p = I_{2n}$ or $T_p = I_{2n+1}$. In order for $\widehat{\Phi}_{T_p}(\chi) \neq 0$ at these primes p , we need also $p^{n+\ell_p} \mid \check{a}$ by Lemma 3.4. If we further require that A is the largest divisor of $m_{\text{III}}m_{\text{IV}}$ dividing χ and $m_{\text{III}}m_{\text{IV}} \mid \Delta_2(\chi)$, then the number of such χ is

$$\ll_{\epsilon} \frac{N^{1+\epsilon}}{AY^{1/6}} \frac{N^{1+\epsilon}}{m_{\text{III}}m_{\text{IV}}Y^{1/3}} \prod_{T_p=I_{2n} \text{ or } I_{2n+1}} p^{-2n-2\ell_p}$$

and for any such χ , we have

$$\hat{\phi}(\chi) \ll Am_{\text{III}}^2 m_{\text{IV}} \prod_{T_p=I_{2n}} p^{3n+\ell_p} \prod_{T_p=I_{2n+1}} p^{3n+1+\ell_p}.$$

Combining these two bounds gives

$$\frac{Y}{N^3} \sum_{\substack{\check{a} \ll N^{1+\epsilon}/Y^{1/6} \\ \check{b} \ll N^{1+\epsilon}/Y^{1/3}}} \hat{\phi}(\check{a}, \check{b}, 0) \ll_{\epsilon} \frac{Y^{1/2+\epsilon}}{N} m_{\text{III}} \prod_{T_p=I_{2n}} p^n \prod_{T_p=I_{2n+1}} p^{n+1} = \frac{Y^{1/2+\epsilon}}{Qm_{\text{IV}}}.$$

Hence, we have

$$S_{\check{a}\check{c}=0} \ll_{\epsilon} \frac{Y^{1/6+\epsilon}}{m_{\text{III}}m_{\text{IV}}^2} + \frac{Y^{1/2+\epsilon}}{Qm_{\text{IV}}}. \quad (11)$$

Next we consider $S_{\Delta_2=0}$. Third, we consider $S_{\Delta_2=0}$. Note that every $\chi \in \widehat{U}(\mathbb{Z})$ with $\Delta_2(\chi) = 0$ is of the form $(\alpha^2, \alpha\beta, \beta^2)$ with $\alpha, \beta \in \mathbb{Z}$. Fix a divisor A of $m_{\text{III}}m_{\text{IV}}$ and nonnegative integers ℓ_p for each prime p with $T_p = I_{\geq 2}$. Suppose A is the largest divisor of $m_{\text{III}}m_{\text{IV}}$ dividing χ and $p^{\ell_p} \parallel \beta$ for all p with $T_p = I_{\geq 2}$. Then similar to the case of $\hat{\phi}(\check{a}, \check{b}, 0)$, we also need $p^{\ell_p} \mid \alpha$ in order for $\widehat{\Phi}_{T_p}(\chi) \neq 0$, in which case

$$\hat{\phi}(\chi) \ll Am_{\text{III}}^2 m_{\text{IV}} \prod_{T_p=I_{2n}} p^{3n+\ell_p} \prod_{T_p=I_{2n+1}} p^{3n+1+\ell_p}.$$

The number of such characters χ is

$$\ll_{\epsilon} \frac{N^{1/2+\epsilon}}{AY^{1/12}} \frac{N^{1/2+\epsilon}}{AY^{1/4}} \prod_{T_p=I_{2n} \text{ or } I_{2n+1}} p^{-2\ell_p}.$$

Combining these two bounds gives

$$S_{\Delta_2=0} \ll_{\epsilon} \frac{Y^{2/3+\epsilon}}{N^2} m_{\text{III}}^2 m_{\text{IV}} \prod_{T_p=I_{2n}} p^{3n} \prod_{T_p=T_{2n+1}} p^{3n+1} = \frac{Y^{2/3+\epsilon}}{Q m_{\text{odd}} m_{\text{III}} m_{\text{IV}}^2}. \quad (12)$$

Finally, we turn to $S_{\neq 0}$. Once again, we fix a divisor A of $m_{\text{III}} m_{\text{IV}}$ and a nonnegative integer k_p for each prime p with $T_p = I_{\geq 2}$. The number of characters $\chi = (\check{a}, \check{b}, \check{c})$ such that A is the largest divisor of $m_{\text{III}} m_{\text{IV}}$ dividing χ , $m_{\text{III}} m_{\text{IV}} \mid \Delta_2(\chi)$ and $p^{2n+k_p} \parallel \Delta_2(\chi)$ for any prime p with $T_p = I_{2n}$ or $T_p = T_{2n+1}$ is

$$\ll_{\epsilon} Y^{\epsilon} \frac{N^{1+\epsilon}}{A Y^{1/3}} \frac{N^{2+\epsilon}}{m_{\text{III}} m_{\text{IV}} Y^{2/3}} \prod_{T_p=I_{2n} \text{ or } I_{2n+1}} p^{-2n-k_p}.$$

Indeed, the above bounds the number of pairs $(\check{b}, \Delta_2(\chi))$ satisfying the desired divisibility conditions, and given \check{b} and $\Delta_2(\chi)$, there are Y^{ϵ} choices for \check{a} and \check{c} . Combining with (10) then gives

$$S_{\neq 0} \ll_{\epsilon} Y^{\epsilon} m_{\text{III}} \prod_{T_p=I_{2n}} p^n \prod_{T_p=I_{2n+1}} p^{n+1} = \frac{Q m_{\text{odd}}}{m_{\text{IV}}} Y^{\epsilon}. \quad (13)$$

Theorem 3.1 now follows from (8), (9), (11), (12), (13), and the AM-GM inequality.

4 The family of cubic fields with prescribed shapes

A cubic ring is a commutative ring with unit that is free of rank 3 as a \mathbb{Z} -module. Given a cubic ring R , the *trace* $\text{Tr}(\alpha)$ of an element $\alpha \in R$ is the trace of the linear map $\times \alpha : R \rightarrow R$. The *discriminant* $\text{Disc}(R)$ of R is then the determinant of the bilinear pairing

$$R \times R \rightarrow \mathbb{Z}, \quad (\alpha, \beta) := \text{Tr}(\alpha\beta).$$

Given a *nondegenerate* cubic ring R , i.e., a cubic ring R with nonzero discriminant, we then consider the cubic étalé algebras $R \otimes \mathbb{Q}$ over \mathbb{Q} and $R \otimes \mathbb{R}$ over \mathbb{R} . There are two possibilities for $R \otimes \mathbb{R}$, namely, \mathbb{R}^3 and $\mathbb{R} \oplus \mathbb{C}$. We have $R \otimes \mathbb{R} \cong \mathbb{R}^3$ when $\text{Disc}(R) > 0$ (equivalently, when the signature of $R \otimes \mathbb{Q}$ is $(3, 0)$) and $R \otimes \mathbb{R} \cong \mathbb{R} \oplus \mathbb{C}$ when $\text{Disc}(R) < 0$ (equivalently, when the signature of $R \otimes \mathbb{Q}$ is $(1, 2)$).

The ring R embeds as a lattice into $R \otimes \mathbb{R}$ with covolume $\sqrt{|\text{Disc}(R)|}$. As regarded as this lattice, the element $1 \in R$ is part of any Minkowski basis, and so the first successive minima of R is simply 1. Let $\ell_1(R) \leq \ell_2(R)$ denote the other two successive minima of R . We define the *skewness* of R by

$$\text{sk}(R) := \ell_2(R)/\ell_1(R).$$

Given a field K , we denote the ring of integers of K by \mathcal{O}_K , and the class group of K by $\text{Cl}(K)$. For positive real numbers X and Z , let $\mathcal{R}_3^{\pm}(X, Z)$ denote the set of cubic fields K that satisfy the following two bounds: $X \leq \pm \text{Disc}(\mathcal{O}_K) < 2X$ and $\text{sk}(\mathcal{O}_K) > Z$. Set $\mathcal{R}_3(X, Z)$ to be the union $\mathcal{R}_3^+(X, Z) \cup \mathcal{R}_3^-(X, Z)$. In this section, we prove the following result.

Theorem 4.1 *Let X and Z be positive real numbers. Then*

$$\sum_{K \in \mathcal{R}_3(X, Z)} |\text{Cl}(K)[2]| \ll X/Z,$$

where the implied constants are independent of X and Z .

This section is organized as follows. In Section 4.1 we recall the parametrization of cubic rings and of 2-torsion elements in the class groups of cubic rings, in terms of integral orbits for the action of $\text{GL}_2(\mathbb{Z})$ on $\text{Sym}^3(\mathbb{Z}^2)$ and of $\text{GL}_2(\mathbb{Z}) \times \text{SL}_3(\mathbb{Z})$ on $\mathbb{Z}^2 \otimes \text{Sym}^2(\mathbb{Z}^3)$, respectively. In §4.2 and §4.3, we then prove Theorem 4.1 using these parametrizations in conjunction with geometry-of-numbers methods.

4.1 The parametrization of cubic rings and the 2-torsion in their class groups

In this section, we recall two parametrizations. First, the parametrization of cubic rings, due to Levi [28], Delone–Faddeev [20], and Gan–Gross–Savin [23], and second, Bhargava’s parametrization [2] of elements in the 2-torsion subgroups of cubic rings. Let $V_3 = \text{Sym}^3(2)$ denote the space of binary cubic forms. We consider the *twisted action* of GL_2 on V_3 given by

$$(\gamma \cdot f)(x, y) := \frac{1}{\det \gamma} f((x, y) \cdot \gamma),$$

for $\gamma \in \text{GL}_2$ and $f(x, y) \in V_3$. Then we have the following result.

Theorem 4.2 ([28, 20, 23]) *There is a natural bijection between the set of $\text{GL}_2(\mathbb{Z})$ -orbits on $V_3(\mathbb{Z})$ and the set of cubic rings.*

We collect some well known facts about the above bijection (for proofs and a more detailed discussion, see [9, §2]). For an integral binary cubic form f , we denote the corresponding cubic ring by R_f . The bijection is discriminant preserving, i.e., we have $\Delta(f) = \text{Disc}(R_f)$. The ring R_f is an integral domain if and only if f is irreducible over \mathbb{Q} . The group of automorphisms of R_f is isomorphic to the stabilizer of f in $\text{GL}_2(\mathbb{Z})$.

The bijection of Theorem 4.2 can be explicitly described as follows: given a cubic ring R , consider the map $R/\mathbb{Z} \rightarrow \wedge^2(R/\mathbb{Z}) \cong \mathbb{Z}$ given by $r \mapsto r \wedge r^2$. This map is easily seen to be a cubic map and gives the binary cubic form corresponding to R . In fact, this map yields the finer bijection

$$V_3(\mathbb{Z}) \longleftrightarrow \{(R, \omega, \theta)\}, \quad (14)$$

where R is a cubic ring and $\langle \omega, \theta \rangle$ is a basis for the 2-dimensional \mathbb{Z} -module R/\mathbb{Z} . The integral binary cubic form corresponding to (R, ω, θ) is $f(x, y)$, where

$$(x\omega + y\theta) \wedge (x\omega + y\theta)^2 = f(x, y)(\omega \wedge \theta). \quad (15)$$

It is easily seen that the actions of $\text{GL}_2(\mathbb{Z})$ on $V_3(\mathbb{Z})$ and on the set of triples (R, ω, θ) agree. Here the latter action is given simply by the natural action of $\text{GL}_2(\mathbb{Z})$ on the basis $\{\omega, \theta\}$ of R/\mathbb{Z} .

Let f be an integral binary cubic form, and let (R, ω, θ) be the corresponding triple. Fix an element $\alpha = n + a\omega + b\theta$ of R , where $n, a,$ and b are integers and $(a, b) \neq (0, 0)$. The ring $\mathbb{Z}[\alpha]$ is a subring of R having finite index denoted $\text{ind}(\alpha)$. It follows from (15) that we have

$$\text{ind}(\alpha) = f(a, b). \quad (16)$$

Clearly $\text{ind}(\alpha) = \text{ind}(\alpha + n)$ for $n \in \mathbb{Z}$. Finally, we note that the bijections of Theorem 4.2 and (15) continue to hold if \mathbb{Z} is replaced by any principal ideal domain [12, Theorem 5].

Next, we describe the parametrization of 2-torsion ideals in the class groups of cubic rings. Let W denote the space $2 \otimes \text{Sym}^2(3)$ of pairs of ternary quadratic forms. For a ring S , we write elements $(A, B) \in W(S)$ as a pair of 3×3 symmetric matrices with coefficients in S . The group $G_{2,3} = \text{GL}_2 \times \text{SL}_3$ acts on W via the action $(\gamma_2, \gamma_3) \cdot (A, B) := (\gamma_3 A \gamma_3^t, \gamma_3 B \gamma_3^t) \gamma_2^t$. We have the *resolvent map* from W to V_3 given by

$$\begin{aligned} W &\rightarrow V_3 \\ (A, B) &\mapsto \det(Ax + By). \end{aligned}$$

The resolvent map respects the group actions on W and V_3 : we have

$$\text{Res}((\gamma_2, \gamma_3) \cdot (A, B)) = (\det \gamma_2) \cdot \text{Res}(A, B). \quad (17)$$

The following result parametrizing 2-torsion ideals in cubic rings is due to Bhargava [2, Theorem 4].

Theorem 4.3 ([2]) *There is a bijection between $\text{GL}_2(\mathbb{Z}) \times \text{SL}_3(\mathbb{Z})$ -orbits on $W(\mathbb{Z})$ and equivalence classes of triples (R, I, δ) , where R is a cubic ring, $I \subset R$ is an ideal of R having rank-3 as a \mathbb{Z} -module, and δ is an invertible element of $R \otimes \mathbb{Q}$ such that $I^2 \subset (\delta)$ and $N(I)^2 = N(\delta)$. Here two triples (R, I, δ) and (R', I', δ') are equivalent if there exists an isomorphism $\phi : R \rightarrow R'$ and an element $\kappa \in R \otimes \mathbb{Q}$ such that $I' = \phi(\kappa I)$ and $\delta' = \phi(\kappa^2 \delta)$. Moreover, the ring R of the triple corresponding to a pair (A, B) is the cubic ring corresponding to $\text{Res}(A, B)$ under the Delone–Faddeev parametrization.*

When $R = R_f$ is the maximal order in a cubic field K , the above result gives a bijection between the set of $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ -orbits on the set of pairs $(A, B) \in W(\mathbb{Z})$ with resolvent f , and the set of equivalence classes of pairs (I, δ) , where I is an ideal of R , $\delta \in K$ and $I^2 = (\delta)$. This latter set is termed the 2-Selmer group $\mathrm{Sel}_2(K)$ of K (see Definition 5.2.4 and Proposition 5.2.8 of [18]) and fits into the exact sequence

$$1 \rightarrow R^\times / (R^\times)^2 \rightarrow \mathrm{Sel}_2(K) \rightarrow \mathrm{Cl}(K)[2] \rightarrow 1,$$

where R^\times denotes the unit group of K . Thus bounds on the 2-Selmer group of K directly imply bounds on the 2-torsion subgroup of the class group of K .

4.2 The number of cubic fields with bounded discriminants and skewed rings of integers

The goal of this section is to prove the following result.

Proposition 4.4 *Let X and Z be positive real numbers. There exists some constant C such that $\mathcal{R}_3^\pm(X, Z)$ is empty if $Z > CX^{1/6}$. Otherwise $|\mathcal{R}_3^\pm(X, Z)| = O(X/Z)$.*

For any subset S of $V_3(\mathbb{R})$, let S^\pm denote the set of elements f such that $\pm\Delta(f) > 0$. Then $V_3(\mathbb{R})^+$ (resp. $V_3(\mathbb{R})^-$) consists of a single $\mathrm{GL}_2(\mathbb{R})$ -orbit and corresponds to the cubic algebra \mathbb{R}^3 (resp. $\mathbb{R} \oplus \mathbb{C}$). We denote this cubic \mathbb{R} -algebra by R^\pm . Let \mathcal{F}_2 denote Gauss' fundamental domain for the action of $\mathrm{GL}_2(\mathbb{Z})$ on $\mathrm{GL}_2(\mathbb{R})$. We write elements of $\mathrm{GL}_2(\mathbb{R})$ in Iwasawa coordinates, in which case we have

$$\mathcal{F}_2 = \{n\alpha k\lambda : n \in N'(t), \alpha(t) \in A', k \in K, \lambda \in \Lambda\},$$

where,

$$N'(t) = \left\{ \begin{pmatrix} 1 & \\ u & 1 \end{pmatrix} : u \in \nu(t) \right\}, \quad A' = \left\{ \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} : t \geq \sqrt[4]{3}/\sqrt{2} \right\}, \quad \Lambda = \left\{ \begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix} : \lambda > 0 \right\}, \quad (18)$$

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 . Elements $n\alpha(t)k\lambda$ are expressed in their Iwasawa coordinates as (n, t, λ, k) . Fix compact sets $B^\pm \subset V_3(\mathbb{R})^\pm$ that are closures of open bounded sets. Then for every point $v \in B^\pm$, the set $\mathcal{F}_2 \cdot v$, viewed as a multiset, is a cover of a fundamental domain for the action of $\mathrm{GL}_2(\mathbb{Z})$ on $V_3(\mathbb{R})^\pm$ of absolutely bounded degree. Recall that for a cubic ring R , its skewness $\mathrm{sk}(R)$ is defined to be the quotient $\ell_2(R)/\ell_1(R)$ where $1, \ell_1(R), \ell_2(R)$ are the successive minima of R , regarded as a lattice inside $R \otimes \mathbb{R}$. We have the following lemma.

Lemma 4.5 *Let $v \in B^\pm$ be any binary cubic form. Let $\gamma = (n, t, \lambda, k) \in \mathcal{F}_2$ be such that $f = \gamma \cdot v$ is an integral binary cubic form. Then we have*

$$\mathrm{sk}(R_f) \asymp t^2$$

where R_f denotes the cubic ring corresponding to f .

Proof: Every binary cubic form v in $V_3(\mathbb{R})^\pm$ gives rise to the cubic algebra R^\pm , where $R^+ \cong \mathbb{R}^3$ and $R^- \cong \mathbb{C} \oplus \mathbb{R}$, along with elements α_v and β_v such that $\langle 1, \alpha_v, \beta_v \rangle$ form a basis for R^\pm . Furthermore, the lattice spanned by $1, \alpha_v$, and β_v has covolume $\sqrt{|\Delta(v)|}$. Since B^\pm is compact, it follows that we have $|\alpha_v| \cdot |\beta_v| \ll \sqrt{|\Delta(v)|}$ for $v \in B^\pm$. Additionally, the action of $\mathrm{GL}_2(\mathbb{R})$ on $V_3(\mathbb{R})$ agrees with the action of $\mathrm{GL}_2(\mathbb{R})$ on pairs (α_v, β_v) by linear change of variables. That is, we have $(\alpha_{\gamma \cdot v}, \beta_{\gamma \cdot v}) = \gamma \cdot (\alpha_v, \beta_v)$.

Let $f = \gamma \cdot v$ be an integral binary cubic form as in the statement of the lemma. Since $\gamma \in \mathcal{F}_2$, it follows that $|\alpha_f| \asymp \lambda t^{-1}$ and $|\beta_f| \asymp \lambda t$. As a consequence, $|\alpha_f| \cdot |\beta_f| \asymp \sqrt{\mathrm{Disc}(f)}$. Therefore, we have $\ell_2(R_f)/\ell_1(R_f) \asymp |\beta_f|/|\alpha_f| \asymp t^2$ as necessary. \square

Next, we have the following lemma, due to Davenport [19], that estimates the number of lattice points within regions of Euclidean space.

Proposition 4.6 ([19]) *Let \mathcal{R} be a bounded, semi-algebraic 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 .

We are now ready to prove Proposition 4.4.

Proof of Proposition 4.4: A general version of the first claim of the proposition, applying to number fields of all degrees, is obtained in [8, Theorem 3.1], and further generalizations are proved in [17]. For completeness, we include a proof for our case below. Let K be a cubic field whose ring of integers \mathcal{O}_K belongs to $\mathcal{R}_3^\pm(X, Z)$, and let $\langle 1, \alpha, \beta \rangle$ be a Minkowski basis for \mathcal{O}_K with $|\alpha| \leq |\beta|$. Consider the ring $\mathbb{Z}[\alpha]$ which is a suborder of \mathcal{O}_K . We have

$$X^{1/2} \asymp \sqrt{\text{Disc}(\mathcal{O}_K)} \ll \sqrt{\text{Disc}(\mathbb{Z}[\alpha])} \ll |\alpha|^3,$$

and it follows that $|\alpha| \gg X^{1/6}$. Since $|\alpha||\beta| \asymp X^{1/2}$, we have $Z = |\beta|/|\alpha| \ll X^{1/2}/X^{2/6} = X^{1/6}$ and the first claim of the proposition follows.

We now estimate $|\mathcal{R}_3^\pm(X, Z)|$ under the assumption that $Z \ll X^{1/6}$ following the setup of [9, §5]. Let v be an element of the compact set B^\pm . If $(n, t, \gamma, k) \cdot v$ corresponds to an cubic ring R with $X \leq \text{Disc}(R) < 2X$ and $\text{sk}(R) > Z$, then it follows that $\lambda \asymp X^{1/4}$ and $t \gg Z^{1/2}$, respectively, where the latter fact follows from Lemma 4.5. Hence we have

$$\begin{aligned} |\mathcal{R}_3^\pm(X, Z)| &\leq \int_{\substack{g=(n,t,\lambda,k) \in \mathcal{F}_2 \\ \lambda \asymp X^{1/4} \\ t \gg Z^{1/2}}} \#\{g \cdot B^\pm \cap V_3(\mathbb{Z})^{\text{irr}}\} dg \\ &\leq \int_{\substack{g=(n,t,\lambda,k) \in \mathcal{F}_2 \\ \lambda \asymp X^{1/4} \\ Z^{1/2} \ll t \ll X^{1/12}}} \#\{g \cdot B^\pm \cap V_3(\mathbb{Z})\} dg, \end{aligned}$$

where the second inequality follows from the observation that if $t \gg X^{1/12}$, then every element $f(x, y)$ in $g \cdot B^\pm$ has x^3 -coefficient less than 1 in absolute value. Therefore no such integral element $f(x, y)$ can be irreducible since its x^3 -coefficient must be 0. Applying Proposition 4.6 on the set $g \cdot B^\pm$, we obtain

$$\begin{aligned} |\mathcal{R}_3^\pm(X, Z)| &\ll \int_{\lambda \asymp X^{1/4}} \int_{Z^{1/2} \ll t \ll X^{1/12}} (\lambda^4 + \lambda^3 t^3) t^{-2} d^\times t d^\times \lambda \\ &\ll \frac{X}{Z} + X^{5/6} \ll \frac{X}{Z}, \end{aligned}$$

since $Z \ll X^{1/6}$. The proposition follows. \square

We end this subsection with a counting result on the number of primitive algebraic integers in a cubic field of bounded size to be used in Section 6.1. We say an element α in a ring R is *primitive* if $\alpha \neq n\beta$ for any $\beta \in R$ and any integer $n \geq 2$. We use the superscript $\text{Tr} = 0$ to denote the subset of elements of trace 0.

Lemma 4.7 *Let K be a cubic field with discriminant D . For any real number $Y > 0$, let $N_K(Y)$ denote the number of primitive elements $\alpha \in \mathcal{O}_K^{\text{Tr}=0}$ with $|\alpha| < Y$. Then*

$$N_K(Y) \leq \begin{cases} 0 & \text{if } Y < \ell_1(K); \\ 1 & \text{if } \ell_1(K) \leq Y < \ell_2(K); \\ \frac{Y^2}{\sqrt{D}} + O\left(\frac{Y}{\ell_1(K)}\right) & \text{if } \ell_2(K) \leq Y. \end{cases} \quad (19)$$

Note that if $\ell_2(K) \leq Y$, then $\frac{Y}{\ell_1(K)} \ll \frac{Y^2}{\sqrt{D}}$ and so we simply have $N_K(Y) \ll \frac{Y^2}{\sqrt{D}}$, which is the best possible bound in this case.

Proof: The first two lines of (19) are clearly true. In fact, they are equalities. Then final claim follows from Proposition 4.6 by replacing $N_K(Y)$ by the overcount where we count all (not merely primitive) traceless elements $\alpha \in \mathcal{O}_K$, since $\mathcal{O}_K^{\text{Tr}=0}$ considered as a lattice inside $(K \otimes \mathbb{R})^{\text{Tr}=0}$ has covolume \sqrt{D} . \square

4.3 The 2-torsion subgroups in the class groups of cubic fields

Let K be a cubic field, and let $f \in V_3(\mathbb{Z})$ be the binary cubic form corresponding to \mathcal{O}_K , the ring of integers of K . A consequence of Theorem 4.3 is that the set of 2-torsion elements in the class group of K injects into the set of $\text{SL}_3(\mathbb{Z})$ -orbits on the elements $(A, B) \in W(\mathbb{Z})$ satisfying $\text{Res}(A, B) = f$.

Choose Iwasawa coordinates (n, t, λ, k_2) for $\text{GL}_2(\mathbb{R})$ as in the previous subsection and (u, s_1, s_2, k_3) for $\text{SL}_3(\mathbb{R})$ as in [3, §2.1]. A Haar-measure for $\text{SL}_3(\mathbb{R})$ in these coordinates is $s_1^{-6} s_2^{-6} du dk_3 d^\times s_1 d^\times s_2$. Let \mathcal{F}_3 denote a fundamental domain for the action of $\text{SL}_3(\mathbb{Z})$ on $\text{SL}_3(\mathbb{R})$, such that \mathcal{F}_3 is contained within a standard Seigel domain in $\text{SL}_3(\mathbb{R})$. Then $\mathcal{F}_{2,3} := \mathcal{F}_2 \times \mathcal{F}_3$ is a fundamental domain for the action of $G_{2,3}(\mathbb{Z})$ on $G_{2,3}(\mathbb{R})$. There are four $G_{2,3}(\mathbb{R})$ -orbits having nonzero discriminant on $W(\mathbb{R})$, and we denote them by $W(\mathbb{R})^{(i)}$, $1 \leq i \leq 4$. For each i , let $\mathcal{B}_i \subset W(\mathbb{R})^{(i)}$ be compact sets, which are closures of open sets, such that $\text{Res}(\mathcal{B}_i) \subset B^+ \cup B^-$, where B^+ and B^- are as in the previous subsection. For each element $w \in \mathcal{B}_i$, the set $\mathcal{F}_{2,3} \cdot w$ is a cover of a fundamental domain for the action of $G_{2,3}(\mathbb{Z})$ on $W(\mathbb{R})^{(i)}$. Let \mathcal{B} denote the union of the \mathcal{B}_i .

Next, let $W(\mathbb{Z})^{\text{irr}}$ denote the set of elements $(A, B) \in W(\mathbb{Z})$ such that the resolvent of (A, B) corresponds to an integral domain, and such that A and B have no common root in $\mathbb{P}^2(\mathbb{Q})$. Elements in $W(\mathbb{Z})$ that are not in $W(\mathbb{Z})^{\text{irr}}$ are said to be *reducible*. Given a reducible element w with resolvent f , either R_f is not an integral domain or w corresponds to the identity element in the class group of R_f . We now have the following lemmas.

Lemma 4.8 *Let $g = (g_2, g_3)$ be an element in $\mathcal{F}_{2,3}$, where $g_2 = (n, t, k_2, \lambda) \in \mathcal{F}_2$ and $g_3 \in \mathcal{F}_3$. Let (A, B) be an integral element in $g \cdot \mathcal{B}$ such that $\text{Res}(A, B) = f$. Then we have*

$$\Delta(f) \asymp \lambda^{12}; \quad \text{sk}(R_f) \asymp t^2.$$

Proof: The lemma follows immediately from (17) in conjunction with Lemma 4.5 and the fact that Δ is a degree-4 homogeneous polynomial in the coefficients of V_3 . \square

Lemma 4.9 *Let (A, B) be an element in $W(\mathbb{Z})$. Denote the coefficients of A and B by a_{ij} and b_{ij} , respectively. If $\det(A) = 0$ or $a_{11} = b_{11} = 0$, then (A, B) is reducible.*

Proof: If $\det(A) = 0$, then the cubic resolvent of (A, B) has x^3 -coefficient 0, implying that (A, B) is reducible. If $a_{11} = b_{11} = 0$ then A and B have a common zero in $\mathbb{P}^2(\mathbb{Q})$, implying that (A, B) corresponds to the identity element in the class group of R_f . \square

We are now ready to prove the second claim of Theorem 4.1.

Proof of Theorem 4.1: We follow the setup and methods of [3]. To begin with, averaging over $w \in \mathcal{B}$ as in [3, (6) and (8)], we obtain

$$\begin{aligned} & \sum_{K \in \mathcal{R}_3^\pm(X, Z)} (|\text{Cl}(K)[2]| - 1) \\ & \ll \int_{g \in \mathcal{F}_{2,3}} |\{w \in g \cdot \mathcal{B} \cap W(\mathbb{Z})^{\text{irr}} : K_{\text{Res}(w)} \in \mathcal{R}_3(X, Z)\}| dg \\ & \ll \int_{s_1, s_2, t \gg 1} |\{w \in ((\lambda, t), (s_1, s_2)) \cdot \mathcal{B} \cap W(\mathbb{Z})^{\text{irr}} : K_{\text{Res}(w)} \in \mathcal{R}_3(X, Z)\}| \frac{d^\times \lambda d^\times t d^\times s_1 d^\times s_2}{t^2 s_1^6 s_2^6}, \end{aligned}$$

where K_f denotes the algebra $\mathbb{Q} \otimes R_f$ for an integral binary cubic form f .

The action of an element $((\lambda, t), (s_1, s_2)) \in \mathcal{F}_{2,3}$ on $W(\mathbb{R})$ multiplies each coordinate c_{ij} of W by a factor which we denote by $w(c_{ij})$. For example, we have $w(a_{11}) = \lambda t^{-1} s_1^{-4} s_2^{-2}$. The volume of \mathcal{B} is some positive constant, and when \mathcal{B} is translated by an element $((\lambda, t), (s_1, s_2))$, the volume is multiplied by a factor of λ^{12} , the product of $w(c_{ij})$ over all the coordinates c_{ij} . Furthermore, the maximum of the volumes of the projections of $((\lambda, t), (s_1, s_2)) \cdot \mathcal{B}$ is

$$\ll \prod_{c_{ij} \in S} w(c_{ij}) = \prod_{c_{ij} \notin S} \lambda^{12} w(c_{ij}),$$

where S denotes the set of coordinates c_{ij} of $W(\mathbb{R})$ such that the length of the projection of $((\lambda, t), (s_1, s_2)) \cdot \mathcal{B}$ onto the c_{ij} -coordinate is at least $\gg 1$.

For the set $((\lambda, t), (s_1, s_2)) \cdot \mathcal{B} \cap W(\mathbb{Z})^{\text{irr}}$ to be empty, it is necessary that the projection of $\mathcal{B}' := ((\lambda, t), (s_1, s_2)) \cdot \mathcal{B}$ onto the b_{11} -coordinate is $\gg 1$. Otherwise, every integral element of \mathcal{B}' has $a_{11} = b_{11} = 0$, and is hence reducible by Lemma 4.9. Similarly, the projections of \mathcal{B}' onto the a_{13} - and a_{22} -coordinates are also $\gg 1$ (since otherwise every integral element (A, B) of \mathcal{B}' satisfy $\det(A) = 0$). Finally, for $\mathcal{B}' \cap W(\mathbb{Z})$ to contain an element whose resolvent cubic form corresponds to a field in $\mathcal{R}_3(X, Z)$, we must have $\lambda \asymp X^{1/12}$ and $Z^{1/2} \ll t \ll X^{1/2}$ by Lemma 4.8.

Therefore, applying Proposition 4.6 to the sets $((\lambda, t), (s_1, s_2)) \cdot \mathcal{B}$, we obtain

$$\begin{aligned} \sum_{K \in \mathcal{R}_3^\pm(X, Z)} (|\text{Cl}(K)[2]| - 1) &\ll \int_{\substack{\lambda, t, s_1, s_2 \\ \lambda \asymp X^{1/12} \\ Z^{1/2} \ll t \ll X^{1/2} \\ s_1, s_2 \gg 1}} (\lambda^{12} (1 + w(a_{11})^{-1} + w(a_{11}a_{12})^{-1}) \frac{d^\times \lambda d^\times t d^\times s_1 d^\times s_2}{t^2 s_1^6 s_2^6}) \\ &\ll \int_{\substack{\lambda, t, s_1, s_2 \\ \lambda \asymp X^{1/12} \\ Z^{1/2} \ll t \ll X^{1/2} \\ s_1, s_2 \gg 1}} (\lambda^{12} + s_1^4 s_2^2 t \lambda^{11} + s_1^4 s_2^4 t^2 \lambda^{10}) \frac{d^\times \lambda d^\times t d^\times s_1 d^\times s_2}{t^2 s_1^6 s_2^6} \\ &\ll X/Z + X^{11/12}/Z^{1/2} + X^{5/6+\epsilon}, \end{aligned}$$

which is sufficient since $Z \ll X^{1/6}$. Theorem 4.1 now follows from this bound and Proposition 4.4.

5 Embedding into the space of binary quartic forms

Recall that $U_0(\mathbb{Z})$ denotes the set of monic cubic polynomials with zero x^2 -coefficient, and $U_0(\mathbb{Z})^{\text{min}}$ denotes the set of elements $f(x) \in U_0(\mathbb{Z})$ such that the elliptic curve $y^2 = f(x)$ has minimal discriminant among all its quadratic twists. We define the height function $H : U_0(\mathbb{Z}) \rightarrow \mathbb{R}_{\geq 0}$ by

$$H(x^3 + Ax + B) = \max\{4|A|^3, 27B^2\}.$$

For $f(x) \in U_0(\mathbb{Z})$, we write $K_f = \mathbb{Q}[x]/(f(x))$, $R_f = \mathbb{Z}[x]/(f(x))$, and let \mathcal{O}_f denote the maximal order in K_f . The Q -invariant $Q(f)$ of f is defined as the index of R_f in \mathcal{O}_f , and $D(f)$ is defined to be the discriminant of K_f . Observe from Table 1 that for primes p of type III, IV and I_{2n+1} , we have $p \mid Q(f)$ and $p \mid D(f)$. Note also $\gcd(Q(f), D(f))$ is squarefree.

In this section, we obtain a bound on the number of elements $f \in U_0(\mathbb{Z})^{\text{min}}$, having bounded height, such that both $Q(f)$ and $\gcd(Q(f), D(f))$ are large.

Theorem 5.1 *Let Q and q be positive real numbers with $Q \geq q$. Let $N_{Q,q}(Y)$ denote the number of elements $f(x) \in U_0(\mathbb{Z})^{\text{min}}$ such that $H(f) < Y$, $|Q(f)| > Q$, and $\gcd(Q(f), D(f)) > q$. Then*

$$N_{Q,q}(Y) \ll_\epsilon \frac{Y^{5/6+\epsilon}}{qQ} + \frac{Y^{7/12+\epsilon}}{Q^{1/2}},$$

where the implied constant is independent of Q , q and Y .

This section is organized as follows. First, in §5.1, we collect classical results on the invariant theory of the action of PGL_2 on the space V_4 of binary quartic forms, and summarize the reduction theory of binary quartics developed in [7]. Next, in §5.2, we restrict to the space $V_4(\mathbb{Z})^{\mathrm{red}}$ of binary quartic forms with a linear factor. We develop the invariant theory for the action of PGL_2 on this space, and construct an embedding $U_0(\mathbb{Z})^{\mathrm{min}} \rightarrow V_4(\mathbb{Z})^{\mathrm{red}}$.

In Sections 5.3, 5.4, and 5.5, we estimate the number of $\mathrm{PGL}_2(\mathbb{Z})$ -orbits on elements in $V_4(\mathbb{Z})^{\mathrm{red}}$ with bounded height and large Q -invariant and whose Q - and D -invariants have a large common factor. We do this by fibering the space $V_4(\mathbb{Z})^{\mathrm{red}}$ by their roots in $\mathbb{P}^1(\mathbb{Z})$. Given an element $r \in \mathbb{P}^1(\mathbb{Z})$, the set of elements in $V_4(\mathbb{Z})$ that vanish on r is a lattice \mathcal{L}_r . We then count the number of elements in \mathcal{L}_r , using the Ekedahl sieve to exploit the condition that $\gcd(Q, D)$ is large.

5.1 The action of PGL_2 on the space V_4 of binary quartic forms

Let V_4 denote the space of binary quartic forms. The group PGL_2 acts on V_4 as follows: given $\gamma \in \mathrm{GL}_2$ and $g(x, y) \in V_4$, define

$$(\gamma \cdot g)(x, y) := \frac{1}{(\det \gamma)^2} g((x, y) \cdot \gamma).$$

It is easy to check that the center of GL_2 acts trivially. Hence this action of GL_2 on V_4 descends to an action of PGL_2 on V_4 .

The ring of invariants for the action of $\mathrm{PGL}_2(\mathbb{C})$ on $V_4(\mathbb{C})$ is freely generated by two elements, traditionally denoted by I and J . Explicitly, for $g(x, y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$, we have

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

We collect results from [7, §2.1] on the reduction theory of integral binary quartic forms. For $i = 0, 1, 2$, we let $V_4(\mathbb{R})^{(i)}$ to be the set of elements in $V_4(\mathbb{R})$ with nonzero discriminant, i -pairs of complex conjugate roots, and $4 - 2i$ real roots. Furthermore, we write $V_4(\mathbb{R})^{(2)} = V_4(\mathbb{R})^{(2+)} \cup V_4(\mathbb{R})^{(2-)}$ as the union of forms that are positive definite and negative definite. The four sets $L^{(i)}$ for $i \in \{0, 1, 2+, 2-\}$ constructed in [7, Table 1] satisfy the following two properties: first, $L^{(i)}$ are fundamental sets for the action of $\mathbb{R}_{>0} \cdot \mathrm{PGL}_2(\mathbb{R})$ on $V_4(\mathbb{R})^{(i)}$ where \mathbb{R} acts via scaling, and second, the sets $L^{(i)}$ are absolutely bounded. It follows that the sets $R^{(i)} := \mathbb{R}_{>0} \cdot L^{(i)}$ are fundamental sets for the action of $\mathrm{PGL}_2(\mathbb{R})$ on $V_4(\mathbb{R})^{(i)}$, and that the coefficients of an element $f(x, y) \in R^{(i)}$ with $H(f) = Y$ are bounded by $O(Y^{1/6})$.

For A' , $N'(t)$, and K defined in (18), set

$$\mathcal{F}_0 = \{n\alpha(t)k : n(u) \in N'(t), \alpha(t) \in A', k \in K\}.$$

Then \mathcal{F}_0 is a fundamental domain for the left multiplication action of $\mathrm{PGL}_2(\mathbb{Z})$ on $\mathrm{PGL}_2(\mathbb{R})$; and the multisets $\mathcal{F}_0 \cdot R^{(i)}$ are n_i -fold fundamental domains for the action of $\mathrm{PGL}_2(\mathbb{Z})$ on $V_4(\mathbb{R})^{(i)}$, where $n_0 = n_{2\pm} = 4$ and $n_1 = 2$. Let $S \subset V_4(\mathbb{Z})^{(i)} = V_4(\mathbb{Z}) \cap V_4(\mathbb{R})^{(i)}$ be any $\mathrm{PGL}_2(\mathbb{Z})$ -invariant set. Let $N_4(S; X)$ denote the number of $\mathrm{PGL}_2(\mathbb{Z})$ -orbits on S with height bounded by X such that each orbit $\mathrm{PGL}_2(\mathbb{Z}) \cdot f$ is counted with weight $1/\#\mathrm{Stab}_{\mathrm{PGL}_2(\mathbb{Z})}(f)$. Let $G_0 \subset \mathrm{PGL}_2(\mathbb{R})$ be a nonempty open bounded K -invariant set, and let $d\gamma = t^{-2}dnd^xtdk$, for $\gamma = ntk$ in Iwasawa coordinates, be a Haar-measure on $\mathrm{PGL}_2(\mathbb{R})$. Then, identically as in [7, Theorem 2.5], we have the following result.

Theorem 5.2 *We have*

$$N_4(S; X) = \frac{1}{n_i \mathrm{Vol}(G_0)} \int_{\gamma \in \mathcal{F}_0} \#\{S \cap \gamma G_0 \cdot R_X^{(i)}\} d\gamma,$$

where $R_X^{(i)}$ denotes the set of elements in $R^{(i)}$ with height bounded by X , the volume of G_0 is computed with respect to $d\gamma$, and for any set $T \subset V_4(\mathbb{R})$, the set of elements in T with height less than X is denoted by T_X .

Apart from its use in this section to obtain a bound on reducible binary quartic forms, Theorem 5.2 will also be used in Section 7 to prove Theorem 1.2.

5.2 Embedding $U_0(\mathbb{Z})^{\min}$ into the space of reducible binary quartics

Let $f(x) = x^3 + Ax + B$ be an element in $U_0(\mathbb{Z})^{\min}$ with $Q(f) = n$. From Theorem 1.6, it follows that there exists an integer r , defined uniquely modulo n , such that $f(x+r)$ is of the form

$$f(x+r) = x^3 + ax^2 + bnx + cn^2.$$

Assume that we have picked r so that $0 \leq r < n$. The ring of integers \mathcal{O}_f in $K_f = \mathbb{Q}[x]/f(x)$ corresponds, under the Delone–Faddeev bijection, to the binary cubic form

$$h(x, y) = nx^3 + ax^2y + bxy^2 + cy^3.$$

Elements in $U_0(\mathbb{Z})^{\min}$ with Q -invariant n thus correspond to integral binary cubic forms that represent n . However, this latter condition is difficult to detect, at least using geometry-of-numbers methods. Instead, we embed the space of binary cubic forms into the space $V_4(\mathbb{Z})^{\text{red}}$ of binary quartic forms with a linear factor over \mathbb{Q} by multiplying by y . In fact, we will replace $V_4(\mathbb{Z})^{\text{red}}$ with its (at most 4 to 1) cover $\tilde{V}_4(\mathbb{Z})$ consisting of pairs $(g(x, y), [\alpha, \beta])$, where g is a reducible binary quartic form and $[\alpha, \beta]$ is a root of f . Explicitly,

$$\tilde{V}_4(\mathbb{Z}) := \{(g(x, y), [\alpha, \beta]) : 0 \neq g(x, y) \in V_4(\mathbb{Z})^{\text{red}}, \alpha, \beta \in \mathbb{Z}, \gcd(\alpha, \beta) = 1, g(\alpha, \beta) = 0\}$$

This gives us the following map $\tilde{\sigma} : U_0(\mathbb{Z})^{\min} \rightarrow \tilde{V}_4(\mathbb{Z})$:

$$\begin{aligned} \tilde{\sigma} : U_0(\mathbb{Z})^{\min} &\rightarrow V_3(\mathbb{Z}) &\rightarrow \tilde{V}_4(\mathbb{Z}) \\ f(x) &\mapsto h(x, y) &\mapsto (yh(x, y), [1, 0]). \end{aligned} \tag{20}$$

The group $\text{PGL}_2(\mathbb{Z})$ acts on $\tilde{V}_4(\mathbb{Z})$ via

$$\gamma \cdot (g(x, y), [\alpha : \beta]) = ((\gamma \cdot g)(x, y), [\alpha : \beta]\gamma^{-1});$$

this is an action since $(\gamma \cdot g)((\alpha, \beta)\gamma^{-1}) = g(\alpha, \beta) = 0$. Aside from the classical invariants I and J , this action has an extra invariant, which we denote by Q , defined as follows. Given $(g, [\alpha : \beta]) \in \tilde{V}_4(\mathbb{Z})$, let $h(x, y) = g(x, y)/(\beta x - \alpha y)$ be the associated binary cubic form and we define

$$Q(g, [\alpha : \beta]) = h(\alpha, \beta), \quad D(g, [\alpha : \beta]) = \Delta(h). \tag{21}$$

The Q -, D -invariants and the discriminant are related by

$$\Delta(g) = Q(g, [\alpha : \beta])^2 D(g, [\alpha : \beta]).$$

We now have the following result.

Proposition 5.3 *There is an injective map*

$$\sigma : U_0(\mathbb{Z})^{\min} \rightarrow \tilde{V}_4(\mathbb{Z}) \rightarrow \text{PGL}_2(\mathbb{Z}) \backslash \tilde{V}_4(\mathbb{Z}),$$

such that for every $f \in U_0(\mathbb{Z})^{\min}$, we have

$$I(f) = I(\sigma(f)); \quad J(f) = J(\sigma(f)); \quad Q(f) = Q(\sigma(f)); \quad D(f) = D(\sigma(f)). \tag{22}$$

Proof: The first three equalities of (22) can be checked by a direct computation. The injectivity of σ then follows from the fact that $I(f)$ and $J(f)$ determine f . Finally, the last equality of (22) can be directly obtained:

$$D(f) = \Delta(f)/Q(f)^2 = \Delta(\sigma(f))/Q(\sigma(f))^2 = D(\sigma(f)),$$

where the second equality follows since $(I(f), J(f)) = (I(\sigma(f)), J(\sigma(f)))$ and so $\Delta(f) = \Delta(\sigma(f))$. \square

Therefore, to prove Theorem 5.1, it suffices to count $\text{PGL}_2(\mathbb{Z})$ -orbits $(g, [\alpha : \beta])$ in $\tilde{V}_4(\mathbb{Z})$, such that both $Q(g, [\alpha : \beta])$ and the radical $\text{rad}(\gcd(Q(g, [\alpha : \beta]), D(g, [\alpha : \beta])))$ are large.

5.3 Counting $\mathrm{PGL}_2(\mathbb{Z})$ -orbits on reducible binary quartic forms

We use the setup of [7, §2], which is recalled in §5.1. Since the sets $L^{(i)}$ are absolutely bounded, the coefficients of any element in $R^{(i)} = \mathbb{R}_{>0} \cdot L^{(i)}$ having height Y are bounded by $O(Y^{1/6})$. Hence the same is true of every element in $G_0 \cdot R_Y^{(i)}$, as G_0 is a bounded set. The set $V_4(\mathbb{Z})^{\mathrm{red}}$ is not a lattice. To apply geometry-of-numbers methods, we fiber it over the set of possible linear factors. We write

$$V_4(\mathbb{Z})^{\mathrm{red}} = \bigcup_{r=[\alpha:\beta]} \mathcal{L}_r, \quad (23)$$

where α and β are coprime integers and for $r = [\alpha : \beta] \in \mathbb{P}^1(\mathbb{Z})$, we define \mathcal{L}_r to be the set of all integral binary quartic forms f such that $f(r) = 0$. From Theorem 5.2, in conjunction with the injection σ of §5.2, we have

$$N_{Q,q}(Y) \ll \sum_{r \in \mathbb{P}^1(\mathbb{Z})} \int_{(ntk) \in \mathcal{F}_0} \#\{g \in \mathcal{L}_r \cap (ntk)G_0R_Y^{(i)} : Q(g) > Q, \mathrm{rad}(\mathrm{gcd}(Q(g), D(g))) > q\} t^{-2} dnd^\times tdk \quad (24)$$

As γ varies over \mathcal{F}_0 , the set $\gamma G_0 R_Y^{(i)}$ becomes skewed. More precisely, if $\gamma = ntk$ in Iwasawa coordinates, then the five coefficients a, b, c, d , and e , of any element of $\gamma G_0 R^{(i)}(Y)$ satisfy

$$a \ll \frac{Y^{1/6}}{t^4}; \quad b \ll \frac{Y^{1/6}}{t^2}; \quad c \ll Y^{1/6}; \quad d \ll t^2 Y^{1/6}; \quad e \ll t^4 Y^{1/6}. \quad (25)$$

Hence when $t \gg Y^{1/24}$, the x^4 -coefficient of any integral binary quartic form in $\gamma G_0 R^{(i)}(Y)$ is 0, forcing a root at the point $[1, 0] \in \mathbb{P}^1(\mathbb{Z})$. Moreover we expect it to be rare that such a binary quartic form has another integral root. In what follow, we first consider the lattice $\mathcal{L}_{[1,0]}$ in §5.4, and consider the rest of the lattices in §5.5.

5.4 The contribution from the root $r = [1 : 0]$

Let $g(x, y) = bx^3y + cx^2y^2 + dxy^3 + ey^4 \in \mathcal{L}_{[1,0]}$ be an integral binary quartic form. We write $Q(g)$ for $Q(g, [1 : 0])$ and $D(g)$ for $D(g, [1 : 0])$. Then we have $Q(g) = b$ and $D(g) = \Delta(bx^3 + cx^2y + dxy^3 + ey^3)$, the discriminant of the binary cubic form $g(x, y)/y$. Hence, if a fixed $t \geq 1$ contributes to the estimate $N_{Q,q}(Y)$ in (24), then we must have

$$t \ll \frac{Y^{1/12}}{Q^{1/2}}. \quad (26)$$

We now fiber over the $O(Y^{1/6}/t^2)$ choices for b . For each such choice, we have $O(Y^\epsilon)$ possible squarefree divisors m of b . Fix such a divisor $m > q$ such that $\mathrm{rad}(\mathrm{gcd}(Q(g), D(g))) = m$. Then $m \mid D(g)$ which implies that

$$3c^2d^2 - 4c^3e \equiv 0 \pmod{m}.$$

Thus, the residue class of e modulo m is determined by c and d , unless $m \mid c$.

From (25), we see that the number of elements in $\mathcal{L}_{[1,0]} \cap (ntk)G_0R_Y^{(i)}$ with b and m fixed as above is bounded by

$$O\left(\frac{t^6 Y^{1/2}}{m} + t^6 Y^{1/3}\right) = O\left(\frac{t^6 Y^{1/2}}{q} + t^6 Y^{1/3}\right),$$

where the second term deals with the case $q \gg Y^{1/6}$. It therefore follows that the contribution to $N_{Q,q}(Y)$ in (24) from the root $r = [1 : 0]$ is bounded by

$$\int_{t=1}^{Y^{1/12}/Q^{1/2}} \frac{Y^{1/6+\epsilon}}{t^2} \left(\frac{t^6 Y^{1/2}}{q} + t^6 Y^{1/3}\right) t^{-2} d^\times t \ll_\epsilon \frac{Y^{5/6+\epsilon}}{qQ} + \frac{Y^{2/3+\epsilon}}{Q}, \quad (27)$$

which is sufficiently small. The contribution from the root $r = [0 : 1]$ can be identically bounded.

5.5 The contribution from a general root $r = [\alpha : \beta]$ with $\alpha\beta \neq 0$

Write $r = [\alpha : \beta]$ where α, β are coprime integers and $\alpha\beta \neq 0$. Throughout this section, we denote the torus element in \mathcal{F}_0 with entries t^{-1} and t by a_t . We have the bijection

$$\begin{aligned} \theta_t : \{\mathcal{L}_r \cap a_t G_0 \cdot R_Y^{(i)}\} &\longleftrightarrow \{a_t^{-1} \mathcal{L}_r \cap G_0 \cdot R_Y^{(i)}\} \\ ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 &\longmapsto t^4ax^4 + t^2bx^3y + cx^2y^2 + t^{-2}dxy^3 + t^{-4}ey^4, \end{aligned} \quad (28)$$

which preserves the invariants I and J . Define $\tilde{V}_4(\mathbb{R})$ to be the set of pairs $(g(x, y), r)$, where $g(x, y) \in V_4(\mathbb{R})$ and $r \in \mathbb{R}^2$ such that $g(r) = 0$. We extend the definitions of the Q - and D -invariants to the space $\tilde{V}_4(\mathbb{R})$ via (21). Set $r_t := r \cdot a_t = [t^{-1}\alpha, t\beta]$. Then we have

$$Q(g, r) = Q(\theta_t \cdot g, r_t), \quad D(g, r) = D(\theta_t \cdot g, r_t).$$

Identifying the space of binary quartics with \mathbb{R}^5 via the coefficients (a, b, c, d, e) , we write

$$a_t^{-1} \mathcal{L}_r = \text{diag}(t^4, t^2, 1, t^{-2}, t^{-4}) \cdot ((\alpha^4, \alpha^3\beta, \alpha^2\beta^2, \alpha\beta^3, \beta^4)^\perp),$$

where $(\alpha^4, \alpha^3\beta, \alpha^2\beta^2, \alpha\beta^3, \beta^4)^\perp$ is the sublattice of \mathbb{Z}^5 perpendicular to $(\alpha^4, \alpha^3\beta, \alpha^2\beta^2, \alpha\beta^3, \beta^4)$ with respect to the usual inner product on \mathbb{R}^5 . Since α and β are coprime, the following vectors form an integral basis for $a_t^{-1} \mathcal{L}_r$:

$$w_1 = (t^4\beta, -t^2\alpha, 0, 0, 0), \quad w_2 = (0, t^2\beta, -\alpha, 0, 0), \quad w_3 = (0, 0, \beta, -t^{-2}\alpha, 0), \quad w_4 = (0, 0, 0, t^{-2}\beta, -t^{-4}\alpha).$$

Define the vector v_t to be $v_t := (t\beta, -t^{-1}\alpha) \in \mathbb{R}^2$. Then it is easy to see that the lengths of w_i are given by:

$$|w_1| = t^3|v_t|, \quad |w_2| = t|v_t|, \quad |w_3| = t^{-1}|v_t|, \quad |w_4| = t^{-3}|v_t|, \quad (29)$$

The next lemma proves that this basis is *almost-Minkowski*. That is, the quotients $\langle w_i, w_j \rangle / (|w_i||w_j|)$, for $i \neq j$, are bounded from above by a constant $c < 1$ independent of t and r .

Lemma 5.4 *For $i \neq j$, we have*

$$\langle w_i, w_j \rangle \leq \frac{1}{2}|w_i||w_j|.$$

Proof: The inner product $\langle w_i, w_j \rangle$ for $i < j$ is 0 unless $j = i + 1$. In those three cases, we have

$$\frac{\langle w_i, w_j \rangle}{|w_i||w_j|} = \frac{|\alpha\beta|}{t^{-2}\alpha^2 + t^2\beta^2} \leq \frac{1}{2},$$

by the AM-GM inequality. \square

We will represent elements in $a_t^{-1} \mathcal{L}_r$ by four-tuples $(a_1, a_2, a_3, a_4) \in \mathbb{Z}^4$, where such a tuple corresponds to the element $a_1w_1 + a_2w_2 + a_3w_3 + a_4w_4$. Then we have the following lemma.

Lemma 5.5 *Let $g(x, y)$ be an element in \mathcal{L}_r , and let $a_t^{-1}g(x, y)$ correspond to the four-tuple (a_1, a_2, a_3, a_4) . Then we have*

$$\begin{aligned} g(x, y) &= (\beta x - \alpha y)(a_1x^3 + a_2x^2y + a_3xy^2 + a_4y^3), \\ Q(g, r) &= a_1\alpha^3 + a_2\alpha^2\beta + a_3\alpha\beta^2 + a_4\beta^3, \\ D(g, r) &= \Delta_3(a_1, a_2, a_3, a_4), \end{aligned}$$

where $\Delta_3(a_1, a_2, a_3, a_4)$ denotes the discriminant of the binary cubic form with coefficients a_i .

The above lemma follows from a direct computation. Next, we determine when an element (a_1, a_2, a_3, a_4) has small length.

Lemma 5.6 Suppose $g \in a_t^{-1}\mathcal{L}_r$, corresponding to (a_1, a_2, a_3, a_4) , belongs to $G_0 \cdot R_Y^{(i)}$ for some i . Then

$$a_1 \ll \frac{Y^{1/6}}{t^3|v_t|}; \quad a_2 \ll \frac{Y^{1/6}}{t|v_t|}; \quad a_3 \ll \frac{Y^{1/6}}{t^{-1}|v_t|}; \quad a_4 \ll \frac{Y^{1/6}}{t^{-3}|v_t|}. \quad (30)$$

Proof: Let $|\cdot|$ denote the length of a binary quartic form, where $V_4(\mathbb{R})$ has been identified with \mathbb{R}^5 in the natural way. Then for g to belong in $G_0 \cdot R_Y^{(i)}$, it must satisfy $|g| \ll Y^{1/6}$. For any real numbers a_1, a_2, a_3, a_4 , we compute

$$\begin{aligned} |a_1w_1 + a_2w_2 + a_3w_3 + a_4w_4|^2 &\geq a_1^2|w_1|^2 + a_2^2|w_2|^2 + a_3^2|w_3|^2 + a_4^2|w_4|^2 \\ &\quad - |a_1||a_2||w_1||w_2| - |a_2||a_3||w_2||w_3| - |a_3||a_4||w_3||w_4| \\ &\geq \frac{3-\sqrt{5}}{4}(a_1^2|w_1|^2 + a_2^2|w_2|^2 + a_3^2|w_3|^2 + a_4^2|w_4|^2). \end{aligned}$$

(Of course, the exact constant is not important.) Therefore in order for $|a_1w_1 + a_2w_2 + a_3w_3 + a_4w_4| \ll Y^{1/6}$, Equation (30) must be satisfied. \square

We now have the following proposition bounding the number of elements in $\mathcal{L}_r \cap a_t G_0 \cdot R_Y^{(i)}$ whose Q - and D -invariants share a large common factor.

Proposition 5.7 For $t \gg 1$, we have

$$\#\{g(x, y) \in \mathcal{L}_r \cap a_t G_0 \cdot R_Y^{(i)} : \text{rad}(\text{gcd}(Q(g, r), D(g, r))) > q\} = \begin{cases} 0 & \text{if } |v_t| \gg Y^{1/6} \\ O\left(\frac{Y^{2/3+\epsilon}}{q|v_t|^4} + \frac{Y^{1/2+\epsilon}}{t|v_t|^3}\right) & \text{otherwise} \end{cases} \quad (31)$$

where the implied constant is independent of r, t , and Y .

Proof: Using the bijection (28) in conjunction with Lemmas 5.5 and 5.6, we see that it is enough to prove that the number of four-tuples of integers (a_1, a_2, a_3, a_4) , satisfying (30) and

$$\text{rad}(\text{gcd}(a_1\alpha^3 + a_2\alpha^2\beta + a_3\alpha\beta^2 + a_4\beta^3, \Delta_3(a_1, a_2, a_3, a_4))) > q,$$

is bounded by the right hand side of (31). Suppose first $|v_t| \gg Y^{1/6}$. Then any binary quartic form $g(x, y)$ represented by the four-tuple (a_1, a_2, a_3, a_4) satisfying (30) must have $a_1 = a_2 = 0$. From Lemma 5.5, it follows that $D(g, r) = 0$ and hence $\Delta(g) = 0$. Since $G_0 \cdot R_Y^{(i)}$ contains no point with $\Delta = 0$, it follows that the intersection is empty, proving the first part of the proposition.

The second part of the proposition is proved by using the Ekedhal sieve as developed in [4]. We carry the sieve out in detail so as to demonstrate that the implied constant in (31) is indeed independent of r and t . Define

$$T_{\alpha, \beta}(a_1, a_2, a_3) := \Delta_3(a_1\beta^3, a_2\beta^3, a_3\beta^3, -(a_1\alpha^3 + a_2\alpha^2\beta + a_3\alpha\beta^2)).$$

It is clear that if $m \mid Q(g, r)$ and $m \mid D(g, r)$ for any integer m , then $m \mid T_{\alpha, \beta}(a_1, a_2, a_3)$.

First, we bound the number of triples (a_1, a_2, a_3) satisfying (30) such that $T_{\alpha, \beta}(a_1, a_2, a_3) = 0$. For a fixed pair $(a_1, a_2) \neq (0, 0)$, by explicitly writing out $T_{\alpha, \beta}(a_1, a_2, a_3)$, we see that there are at most three possible values of a_3 with $T_{\alpha, \beta}(a_1, a_2, a_3) = 0$. This gives a bound of $O(Y^{1/3}/(t^4|v_t|^2))$ on the number of triples (a_1, a_2, a_3) with $T_{\alpha, \beta}(a_1, a_2, a_3) = 0$. Multiplying with the number of all possibilities for a_4 , we obtain the bound

$$O\left(\frac{Y^{1/2}}{t|v_t|^3}\right) \quad (32)$$

on the number of four-tuples of integers (a_1, a_2, a_3, a_4) , satisfying (30) and $T_{\alpha, \beta}(a_1, a_2, a_3) = 0$.

Next, we fiber over triples (a_1, a_2, a_3) with $T_{\alpha, \beta}(a_1, a_2, a_3) \neq 0$ and satisfying (30). In this case, we have $(a_1, a_2) \neq (0, 0)$. Hence by (30), we may assume $\alpha, \beta, t \ll Y^{1/6}$. Hence the value of $T_{\alpha, \beta}(a_1, a_2, a_3)$ is bounded by a polynomial in Y of fixed degree. It follows that the number of squarefree divisors of $T_{\alpha, \beta}(a_1, a_2, a_3)$ is bounded by $O_\epsilon(Y^\epsilon)$. Fix one such divisor $m > q$. We now fiber over a positive squarefree integer $\delta \ll Y^{1/6}/(t^3|v_t|)$ such that $\text{rad}(\gcd(a_1, a_2)) = \delta$. The number of such possible (a_1, a_2) is

$$\ll \frac{1}{\delta^2} \frac{Y^{1/6}}{t^3|v_t|} \frac{Y^{1/6}}{t|v_t|}.$$

Fix any such pair. Let a_3 be any integer satisfying (30) such that $T_{\alpha, \beta}(a_1, a_2, a_3) \neq 0$. Let $m_1 = \gcd(m, \delta)$ and let $m_2 = m/m_1 > q/\delta$. Then the polynomial $\Delta_3(a_1, a_2, a_3, a_4)$ is identically 0 modulo m_1 and quadratic in a_4 modulo any prime factor of m_2 . Hence the number of these quadruples with the extra condition that $m \mid \Delta_3(a_1, a_2, a_3, a_4)$ is

$$\ll \frac{1}{\delta^2} \frac{Y^{1/6}}{t^3|v_t|} \frac{Y^{1/6}}{t|v_t|} \frac{Y^{1/6}}{t^{-1}|v_t|} \left(\frac{1}{q/\delta} \frac{Y^{1/6}}{t^{-3}|v_t|} + 1 \right) \ll_\epsilon \frac{Y^{2/3}}{\delta q|v_t|^4} + \frac{Y^{1/2}}{\delta^2 t^3 |v_t|^3}.$$

Summing over δ and all possible divisors m gives the bound

$$O\left(\frac{Y^{2/3+\epsilon}}{q|v_t|^4} + \frac{Y^{1/2+\epsilon}}{t^3|v_t|^3}\right). \quad (33)$$

The proposition now follows from (32) and (33). \square

We now impose the condition on the Q -invariant. From Lemma 5.5 and (30), we obtain

$$Q < |Q(g, r)| = |a_1\alpha^3 + a_2\alpha^2\beta + a_3\alpha\beta^2 + a_4\beta^3| \ll Y^{1/6}|v_t|^2.$$

In conjunction with (24) and the estimates of Proposition 5.7, this yields

$$\begin{aligned} N_{Q, q}(Y) &\ll_\epsilon \sum_{k \ll \log Y} \int_{t \gg 1} \sum_{\substack{r=[\alpha:\beta] \\ 2^k < |v_t| \leq 2^{k+1}}} \left(\frac{Y^{2/3+\epsilon}}{q|v_t|^4} + \frac{Y^{1/2+\epsilon}}{t|v_t|^3} \right) t^{-2} d^\times t \\ &\ll_\epsilon \sum_{k \ll \log Y} \int_{t \gg 1} \left(\frac{Y^{5/6+\epsilon}}{qQ} + \frac{Y^{7/12+\epsilon}}{tQ^{1/2}} \right) t^{-2} d^\times t \\ &\ll_\epsilon \frac{Y^{5/6+\epsilon}}{qQ} + \frac{Y^{7/12+\epsilon}}{Q^{1/2}}. \end{aligned}$$

This concludes the proof of Theorem 5.1.

6 Uniformity estimates

In this section, we prove Theorems 1.4 and 1.5, the main uniformity estimates. First, in §6.1, we use the results of §3 to prove Theorem 1.4. Next, in §6.2, we combine the results of §4 and §5 in order to obtain Theorem 1.5.

6.1 The family of elliptic curves with squarefree index

Recall the family \mathcal{E} defined in the introduction. The assumption that elliptic curves $E \in \mathcal{E}$ satisfy $j(E) \leq \log(\Delta(E))$ implies the height bound $H(E) \ll \Delta(E)^{1+\epsilon}$. Given $E \in \mathcal{E}$, let $E : y^2 = f(x) = x^3 + Ax + B$ be the minimal Weierstrass model for E . Given an étalé algebra K over \mathbb{Q} with ring of integers \mathcal{O}_K , let $\mathcal{O}_K^{\text{Tr}=0}$ denote the set of traceless integral elements in K . Consider the map

$$\mathcal{E} \rightarrow \{(K, \alpha) : K \text{ cubic algebra over } \mathbb{Q}, \alpha \in \mathcal{O}_K^{\text{Tr}=0}\}$$

sending $E : y^2 = f(x)$ to the pair $(\mathbb{Q}[x]/f(x), x)$. This map is injective since if E corresponds to the pair (K, α) , then $y^2 = N_{K/\mathbb{Q}}(x - \alpha)$ recovers E . In order to parametrize elements in \mathcal{E}_{sf} , we will instead use the following modified map:

$$\begin{aligned} \sigma : \mathcal{E} &\rightarrow \{(K, \alpha) : K \text{ cubic étale algebra over } \mathbb{Q}, \alpha \in \mathcal{O}_K^{\text{Tr}=0}\} \\ E : y^2 = f(x) &\mapsto (\mathbb{Q}[x]/f(x), \text{Prim}(x)), \end{aligned} \quad (34)$$

where for $0 \neq x \in \mathcal{O}_K$, the element $\text{Prim}(x)$ is the unique primitive integer in \mathcal{O}_K which is a positive rational multiple of x . Note that the map σ restricted to \mathcal{E}_{sf} is injective due to the squarefree condition on $\Delta(E)/C(E)$ at primes at least 5 and that E has good reduction at 2 and 3. We start with the following lemma.

Lemma 6.1 *Let E be an elliptic curve and let $\sigma(E) = (K, \alpha)$. Then $|\text{Sel}_2(E)| \ll_{\epsilon} |\text{Cl}(K)[2]| \cdot |\Delta(E)|^{\epsilon}$. Furthermore, if $E \in \mathcal{E}_{\text{sf}}$, then $|\alpha| \ll H(E)^{1/6}$.*

Proof: The first claim is a direct consequence of [15, Proposition 7.1]. The second claim is immediate since the minimal Weierstrass model of E is given by $y^2 = (x - \beta_1)(x - \beta_2)(x - \beta_3)$, where the β_i are the conjugates of an absolutely bounded rational multiple of α . \square

We now prove the following result.

Proposition 6.2 *For positive real numbers X and $Q \leq X$, we have*

$$\left| \{(E, \eta) : E \in \mathcal{E}_{\text{sf}}, \eta \in \text{Sel}_2(E), X < C(E) \leq 2X, QX < \Delta(E) \leq 2QX\} \right| \ll_{\epsilon} X^{5/6+\epsilon}/Q^{1/6}. \quad (35)$$

where the implied constant is independent of X and Q .

Proof: Let $E \in \mathcal{E}_{\text{sf}}$ be an elliptic curve satisfying the conductor and discriminant bounds of (35), and let $\sigma(E) = (K, \alpha)$. It is easy to verify from Table 1 that $\Delta(K) = C(E)^2/\Delta(E)$. Therefore, it follows that $X/(2Q) < \Delta(K) \leq 4X/Q$, and that $|\alpha| \ll H(E)^{1/6} \ll_{\epsilon} (QX)^{1/6+\epsilon}$.

Since the map σ is injective, it follows that the left hand side of (35) is

$$\ll_{\epsilon} X^{\epsilon} \sum_{\substack{[K:\mathbb{Q}]=3 \\ \frac{X}{2Q} < \Delta(K) \leq \frac{4X}{Q}}} N'_K((QX)^{1/6+\epsilon} |\text{Cl}(K)[2]|), \quad (36)$$

where $N'_K(Y)$ denotes the number of primitive elements α in $\mathcal{O}_K^{\text{Tr}=0}$ such that $|\alpha| < Y$ and the pair (K, α) is in the image of σ . We now split the above sum over cubic algebras K into three parts, corresponding to the sizes $\ell_1(K)$ and $\ell_2(K)$ of the successive minima of $\mathcal{O}_K^{\text{Tr}=0}$.

First, if $(QX)^{1/6+\epsilon} \ll \ell_1(K)$, then the contribution to (36) is 0. Second, assume that $\ell_2(K) \ll (QX)^{1/6+\epsilon}$. Then Lemma 4.7 yields the bound

$$N'_K((QX)^{1/6+\epsilon}) \ll_{\epsilon} (QX)^{1/3+\epsilon}/\sqrt{X/Q} \ll \frac{Q^{5/6}}{X^{1/6-\epsilon}}.$$

Using Bhargava's result [3, Theorem 5] to bound the sum of $|\text{Cl}(K)[2]|$ over cubic fields K with the prescribed discriminant range, and using the well known genus-theory bounds $\text{Cl}(K)[2] \ll |\Delta(K)|^{\epsilon}$, for each reducible cubic K , we obtain:

$$\sum_{\substack{[K:\mathbb{Q}]=3 \\ \frac{X}{2Q} < \Delta(K) \leq \frac{4X}{Q} \\ \ell_2(K) \ll (QX)^{1/6+\epsilon}}} N'_K((QX)^{1/6+\epsilon} |\text{Cl}(K)[2]|) \ll_{\epsilon} X^{\epsilon} \cdot \frac{Q^{5/6}}{X^{1/6-\epsilon}} \cdot \frac{X}{Q} = \frac{X^{5/6+2\epsilon}}{Q^{1/6}}.$$

Finally, we bound the contribution of cubic étale algebras K such that $\ell_1(K) \ll (QX)^{1/6+\epsilon} \ll \ell_2(K)$. In this case, we have $N'_K((QX)^{1/6+\epsilon}) \leq 1$ and

$$\text{sk}(K) = \ell_2(K)/\ell_1(K) \gg \sqrt{\Delta(K)}/\ell_1(K)^2 \gg X^{1/6}/Q^{5/6}.$$

Suppose first $K = \mathbb{Q} \oplus L$ is reducible. Then $\mathcal{O}_K^{\text{Tr}=0}$ has an integral basis given by $\{(-2, 1), (0, \sqrt{d})\}$ where $\Delta(K) = d$ or $4d$. When d is small, say bounded by 100, we get an $O(1)$ contribution to (36). When d is large, the above basis is a Minkowski basis and $(-2, 1)$ is the smallest, and hence unique, primitive traceless element. However, this point does not correspond to an elliptic curve since the corresponding cubic polynomial is $(x-2)(x+1)^2$ which has a double root. Hence, we get no contribution in this case. It remains to consider the case where K is a cubic field. Applying Theorem 4.1, we obtain a bound of

$$O_\epsilon(X^\epsilon(X/Q)/(X^{1/6}/Q^{5/6})) = O_\epsilon(X^{5/6+\epsilon}/Q^{1/6}),$$

on the contribution to (36) over cubic fields K with $\ell_1(K) \ll (QX)^{1/6+\epsilon} \ll \ell_2(K)$, as desired. \square

Proof of Theorem 1.4: Note if the conductor $C(E)$ is bounded by X and the index $\Delta(E)/C(E)$ is squarefree, then the index is also bounded by X . Divide the conductor range $[1, X]$ into $\log X$ dyadic ranges, and for each such range divide the index range $[M, X]$ into $\log X$ dyadic ranges, and then apply Proposition 6.2 on each pair of dyadic ranges. Theorem 1.4 follows. \square

6.2 The family of elliptic curves with bounded index

As in §3, let Σ be a finite set of pairs (p, T_p) , where p is a prime number and $T_p = \text{III}, \text{IV},$ or $\text{I}_{\geq 2}$ is a Kodaira symbol. Recall the invariants $Q(\Sigma)$, $m_{\text{odd}}(\Sigma)$ and $m_T(\Sigma)$ for Kodaira symbols T . We further define $m_{\text{even}}(\Sigma)$ to be the product of p over pairs (p, I_{2k}) in Σ . We define $\mathcal{E}(\Sigma)$ to be the set of elliptic curves $E \in \mathcal{E}$ such that the Kodaira symbol at p of E is T_p for every pair $(p, T_p) \in \Sigma$. Given a set of five positive real numbers

$$S = \{m_{\text{III}}, m_{\text{IV}}, m_{\text{even}}, m_{\text{odd}}, Q\},$$

we let $\mathcal{E}(S)$ denote the set of elliptic curves E such that the product P of primes at which E has Kodaira symbol III (resp. IV, $\text{I}_{2(k \geq 1)}$, $\text{I}_{2(k \geq 1)+1}$) satisfies $m_{\text{III}} \leq P < 2m_{\text{III}}$ (resp. $m_{\text{IV}} \leq P < 2m_{\text{IV}}$, $m_{\text{even}} \leq P < 2m_{\text{even}}$, $m_{\text{odd}} \leq P < 2m_{\text{odd}}$), and $Q \leq Q(E) < 2Q$. The following result is a consequence of Theorems 3.1 and 5.1.

Proposition 6.3 *Let $S = \{m_{\text{III}}, m_{\text{IV}}, m_{\text{even}}, m_{\text{odd}}, Q\}$ be as above and let Y be a positive real number. Then*

$$\begin{aligned} & \#\{E \in \mathcal{E}(S) : |\Delta(E)| < Y\} \\ & \ll_\epsilon Y^\epsilon \min\left(\frac{Y^{5/6}m_{\text{even}}}{Q^2m_{\text{IV}}} + \frac{Qm_{\text{III}}m_{\text{even}}m_{\text{odd}}^2}{Y^{1/6}}, \frac{Y^{5/6}}{Qm_{\text{III}}m_{\text{IV}}m_{\text{odd}}} + \frac{Y^{7/12}}{Q^{1/2}}\right). \end{aligned} \quad (37)$$

Proof: First note that if $E \in \mathcal{E}$, then $H(E) \ll \Delta(E)^{1+\epsilon}$ from the j -invariant bound. It is enough to prove that the left hand side of (37) is bounded (up to a factor of Y^ϵ) by both terms in the minimum. For the second term, this is a direct consequence of Theorem 5.1 and Table 1.

For the first term, note that the set of monic cubic polynomials corresponding to curve in $\mathcal{E}(S)$ is clearly the union of $O_\epsilon(Y^\epsilon m_{\text{III}}m_{\text{IV}}m_{\text{even}}m_{\text{odd}})$ sets $U_0(\mathbb{Z})_\Sigma$, where each such Σ satisfies $m_{\text{III}}(\Sigma) \sim m_{\text{III}}$, $m_{\text{IV}}(\Sigma) \sim m_{\text{IV}}$, $m_{\text{even}}(\Sigma) \sim m_{\text{even}}$, $m_{\text{odd}}(\Sigma) \sim m_{\text{odd}}$, and $Q(\Sigma) \sim Q$. In §3, we obtained bounds on the number of elements in $U(\mathbb{Z})_\Sigma$ with height bounded by Y . Since the set $U(\mathbb{Z})_\Sigma$ is invariant under the linear \mathbb{Z} -action, we have

$$|\{f \in U_0(\mathbb{Z})_\Sigma : H(f) < Y\}| \ll Y^{-1/6} |\{f \in U(\mathbb{Z})_\Sigma : H(f) < Y\}|.$$

Combining this with Theorem 3.1, and multiplying with the number of different Σ 's required to cover the set $\mathcal{E}(S)$, we obtain the result. \square

Proof of Theorem 1.5: Given positive real numbers X and Y , let $\mathcal{E}(S; X, Y)$ denote the set of $E \in \mathcal{E}(S)$ that satisfy $X \leq C(E) < 2X$, and $Y \leq \Delta(E) < 2Y$. Fix constants $0 < \kappa < 7/4$ and $0 < \delta$. We first

obtain bounds on the sizes of the sets $\mathcal{E}(S; X, Y)$. Let E be an elliptic curve in $\mathcal{E}(S; X, Y)$, and let P be the contribution to the conductor of E that is prime to $m_{\text{III}}m_{\text{IV}}m_{\text{even}}m_{\text{odd}}$. Then we have by Table 1

$$\begin{aligned} X &\asymp C(E) \asymp m_{\text{III}}^2 m_{\text{IV}}^2 m_{\text{even}} m_{\text{odd}} P; \\ Y &\asymp \Delta(E) \asymp m_{\text{III}} m_{\text{IV}}^2 m_{\text{odd}} Q^2 P. \end{aligned}$$

Therefore, in order for $\mathcal{E}(S; X, Y)$ to be nonempty, we must have

$$\frac{Y}{Q^2} \asymp \frac{X}{m_{\text{III}} m_{\text{even}}}. \quad (38)$$

First note that we have

$$\frac{Y^{5/6} m_{\text{even}}}{Q^2 m_{\text{IV}}} \ll \frac{X}{Y^{1/6}}. \quad (39)$$

Moreover,

$$\begin{aligned} \min\left(\frac{Q m_{\text{III}} m_{\text{even}} m_{\text{odd}}^2}{Y^{1/6}}, \frac{Y^{5/6}}{Q m_{\text{III}} m_{\text{IV}} m_{\text{odd}}}\right) &\leq \left(\frac{Y^{15/6-1/6} m_{\text{even}}}{Q^2 m_{\text{III}}^2 m_{\text{IV}}^3 m_{\text{odd}}}\right)^{1/4} \ll X^{1/4} Y^{1/3}, \\ \min\left(\frac{Q m_{\text{III}} m_{\text{even}} m_{\text{odd}}^2}{Y^{1/6}}, \frac{Y^{7/12}}{Q^{1/2}}\right) &\leq (Y m_{\text{III}} m_{\text{even}} m_{\text{odd}}^2)^{1/3} \ll \frac{Y^{2/3}}{X^{1/3}}. \end{aligned} \quad (40)$$

Assume that Y satisfies the bound $X^{1+\delta} \ll Y \ll X^\kappa$ for $\delta > 0$ and $\kappa < 7/4$. Proposition 6.3, (39), and (40) imply that we have

$$|\mathcal{E}(S; X, Y)| \ll_\epsilon X^{5/6-\theta+\epsilon}, \quad (41)$$

for some positive constant θ depending only on δ and κ . It is clear that the set

$$\{E \in \mathcal{E}_\kappa : C(E) < X, |\Delta(E)| > C(E)X^\delta\}$$

is the union of $O_\epsilon(X^\epsilon)$ sets $\mathcal{E}(S; X_1, Y_1)$, with $X_1 \leq X$ and $X_1^{1+\delta} \ll Y_1 \ll X_1^\kappa$. Theorem 1.5 now follows from (41). \square

6.3 Additional uniformity estimates

We will also need (albeit much weaker) estimates on the number of elliptic curves with bounded height and additive reduction, as well as on the number of $\text{PGL}_2(\mathbb{Z})$ -orbits on integral binary quartic forms whose discriminants are divisible by a large square.

We begin with the following result which follows immediately from the proof of [7, Proposition 3.16].

Proposition 6.4 *The number of pairs $(A, B) \in \mathbb{Z}^2$ such that $H(A, B) < X$ and such that $p^2 \mid \Delta(A, B)$ is $O(X^{5/6}/p^{3/2})$, where the implied constant is independent of X and p .*

Next, we have the following estimate which is proved in [10]

Proposition 6.5 *The number of $\text{PGL}_2(\mathbb{Z})$ -orbits f on $V_4(\mathbb{Z})$ such that $H(f) < X$ and $n^2 \mid \Delta(f)$ for some $n > M$ is bounded by*

$$O\left(\frac{X^{5/6}}{M^{1-\epsilon}} + X^{19/24+\epsilon}\right),$$

where the error terms are independent of X and M .

Proof: This is proved in [10], so we merely give a sketch of the proof. The idea is to embed the space of integral binary quartic forms into the space $W_4(\mathbb{Z})$ of pairs of integral quaternary quadratic forms:

$$\pi : V_4(\mathbb{Z}) \rightarrow W_4(\mathbb{Z})$$

$$ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 \mapsto \left(\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -24a & 6b & 2c \\ 0 & 6b & -4c & -3d \\ 0 & 2c & -3d & -6e \end{bmatrix} \right).$$

Under this map, the cubic resolvents of f and $\pi(f)$ are the same, and hence f and $\pi(f)$ have the same height and discriminant. We also note that π has an algebraic interpretation: the $\mathrm{PGL}_2(\mathbb{Z})$ -orbit of a nondegenerate element in $V_4(\mathbb{Z})$ with cubic resolvent $g(x)$ corresponds to an element in $H^1(\mathbb{Q}, E_g[2])$, while the $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_4(\mathbb{Z})$ -orbit of an element in $W_4(\mathbb{Z})$ corresponds with cubic resolvent $g(x)$ corresponds to an element in $H^1(\mathbb{Q}, E_g[4])$. Then the map π simply corresponds to natural map

$$H^1(\mathbb{Q}, E_g[2]) \rightarrow H^1(\mathbb{Q}, E_g[4]).$$

As proven in [6], every element in $W_4(\mathbb{Z})$ having integral coefficients and discriminant divisible by n^2 , for some squarefree integer n , is $\mathrm{GL}_2(\mathbb{Q}) \times \mathrm{GL}_4(\mathbb{Q})$ -equivalent to some element in $W_4(\mathbb{Z})$ whose discriminant is divisible by n^2 for mod n reasons (in the terminology of [4]). Then an application of the Ekedhal sieve in conjunction with geometry-of-numbers methods counting $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_4(\mathbb{Z})$ -orbits on $W_4(\mathbb{Z})$, yields the result. \square

7 Asymptotics for families of elliptic curves

Let p be a fixed prime. An elliptic curve E over \mathbb{Q} has either good reduction, multiplicative reduction, or additive reduction at p . For every prime $p \geq 5$, let Σ_p be a nonempty subset of possible reduction types. We say that $\Sigma = (\Sigma_p)_p$ is a *collection of reduction types* and that such a collection is *large* if for all large enough primes p , the set Σ_p contains at least the good and multiplicative reduction types.

For a large collection Σ , let $\mathcal{E}_{\mathrm{sf}}(\Sigma)$ (resp. $\mathcal{E}_\kappa(\Sigma)$) denote the set of elliptic curves $E \in \mathcal{E}_{\mathrm{sf}}$ (resp. $E \in \mathcal{E}_\kappa$) such that for all primes $p \geq 5$, the reduction type of E at p belongs to Σ_p . In this section, we prove the following theorem, from which Theorems 1.1 and 1.2 immediately follow.

Theorem 7.1 *Let Σ be a large collection of elliptic curves. Let $\kappa < 7/4$ be a positive constant. Then we have*

$$\#\{E \in \mathcal{E}_{\mathrm{sf}}(\Sigma)^\pm : C(E) < X\} \sim \frac{\alpha^\pm}{60\sqrt{3}} \frac{\Gamma(1/2)\Gamma(1/6)}{\Gamma(2/3)} \prod_p (c_g(p)e_g(p) + c_m(p)e_m(p) + c_a(p)e_a(p)) \cdot X^{5/6},$$

$$\#\{E \in \mathcal{E}_\kappa(\Sigma)^\pm : C(E) < X\} \sim \frac{\alpha^\pm}{60\sqrt{3}} \frac{\Gamma(1/2)\Gamma(1/6)}{\Gamma(2/3)} \prod_p (c_g(p)f_g(p) + c_m(p)f_m(p) + c_a(p)f_a(p)) \cdot X^{5/6},$$
(42)

where $\alpha^+ = 1$, $\alpha^- = \sqrt{3}$, $c_g(p)$ (resp. $c_m(p)$, $c_a(p)$) is 1 or 0 depending on whether Σ_p contains the good (resp. multiplicative, additive) reduction type, and $e_*(p)$ and $f_*(p)$ are given by

$$e_g(p) := 1 - \frac{1}{p}; \quad e_m(p) := \frac{1}{p} \left(1 + \frac{1}{p^{1/6}}\right) \left(1 - \frac{1}{p}\right)^2; \quad e_a(p) := \frac{1}{p^2} \left(1 + \frac{1}{p^{1/6}}\right) \left(1 - \frac{1}{p}\right);$$

$$f_g(p) := 1 - \frac{1}{p}; \quad f_m(p) := \frac{1}{p} \left(1 - \frac{1}{p^{1/6}}\right)^{-1} \left(1 - \frac{1}{p}\right)^2;$$

$$f_a(p) := \frac{1}{p^{5/3}} \left(1 - \frac{1}{p}\right) \left(1 + \frac{1}{p^{1/6}} + \frac{1}{p^{7/6}}\right) + \frac{1}{p^2} \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{p^{1/6}}\right)^{-1} \left(3 - \frac{2}{p^{1/2}}\right).$$

Furthermore, when elliptic curves in $\mathcal{E}_{\mathrm{sf}}(\Sigma)$ are ordered by conductor, the average size of their 2-Selmer groups is 3.

7.1 The family \mathcal{E} ordered by discriminant

We write elliptic curves $E \in \mathcal{E}$ in their minimal short Weierstrass model. In this case, it is easy to check that we have

$$\mathcal{E} = \{E_{AB} : j(E_{AB}) < \log(\Delta(E_{AB})), 16 \mid A, B \equiv 16 \pmod{64}, 3 \nmid A\}$$

Moreover, for every $E_{AB} \in \mathcal{E}$, we have $\Delta(E_{AB}) = \Delta(A, B)/2^8$. To count elements in \mathcal{E} with bounded discriminant, we need to incorporate the bound $j(E_{AB}) < \log \Delta(E_{AB})$, which is not a semialgebraic condition in A and B . However it is clearly definable in an o-minimal structure. Hence we use the following result of Barroero–Widmer [1, Theorem 1.3].

Theorem 7.2 *Let m and n be positive integers, let $\Lambda \subset \mathbb{R}^n$ be a lattice and denote the successive minima of Λ by λ_i . Let $Z \subset \mathbb{R}^{m+n}$ be a definable family, and suppose the fibers Z_T are bounded. Then there exists a constant $c_Z \in \mathbb{R}$, depending only on the family Z , such that*

$$\left| \#(Z_T \cap \Lambda) - \frac{\text{Vol}(Z_T)}{\det(\Lambda)} \right| \leq c_Z \sum_{j=0}^{n-1} \frac{V_j(Z_T)}{\lambda_1 \cdots \lambda_j},$$

where $V_j(Z_T)$ is the sum of the j -dimensional volumes of the orthogonal projections of Z_T on every j -dimensional coordinate subspace of \mathbb{R}^n .

For a pair $(A, B) \in \mathbb{R}^2$ with $\Delta(A, B) \neq 0$, let $j(A, B)$ denote $j(E_{AB})$. For any set $S \subset \mathbb{Z}^2$ defined by congruence conditions, let $\nu(S)$ denote the volume of the closure of S in $\hat{\mathbb{Z}}^2$. Equivalently, $\nu(S)$ is the product over the primes p of the closure of S in \mathbb{Z}_p^2 . We have the following immediate consequence of Theorem 7.2.

Proposition 7.3 *Let $\Lambda \subset \mathbb{Z}^2$ denote a set of pairs (A, B) defined by congruence conditions on A and B modulo some positive integer $n < X^{1/3-\epsilon}$. Then we have*

$$\#\{(A, B) \in \Lambda : j(A, B) < \log(2^{-8}\Delta(A, B)), 0 < \pm\Delta(A, B) < X\} = \nu(\Lambda)c_\infty^\pm(X) + O_\epsilon(X^{1/2+\epsilon}),$$

where $c_\infty^\pm(X)$ denotes the volume of the set

$$C^\pm(X) := \{(A, B) \in \mathbb{R}^2 : j(A, B) < \log(2^{-8}\Delta(A, B)), 0 < \pm\Delta(A, B) < X\}$$

computed with respect to Euclidean measure normalized so that \mathbb{Z}^2 has covolume 1.

Since the set \mathcal{E} arises by imposing congruence conditions modulo infinitely many primes, we use a simple sieve to determine asymptotics for the number of elliptic curves in \mathcal{E} with bounded discriminant.

Theorem 7.4 *We have*

$$\#\{E \in \mathcal{E} : 0 < \pm\Delta(E) < X\} \sim \frac{\alpha^\pm}{60\sqrt{3}} \cdot \frac{\Gamma(1/2)\Gamma(1/6)}{\Gamma(2/3)} \cdot \prod_{p \geq 5} \left(1 - \frac{1}{p^{10}}\right) X^{5/6},$$

where $\alpha^+ = 1$ and $\alpha^- = \sqrt{3}$.

Proof: First, we describe the set of elliptic curves $E_{AB} : y^2 = x^3 + Ax + B$ that have good reduction at 2 and 3 in Tables 3 and 4, respectively. In both tables, the first column describes the congruence conditions on A , the second describes congruence conditions at B , the third gives the 2-part (resp. the 3-part) of the discriminant $\Delta(A, B) = 4A^3 + 27B^2$, and the fourth column gives the density of these congruence conditions inside the space $(A, B) \in \mathbb{Z}_p^2$ for $p = 2$ and 3 . Below, δ is either 0 or 1.

We now apply Proposition 7.3. Let $1 \leq i \leq 9$ and $1 \leq j \leq 11$ be integers, and consider the set of integers (A, B) that satisfy line i of Table 3 and line j of Table 4. Let $\nu_{ij} = \nu_2(i) \cdot \nu_3(j)$ denote the density of this set of integers, and let $\Delta_{ij} = \Delta_2(i) \cdot \Delta_3(j)$ denote the product of the 2- and 3-parts of the discriminant $\Delta(A, B)$. It is necessary to count the number of pairs $(A, B) \in \mathbb{Z}^2$ that satisfy the following properties:

A	B	Δ_2	Density
$\equiv 0 \pmod{2^4}$	$\equiv 2^4 \pmod{2^6}$	2^8	2^{-10}
$\equiv (5 + \delta \cdot 2^6) \pmod{2^7}$	$\equiv (22 + \delta \cdot 2^6) \pmod{2^7}$	2^8	2^{-13}
$\equiv (13 + \delta \cdot 2^6) \pmod{2^7}$	$\equiv (14 + \delta \cdot 2^6) \pmod{2^7}$	2^8	2^{-13}
$\equiv (21 + \delta \cdot 2^6) \pmod{2^7}$	$\equiv (38 + \delta \cdot 2^6) \pmod{2^7}$	2^8	2^{-13}
$\equiv (29 + \delta \cdot 2^6) \pmod{2^7}$	$\equiv (94 + \delta \cdot 2^6) \pmod{2^7}$	2^8	2^{-13}
$\equiv (37 + \delta \cdot 2^6) \pmod{2^7}$	$\equiv (54 + \delta \cdot 2^6) \pmod{2^7}$	2^8	2^{-13}
$\equiv (45 + \delta \cdot 2^6) \pmod{2^7}$	$\equiv (46 + \delta \cdot 2^6) \pmod{2^7}$	2^8	2^{-13}
$\equiv (53 + \delta \cdot 2^6) \pmod{2^7}$	$\equiv (70 + \delta \cdot 2^6) \pmod{2^7}$	2^8	2^{-13}
$\equiv (61 + \delta \cdot 2^6) \pmod{2^7}$	$\equiv (126 + \delta \cdot 2^6) \pmod{2^7}$	2^8	2^{-13}

Table 3: Elliptic curves E_{AB} with good reduction at 2

A	B	Δ_3	Density
$3 \nmid A$	-	1	$2 \cdot 3^{-1}$
$3^4 \parallel A$	$3^6 \mid B$	3^{12}	$2 \cdot 3^{-11}$
$\equiv 2 \cdot 3^3 \pmod{3^6}$	$\equiv (\pm 20, \pm 34) \cdot 3^3 \pmod{3^7}$	3^{12}	$4 \cdot 3^{-13}$
$\equiv 5 \cdot 3^3 \pmod{3^6}$	$\equiv (\pm 11, \pm 16) \cdot 3^3 \pmod{3^7}$	3^{12}	$4 \cdot 3^{-13}$
$\equiv 8 \cdot 3^3 \pmod{3^6}$	$\equiv (\pm 2, \pm 29) \cdot 3^3 \pmod{3^7}$	3^{12}	$4 \cdot 3^{-13}$
$\equiv 11 \cdot 3^3 \pmod{3^6}$	$\equiv (\pm 7, \pm 20) \cdot 3^3 \pmod{3^7}$	3^{12}	$4 \cdot 3^{-13}$
$\equiv 14 \cdot 3^3 \pmod{3^6}$	$\equiv (\pm 16, \pm 38) \cdot 3^3 \pmod{3^7}$	3^{12}	$4 \cdot 3^{-13}$
$\equiv 17 \cdot 3^3 \pmod{3^6}$	$\equiv (\pm 2, \pm 25) \cdot 3^3 \pmod{3^7}$	3^{12}	$4 \cdot 3^{-13}$
$\equiv 20 \cdot 3^3 \pmod{3^6}$	$\equiv (\pm 7, \pm 34) \cdot 3^3 \pmod{3^7}$	3^{12}	$4 \cdot 3^{-13}$
$\equiv 23 \cdot 3^3 \pmod{3^6}$	$\equiv (\pm 11, \pm 38) \cdot 3^3 \pmod{3^7}$	3^{12}	$4 \cdot 3^{-13}$
$\equiv 26 \cdot 3^3 \pmod{3^6}$	$\equiv (\pm 25, \pm 29) \cdot 3^3 \pmod{3^7}$	3^{12}	$4 \cdot 3^{-13}$

Table 4: Elliptic curves E_{AB} with good reduction at 3

1. The pair (A, B) satisfies the i th (resp. j)th condition of Table 3 (resp. Table 4);
2. $0 < \pm \Delta(A, B) < \Delta_{ij} X$;
3. $j(A, B) < \log(\Delta(A, B)/\Delta_{ij})$;
4. for all primes $p \geq 5$, either $p^4 \nmid A$ or $p^6 \nmid B$.

Counting the pairs (A, B) which satisfy the first four properties is immediate from Proposition 7.3, and the fifth condition can be imposed by applying a simple inclusion exclusion sieve. We thus obtain

$$\#\{E \in \mathcal{E} : 0 < \pm \Delta(E) < X\} \sim \sum_{i,j} \nu_{ij} \cdot \prod_{p \geq 5} (1 - p^{-10}) \cdot c_{\infty}^{\pm}(\Delta_{ij} \cdot X).$$

The values $c_{\infty}^{\pm}(X)$ scale as follows: we have

$$c_{\infty}^{\pm}(X) = X^{5/6} c_{\infty}^{\pm}(1) + o(X).$$

Furthermore, the values $c_{\infty}^{\pm}(1)$ are computed in [31, §2] to be

$$c_{\infty}^{+}(1) = \frac{2}{4^{1/3} \cdot 27^{1/2}} \cdot \frac{1}{5} \cdot B(1/2, 1/6); \quad c_{\infty}^{-}(1) = \frac{2}{4^{1/3} \cdot 27^{1/2}} \cdot \frac{3}{5} \cdot B(1/2, 1/3) = \sqrt{3} c_{\infty}^{+}(1).$$

Above, $B(x, y)$ denotes the beta function given by

$$B(x, y) = \int_0^1 t^{x-1} (1-t)^{y-1} dt = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)}.$$

We therefore obtain

$$\begin{aligned}
\#\{E \in \mathcal{E} : 0 < \pm\Delta(E) < X\} &\sim \sum_{i,j} \nu_{ij} \Delta_{ij}^{5/6} \cdot \prod_{p \geq 5} (1 - p^{-10}) \cdot c_{\infty}^{\pm}(1) \cdot X^{5/6} \\
&= c_{\infty}^{\pm}(1) \left(\sum_i \nu_2(i) \Delta_2(i)^{5/6} \right) \left(\sum_i \nu_3(i) \Delta_3(i)^{5/6} \right) \prod_{p \geq 5} (1 - p^{-10}) \cdot X^{5/6} \\
&= \frac{2^{2/3}}{4} \frac{2\alpha^{\pm}}{4^{1/3} \cdot 3^{3/2} \cdot 5} \frac{\Gamma(1/2)\Gamma(1/6)}{\Gamma(2/3)} \prod_{p \geq 5} (1 - p^{-10}) \cdot X^{5/6} \\
&= \frac{\alpha^{\pm}}{60\sqrt{3}} \frac{\Gamma(1/2)\Gamma(1/6)}{\Gamma(2/3)} \prod_{p \geq 5} (1 - p^{-10}) \cdot X^{5/6},
\end{aligned}$$

as necessary \square

7.2 Ordering elliptic curves by conductor

Suppose that \mathcal{G} is equal to $\mathcal{E}_*(\Sigma)$ for a large collection of reduction types Σ , where $*$ is either sf or some positive $\kappa < 7/4$. Pick a small positive constant $\delta < 1/9$. Then there exists a positive constant θ such that

$$\begin{aligned}
\#\{E \in \mathcal{G}^{\pm} : C(E) < X\} &= \sum_{n \geq 1} \#\{E \in \mathcal{G}^{\pm} : \text{ind}(E) = n; \Delta(E) < nX\} \\
&= \sum_{\substack{n, q \geq 1 \\ nq < X^{\delta}}} \mu(q) \#\{E \in \mathcal{G}^{\pm} : nq \mid \text{ind}(E); \Delta(E) < nX\} \\
&= \sum_{\substack{n, q \geq 1 \\ nq < X^{\delta}}} \mu(q) \#\{E \in \mathcal{G}^{\pm} : nq \mid \text{ind}(E); \Delta(E) < nX\} + O(X^{5/6-\theta})
\end{aligned} \tag{43}$$

where we bound the tail using the uniformity estimates in Theorems 1.4 and 1.5. We perform another inclusion exclusion sieve to evaluate each summand of the right hand side of the above equation: for each prime p , let $\chi_{\Sigma_p, nq} : \mathbb{Z}_p^2 \rightarrow \mathbb{R}$ denote the characteristic function of the set of all $(A, B) \in \mathbb{Z}_p^2$ that satisfy the reduction type specified by Σ_p and satisfy $nq \mid \text{ind}(E_{AB})$. Let χ_p denote $1 - \chi_{\Sigma_p, nq}$, and define $\chi_k := \prod_{p \mid k} \chi_p$ for squarefree integers k . Then we have

$$\prod_p \chi_{\Sigma_p, nq}(A, B) = \sum_k \mu(k) \chi_k(A, B)$$

for every $(A, B) \in \mathbb{Z}^2$. Set $\nu_*(nq, \Sigma)$ to be the product over all primes p of the integral of $\chi_{\Sigma_p, nq}$. Therefore, for $nq < X^{\delta}$, we obtain

$$\begin{aligned}
\#\{E \in \mathcal{G}^{\pm} : nq \mid \text{ind}(E); \Delta(E) < nX\} &= \sum_{\substack{(A, B) \in \mathbb{Z}^2 \\ 0 < \pm\Delta(E_{AB}) < nX}} \sum_{k \geq 1} \mu(k) \chi_k(A, B) \\
&= \sum_{\substack{(A, B) \in \mathbb{Z}^2 \\ 0 < \pm\Delta(E_{AB}) < nX}} \sum_{k=1}^{X^{4\delta}} \mu(k) \chi_k(A, B) + O\left(\frac{(nX)^{5/6}}{X^{2\delta}}\right) \\
&= c_{\infty}^{\pm}(nX) \nu_*(nq, \Sigma) + O_{\epsilon}(X^{1/2+2\delta+\epsilon} + X^{5/6-7\delta/6}),
\end{aligned}$$

where the second equality follows from the uniformity estimate in Proposition 6.4, and the third follows from Proposition 7.3 and adding up the volume terms by simply reversing the inclusion exclusion sieve. Note that the constant δ has been specifically picked to be small enough so that Proposition 7.3 applies.

For each n , let $\lambda_*(n, \Sigma)$ denote the volume of the closure in $\hat{\mathbb{Z}}^2$ of the set of all $(A, B) \in \mathbb{Z}^2$ such that E_{AB} belongs to $\mathcal{G} = \mathcal{E}_*(\Sigma)$ and E_{AB} has index n . Returning to (43), we obtain

$$\begin{aligned} \#\{E \in \mathcal{G}^\pm : C(E) < X\} &= c_\infty^\pm(1)X^{5/6} \sum_{\substack{n, q \geq 1 \\ nq < X^\delta}} \mu(q)n^{5/6}\nu_*(nq, \Sigma) + o(X^{5/6}) \\ &= c_\infty^\pm(1)X^{5/6} \sum_{n \geq 1} n^{5/6}\lambda_*(n, \Sigma), \end{aligned}$$

where again, the final equality follows by reversing the inclusion exclusion sieve of (43).

For each prime p and $k \geq 0$, let $\bar{\nu}_*(p^k, \Sigma)$ denote the p -adic density of the set of all $(A, B) \in \mathbb{Z}^2$ such that $E_{AB} \in \mathcal{E}_*(\Sigma)$ and $\text{ind}_p(E_{AB}) = p^k$. The constant $\lambda_*(n, \Sigma)$ is a product over all p of local densities:

$$\begin{aligned} \lambda_*(n, \Sigma) &= \prod_{p^n} \bar{\nu}_*(p^0, \Sigma) \prod_{\substack{p^k \parallel n \\ k \geq 1}} \bar{\nu}_*(p^k, \Sigma) \\ &= \prod_p \bar{\nu}_*(p^0, \Sigma) \prod_{\substack{p^k \parallel n \\ k \geq 1}} \frac{\bar{\nu}_*(p^k, \Sigma)}{\bar{\nu}_*(p^0, \Sigma)}. \end{aligned}$$

Hence $\lambda_*(n, \Sigma)$ is a multiplicative function in n , and we have

$$\begin{aligned} \sum_{n \geq 1} n^{5/6}\lambda_*(n, \Sigma) &= \prod_p \bar{\nu}_*(p^0, \Sigma) \prod_p \left(\sum_{k=0}^{\infty} p^{5k/6} \frac{\bar{\nu}_*(p^k, \Sigma)}{\bar{\nu}_*(p^0, \Sigma)} \right) \\ &= \prod_p \left(\sum_{k=0}^{\infty} p^{5k/6} \bar{\nu}_*(p^k, \Sigma) \right). \end{aligned}$$

The values of $\bar{\nu}_*(p^k, \Sigma)$ are easily computed from Table 2. We then have (42), proving the first part of Theorem 7.1.

7.3 The average size of the 2-Selmer groups of elliptic curves in $\mathcal{E}_{\text{sf}}(\Sigma)$

Let Σ be a large collection of reduction types. For a positive integers n and a positive real number X , let $\mathcal{E}(\Sigma, n, X)$ denote the set of elliptic curves $E \in \mathcal{E}_{\text{sf}}(\Sigma)$, such that $n \mid \text{ind}(E)$ and $|\Delta(E)| < X$. Then, as in the previous subsection, we have

$$\begin{aligned} \sum_{\substack{E \in \mathcal{E}(\Sigma)^\pm \\ C(E) < X}} (|\text{Sel}_2(E)| - 1) &= \sum_{n, q \geq 1} \mu(q) \sum_{E \in \mathcal{E}(\Sigma, nq, nX)^\pm} (|\text{Sel}_2(E)| - 1) \\ &= \sum_{\substack{n, q \geq 1 \\ nq < X^\theta}} \mu(q) \sum_{E \in \mathcal{E}(\Sigma, nq, nX)^\pm} (|\text{Sel}_2(E)| - 1) + O_\epsilon(X^{5/6 - \theta/6 + \epsilon}), \end{aligned}$$

for every $\theta > 0$, where the second equality is a consequence of Theorem 1.4. Therefore, the final assertion of Theorem 7.1 follows immediately from the following result.

Proposition 7.5 *There exist positive constants θ and θ_1 such that*

$$\sum_{E \in \mathcal{E}(\Sigma, nq, nX)^\pm} (|\text{Sel}_2(E)| - 1) = 2|\mathcal{E}(\Sigma, nq, nX)^\pm| + O(X^{5/6 - \theta_1}),$$

for every $nq < X^\theta$.

Given the uniformity estimate Proposition 6.5 that we have already proved, the proof of Proposition 7.5 very closely follows the proof of [7, Theorem 3.1]. In what follows, we briefly sketch the proof of Theorem 7.1, indicating the change needed at the places where it differs from [7]. The starting point of the proof is the following parametrization of the 2-Selmer groups of elliptic curves in terms of orbits on integral binary quartic forms. This correspondence is due to Birch and Swinnerton-Dyer, and we state it in the form of [7, Theorem 3.5].

Theorem 7.6 *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over \mathbb{Q} , and set $I = I(E) := -3A$ and $J = J(E) := -27B$. Then there is a bijection between $\text{Sel}_2(E)$ and the set of $\text{PGL}_2(\mathbb{Q})$ -equivalence classes of locally soluble integral binary quartic forms with invariants 2^4I and 2^6J .*

Moreover, 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 $\text{PGL}_2(\mathbb{Q})$ -equivalence class, and this class corresponds to the identity element in $\text{Sel}_2(\mathbb{Q})$.

The second step in the proof is to obtain asymptotics for the number of $\text{PGL}_2(\mathbb{Z})$ -orbits on the set of integral binary quartic forms whose coefficients satisfy congruence conditions modulo some small number n , where these forms have bounded invariants. In [7], the invariants were bounded by height. Here instead, we bound their discriminants and corresponding j -invariant: for an element $f \in V_4(\mathbb{R})$ with $\Delta(f) \neq 0$, define $j(f)$ to be $j(E)$ with E given by

$$E : y^2 = x^3 - (I/3)x - J/27.$$

For any $\text{PGL}_2(\mathbb{Z})$ -invariant set $S \subset V_4(\mathbb{Z})$, let $N_4^{(i)}(S; X)$ denote the number the number of $\text{PGL}_2(\mathbb{Z})$ -orbits on integral elements $f \in S \subset V_4^{(i)}(\mathbb{Z})$, that do not have a linear factor over \mathbb{Q} , and satisfy $\Delta(f) < X$ and $j(f) < \log \Delta(f)$.

In §5, we defined the sets $R^{(i)}$ which are fundamental sets for the action of $\text{PGL}_2(\mathbb{R})$ on $V(\mathbb{R})^{(i)}$. Then $R^{(i)}$ contains one element $f \in V(\mathbb{R})^{(i)}$ having invariants I and J , for each $(I, J) \in \mathbb{R}^2$ with $4I^3 - J^2 \in \mathbb{R}_{>0}$ for $i = 0, 2\pm$ and $4I^3 - J^2 \in \mathbb{R}_{<0}$ for $i = 1$. Furthermore, the coefficients of such an f are bounded by $O(H(f)^{1/6})$. Define the sets

$$R^{(i)}(X) := \{f \in R^{(i)} : 0 < |\Delta(f)| < X; j(f) < \log \Delta(f)\}.$$

Clearly, if $f \in R^{(i)}(X)$ with $\Delta(f) = X$, then $H(f) \ll X^{1+\epsilon}$ and so the coefficients of f are bounded by $O(X^{1/6+\epsilon})$.

Let $\delta = 1/18$ be fixed. Let $L \subset V(\mathbb{Z})$ be a lattice defined by congruence conditions modulo n , where $n < X^\delta$. Denote the set of elements in L that have no linear factor by L^{irr} and define $\nu(L)$ to be the volume of the completion of L in $V_4(\hat{\mathbb{Z}})$. Let $G_0 \subset \text{PGL}_2(\mathbb{R})$ be a nonempty bounded open ball, and set $n_1 = 2$, $n_0 = n_{2\pm} = 4$. Identically to [7, §2.3], it follows that $N_4^{(i)}(L, X)$ is given by

$$\begin{aligned} N_4^{(i)}(L, X) &= \frac{1}{n_i \text{Vol}(G_0)} \int_{\gamma \in \text{PGL}_2(\mathbb{Z}) \setminus \text{PGL}_2(\mathbb{R})} \#\{\gamma G_0 \cdot R^{(i)}(X) \cap L^{\text{irr}}\} d\gamma \\ &= \frac{1}{n_i} \int_{\gamma \in \text{PGL}_2(\mathbb{Z}) \setminus \text{PGL}_2(\mathbb{R})} \nu(L) \text{Vol}(G_0 \cdot R^{(i)}(X)) d\gamma + O(X^{7/9}), \end{aligned} \tag{44}$$

where the error term is obtained in a similar manner to [7, (18)–(20)]. There are two differences: first, we use Theorem 7.2 (instead of Davenport's result stated as [7, Proposition 2.6]) to estimate the number of lattice points in $\gamma G_0 \cdot R^{(i)}(X)$. Second, since we are imposing congruence conditions on L modulo $n < X^\delta$ with $\delta = 1/18$, we cut off the integral over γ when the t -coefficient of γ in its Iwasawa coordinate is $\gg X^{1/36}$. That way, the coefficients of the ball $\gamma G_0 \cdot R^{(i)}(X)$ are always bigger than n . The precise values of $\delta = 1/18$ and $7/9$, the exponent of the error term, are not important.

The third step in the proof is to introduce a bounded weight function $m : V_4(\mathbb{Z}) \rightarrow \mathbb{R}$, which is the product $m = \prod_p m_p$ of local weight functions $m_p : V_4(\mathbb{Z}_p) \rightarrow \mathbb{R}$, such that for all but negligibly many ($\ll_\epsilon X^{3/4+\epsilon}$) elliptic curves E_{AB} , we have

$$|\text{Sel}_2(E_{AB})| - 1 = \sum_{f \in \frac{V_4(\mathbb{Z})_{A,B}}{\text{PGL}_2(\mathbb{Z})}} m(f),$$

where f is varying over $\mathrm{PGL}_2(\mathbb{Z})$ -orbits on integral binary quartic forms with no linear factor and invariants $I(f) = -3 \cdot 2^4 I$ and $J(f) = -27 \cdot 2^6 J$. In our situation, we do not need any changes to this part of the proof.

The fourth and final part of the proof is to perform a sieve so as to count $\mathrm{PGL}_2(\mathbb{Z})$ -orbits on integral binary quartic forms with bounded invariants, so that each form f is weighted by $m(f)$. Performing a standard inclusion-exclusion sieve using (44) together with the uniformity estimate Proposition 6.5 and the volume computations of [7, §3.3 and §3.6] yields Proposition 7.5. This concludes the proof of Theorem 7.1.

References

- [1] Fabrizio Barroero and Martin Widmer, *Counting lattice points and O -minimal structures*, Int. Math. Res. Not. IMRN (2014), no. 18, 4932–4957. MR 3264671
- [2] Manjul Bhargava, *Higher composition laws. II. On cubic analogues of Gauss composition*, Ann. of Math. (2) **159** (2004), no. 2, 865–886.
- [3] ———, *The density of discriminants of quartic rings and fields*, Ann. of Math. (2) **162** (2005), no. 2, 1031–1063.
- [4] ———, *The geometric squarefree sieve and unramified nonabelian extensions of quadratic fields*, 2014, <http://arxiv.org/abs/1402.0031>.
- [5] Manjul Bhargava and Piper Harron, *The equidistribution of lattice shapes of rings of integers in cubic, quartic, and quintic number fields*, Compos. Math. **152** (2016), no. 6, 1111–1120. MR 3518306
- [6] Manjul Bhargava and Arul Shankar, *The average number of elements in the 4-selmer groups of elliptic curves is 7*, <http://arxiv.org/abs/1312.7333>.
- [7] Manjul Bhargava and Arul Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. of Math. (2) **181** (2015), no. 1, 191–242. MR 3272925
- [8] Manjul Bhargava, Arul Shankar, Takashi Taniguchi, Frank Thorne, Jacob Tsimerman, and Yongqiang Zhao, *Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves*, (2017, preprint), <http://arxiv.org/abs/1701.02458>.
- [9] Manjul Bhargava, Arul Shankar, and Jacob Tsimerman, *On the Davenport-Heilbronn theorems and second order terms*, Invent. Math. **193** (2013), no. 2, 439–499. MR 3090184
- [10] Manjul Bhargava, Arul Shankar, and Jerry Wang, *Geometry-of-numbers methods over global fields II: Coregular vector spaces*.
- [11] ———, *Squarefree values of polynomial discriminants II*.
- [12] ———, *Geometry-of-numbers methods over global fields I: Prehomogeneous vector spaces*, 2015, <http://arxiv.org/abs/1512.03035>.
- [13] ———, *Squarefree values of polynomial discriminants I*, 2016, <http://arxiv.org/abs/1611.09806>.
- [14] Armand Brumer, *The average rank of elliptic curves. I*, Invent. Math. **109** (1992), no. 3, 445–472.
- [15] Armand Brumer and Kenneth Kramer, *The rank of elliptic curves*, Duke Math. J. **44** (1977), no. 4, 715–743. MR 0457453
- [16] Armand Brumer and Oisín McGuinness, *The behavior of the Mordell-Weil group of elliptic curves*, Bull. Amer. Math. Soc. (N.S.) **23** (1990), no. 2, 375–382.
- [17] Val Chiche-Lapierre, *Length of elements in a minkowski basis for an order in a number field*, PhD dissertation, University of Toronto, 2019, forthcoming.

- [18] Henri Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000. MR 1728313
- [19] H. Davenport, *On a principle of Lipschitz*, J. London Math. Soc. **26** (1951), 179–183.
- [20] B. N. Delone and D. K. Faddeev, *Theory of Irrationalities of Third Degree*, Acad. Sci. URSS. Trav. Inst. Math. Stekloff, **11** (1940), 340. MR 0004269
- [21] W. Duke and E. Kowalski, *A problem of Linnik for elliptic curves and mean-value estimates for automorphic representations*, Invent. Math. **139** (2000), no. 1, 1–39, With an appendix by Dinakar Ramakrishnan. MR 1728875
- [22] É. Fouvry, M. Nair, and G. Tenenbaum, *L'ensemble exceptionnel dans la conjecture de Szpiro*, Bull. Soc. Math. France **120** (1992), no. 4, 485–506. MR 1194273
- [23] Wee Teck Gan, Benedict Gross, and Gordan Savin, *Fourier coefficients of modular forms on G_2* , Duke Math. J. **115** (2002), no. 1, 105–169. MR 1932327
- [24] Dorian Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), Lecture Notes in Math., vol. 751, Springer, Berlin, 1979, pp. 108–118.
- [25] D. R. Heath-Brown, *The average analytic rank of elliptic curves*, Duke Math. J. **122** (2004), no. 3, 591–623.
- [26] Ruthi Hortsch, *Counting elliptic curves of bounded Faltings height*, Acta Arith. **173** (2016), no. 3, 239–253. MR 3512854
- [27] Nicholas M. Katz and Peter Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, vol. 45, American Mathematical Society, Providence, RI, 1999.
- [28] F Levi, *Kubische Zahlkörper und binäre kubische Formenklassen*, Akad. Wiss. Leipz., Mat.-Nat. Kl., 26–37.
- [29] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR 1312368
- [30] Takashi Taniguchi and Frank Thorne, *Levels of distribution for sieve problems in prehomogeneous vector spaces*, 2014, <http://arxiv.org/abs/1707.01850>.
- [31] Mark Watkins, *Some heuristics about elliptic curves*, Experiment. Math. **17** (2008), no. 1, 105–125.
- [32] Matthew P. Young, *Low-lying zeros of families of elliptic curves*, J. Amer. Math. Soc. **19** (2006), no. 1, 205–250.