Invent math (2013) 193:439–499
DOI 10.1007/s00222-012-0433-0

On the Davenport–Heilbronn theorems and second order terms

Manjul Bhargava · Arul Shankar · Jacob Tsimerman

Received: 30 May 2010 / Accepted: 17 October 2012 / Published online: 11 December 2012

Abstract We give simple proofs of the Davenport–Heilbronn theorems, which provide the main terms in the asymptotics for the number of cubic fields having bounded discriminant and for the number of 3-torsion elements in the class groups of quadratic fields having bounded discriminant. We also establish second main terms for these theorems, thus proving a conjecture of Roberts. Our arguments provide natural interpretations for the various constants appearing in these theorems in terms of local masses of cubic rings.

1 Introduction

The classical theorems of Davenport and Heilbronn [15] provide asymptotic formulae for the number of cubic fields having bounded discriminant and for the total number of 3-torsion elements in the class groups of quadratic fields having bounded discriminant. Specifically, the theorems state:

M. Bhargava (✉)
Department of Mathematics, Princeton University, Princeton, NJ 08544, USA
e-mail: bhargava@math.princeton.edu

A. Shankar
Institute for Advanced Study, Princeton, NJ 08540, USA
e-mail: ashankar@math.ias.edu

J. Tsimerman
Department of Mathematics, Harvard University, Cambridge, MA 02138, USA
e-mail: jacobt@math.harvard.edu

Theorem 1 (Davenport–Heilbronn) *Let* $N_3(\xi,\eta)$ *denote the number of cubic fields* K*, up to isomorphism, that satisfy* $\xi < \mathrm{Disc}(K) < \eta$*. Then*

$$\begin{aligned} N_3(0,X) &= \frac{1}{12\zeta(3)}X + o(X);\\ N_3(-X,0) &= \frac{1}{4\zeta(3)}X + o(X). \end{aligned} \tag{1}$$

Theorem 2 (Davenport–Heilbronn) *Let* D *denote the discriminant of a quadratic field and let* $\mathrm{Cl}_3(D)$ *denote the* 3*-torsion subgroup of the ideal class group* $\mathrm{Cl}(D)$ *of* D*. Then*

$$\begin{aligned} \sum_{0<D<X} \#\mathrm{Cl}_3(D) &= \frac{4}{3}\cdot \sum_{0<D<X} 1 + o(X);\\ \sum_{-X<D<0} \#\mathrm{Cl}_3(D) &= 2\cdot \sum_{-X<D<0} 1 + o(X). \end{aligned} \tag{2}$$

The Davenport–Heilbronn theorems, and the methods underlying their proofs, have seen applications in numerous works (see, e.g., [1, 3, 5, 10, 18, 19, 32, 33]).

Subsequent to their 1971 paper, extensive computations were undertaken by a number of authors (see, e.g., Llorente–Quer [25] and Fung–Williams [20]) in an attempt to numerically verify the Davenport–Heilbronn theorems. However, computations up to discriminants even as large as 10^7 were found to agree quite poorly with these theorems. This in turn led to questions about the magnitude of the error term in these theorems, and the problem of determining precise second order terms.

In a related work, Belabas [1] developed a very fast method for enumerating cubic fields—indeed, in essentially linear time with the discriminant—allowing him to make tables of cubic fields up to absolute discriminant 10^{11}. These computations still seemed to agree rather poorly with the first Davenport–Heilbronn theorem, and led Belabas to guess only the existence of error terms smaller than $O(X/(\log X)^a)$ for any a. However, Belabas [2] later obtained the first subexponential error terms for these theorems of the form $O(X\exp(-\sqrt{\log X \log\log X}))$.

In 2000, Roberts [26] conducted a remarkable study of these latter computations in conjunction with certain theoretical considerations, which led him to conjecture a precise *second main term* for Theorem 1. This conjectural second main term took the form of a certain explicit constant times $X^{5/6}$. Further computations carried out in the last few years have revealed Roberts' conjecture to agree extremely well with the data. Meanwhile, on the theoretical side, power-saving error terms for Theorems 1 and 2 were obtained by Belabas, the first author, and Pomerance [4], who showed error terms of $O(X^{7/8+\epsilon})$.

The purpose of the current article is to prove the above conjecture of Roberts. More precisely, we prove the following theorem.

Theorem 3 *Let $N_3(\xi,\eta)$ denote the number of cubic fields K, up to isomorphism, that satisfy $\xi < \mathrm{Disc}(K) < \eta$. Then*

$$\begin{aligned} N_3(0,X) &= \frac{1}{12\zeta(3)}X + \frac{4\zeta(1/3)}{5\Gamma(2/3)^3\zeta(5/3)}X^{5/6} + O_\epsilon\big(X^{5/6-1/48+\epsilon}\big);\\ N_3(-X,0) &= \frac{1}{4\zeta(3)}X + \frac{\sqrt{3}\cdot 4\zeta(1/3)}{5\Gamma(2/3)^3\zeta(5/3)}X^{5/6} + O_\epsilon\big(X^{5/6-1/48+\epsilon}\big). \end{aligned} \tag{3}$$

Davenport and Heilbronn also proved a refined version of Theorem 1, where they give the asymptotics for the number of cubic fields K having bounded discriminant satisfying any specified set of splitting conditions at finitely many primes. Roberts also conjectures a precise second main term for the number of such fields K having discriminant bounded by X (see [26, Sect. 5]). We also prove Roberts' refined conjecture in Sect. 9.

By essentially identical methods, we also prove the analogue of Roberts' conjecture for the second Davenport–Heilbronn theorem, i.e., a precise second order term in Theorem 2. Specifically, we prove:

Theorem 4 *Let D denote the discriminant of a quadratic field and let $\mathrm{Cl}_3(D)$ denote the 3-torsion subgroup of the ideal class group $\mathrm{Cl}(D)$ of D. Then*

$$\begin{aligned} \sum_{0<D<X} \#\mathrm{Cl}_3(D) &= \frac{4}{3}\cdot \sum_{0<D<X} 1 + \frac{8\zeta(1/3)}{5\Gamma(2/3)^3}\prod_p\left(1-\frac{p^{1/3}+1}{p(p+1)}\right)X^{5/6}\\ &\quad + O_\epsilon\big(X^{5/6-1/48+\epsilon}\big);\\ \sum_{-X<D<0} \#\mathrm{Cl}_3(D) &= 2\cdot \sum_{-X<D<0} 1 + \frac{\sqrt{3}\cdot 8\zeta(1/3)}{5\Gamma(2/3)^3}\prod_p\left(1-\frac{p^{1/3}+1}{p(p+1)}\right)X^{5/6}\\ &\quad + O_\epsilon\big(X^{5/6-1/48+\epsilon}\big). \end{aligned} \tag{4}$$

In the process, we present a simpler approach to proving the original Davenport–Heilbronn theorems, and also a simpler approach to establishing the theorem of Davenport [13] on the density of discriminants of binary cubic forms. The second main term of the latter theorem of Davenport (who obtained only a second term of $O(X^{15/16})$) was first discovered by Shintani [30] using Sato and Shintani's theory of zeta functions for prehomogeneous vector spaces [27]. In this article, we also give an elementary derivation of this second main term of Shintani. More precisely, we prove:

Theorem 5 (Davenport–Shintani) *Let $N(\xi,\eta)$ denote the number of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of irreducible integer-coefficient binary cubic forms f satisfying $\xi < \mathrm{Disc}(f) < \eta$. Then*

$$\begin{aligned} N(0,X) &= \frac{\pi^2}{72}X + \frac{\sqrt{3}\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{30\Gamma(2/3)}X^{5/6} + O_\epsilon\big(X^{3/4+\epsilon}\big); \\ N(-X,0) &= \frac{\pi^2}{24}X + \frac{\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{10\Gamma(2/3)}X^{5/6} + O_\epsilon\big(X^{3/4+\epsilon}\big). \end{aligned} \tag{5}$$

In order to prove Theorems 3 and 4, we need (in particular) to apply a new, stronger version of Theorem 5 where we count equivalence classes of binary cubic forms satisfying any finite or other suitable set of congruence conditions. Such a theorem was obtained by Davenport–Heilbronn but their method does not yield second main terms. Meanwhile, Shintani's zeta function method does not immediately apply to cubic forms satisfying given congruence conditions. We prove this congruence version of Theorem 5 in Sect. 6.

In fact, we use this more general version of Theorem 5 to prove a generalization of Theorems 3 and 4 that also allows us to count cubic orders satisfying certain specified sets of local conditions. To state this more general theorem, we first restate Theorem 5 as:

Theorem 6 *Let $M_3(\xi,\eta)$ denote the number of isomorphism classes of orders R in cubic fields that satisfy $\xi < \mathrm{Disc}(R) < \eta$. Then*

$$\begin{aligned} M_3(0,X) &= \frac{\pi^2}{72}X + \frac{\sqrt{3}\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{30\Gamma(2/3)}X^{5/6} + O_\epsilon(X^{3/4+\epsilon}); \\ M_3(-X,0) &= \frac{\pi^2}{24}X + \frac{\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{10\Gamma(2/3)}X^{5/6} + O_\epsilon(X^{3/4+\epsilon}). \end{aligned} \tag{6}$$

The proof of Theorem 6 is relatively straightforward, given Theorem 5 and the "Delone–Faddeev bijection" between isomorphism classes of cubic orders and $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of irreducible binary cubic forms (which we describe in more detail in Sect. 2).

The generalization of Theorems 3 and 4 (which will also then include Theorem 6) that we will prove allows one to count cubic orders of bounded discriminant satisfying any desired finite (or, in many natural cases, infinite) sets of local conditions. To state the theorem, for each prime p let Σ_p be any set of isomorphism classes of orders in étale cubic algebras over $\mathbb{Q}_p$; also, let Σ_∞ denote any set of isomorphism classes of étale cubic algebras over $\mathbb{R}$ (i.e., $\Sigma_\infty \subseteq \{\mathbb{R}^3, \mathbb{R}\oplus\mathbb{C}\}$). We say that the collection $(\Sigma_p)\cup\Sigma_\infty$ is *acceptable* if, for all sufficiently large primes p, the set Σ_p contains all maximal cubic orders over $\mathbb{Z}_p$ that are not totally ramified. We say that the collection $(\Sigma_p) \cup \Sigma_\infty$ is *strongly acceptable* if, for all sufficiently large primes p, the set Σ_p consists of the set of all cubic orders over $\mathbb{Z}_p$, the set of all maximal cubic orders over $\mathbb{Z}_p$, or the set of all maximal cubic orders over $\mathbb{Z}_p$ that are not totally ramified.

We wish to asymptotically count the total number of cubic orders R of absolute discriminant less than X that agree with such local specifications, i.e., $R \otimes \mathbb{Z}_p \in \Sigma_p$ for all p and $R \otimes \mathbb{R} \in \Sigma_\infty$. This asymptotic count—with the first *two* main terms—is contained in the following theorem:

Theorem 7 *Let $(\Sigma_p) \cup \Sigma_\infty$ be a strongly acceptable collection of local specifications, and let Σ denote the set of all isomorphism classes of orders R in cubic fields for which $R \otimes \mathbb{Z}_p \in \Sigma_p$ for all p and $R \otimes \mathbb{R} \in \Sigma_\infty$. For a free $\mathbb{Z}_p$-module M, define $M^{\mathrm{Prim}} \subset M$ by $M^{\mathrm{Prim}} := M \backslash \{p \cdot M\}$. Let $N_3(\Sigma; X)$ denote the number of cubic orders $R \in \Sigma$ that satisfy $|\mathrm{Disc}(R)| < X$. Then*

$$\begin{aligned} N_3(\Sigma; X) &= \left(\frac{1}{2} \sum_{R \in \Sigma_\infty} \frac{1}{|\mathrm{Aut}(R)|}\right) \cdot \prod_p \left(\frac{p-1}{p} \cdot \sum_{R \in \Sigma_p} \frac{1}{\mathrm{Disc}_p(R)} \cdot \frac{1}{|\mathrm{Aut}(R)|}\right) \cdot X \\ &\quad + \frac{1}{\zeta(2)} \left(\sum_{R \in \Sigma_\infty} c_2(R)\right) \cdot \prod_p \Bigg(\left(1 - p^{-1/3}\right) \\ &\quad \cdot \sum_{R \in \Sigma_p} \frac{1}{\mathrm{Disc}_p(R)} \cdot \frac{1}{|\mathrm{Aut}(R)|} \int_{(R/\mathbb{Z}_p)^{\mathrm{Prim}}} i(x)^{2/3} dx \Bigg) \cdot X^{5/6} \\ &\quad + O_\epsilon\left(X^{5/6 - 1/48 + \epsilon}\right), \end{aligned} \tag{7}$$

where $\mathrm{Disc}_p(R)$ denotes the discriminant of R over $\mathbb{Z}_p$ as a power of p, $i(x)$ denotes the index of $\mathbb{Z}_p[x]$ in R, dx assigns measure 1 to $(R/\mathbb{Z}_p)^{\mathrm{Prim}}$, and

$$c_2(R) = \begin{cases} \frac{\sqrt{3}\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{30\Gamma(2/3)} & \text{if } R \cong \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R} \\ \frac{\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{10\Gamma(2/3)} & \text{if } R \cong \mathbb{R} \oplus \mathbb{C}. \end{cases}$$

Note that the case where Σ_p consists of the maximal cubic orders over $\mathbb{Z}_p$ for all p yields Theorem 3, and also yields a corresponding interpretation of the asymptotic constants in Theorem 3 as a product of local Euler factors. Indeed, these Euler factors correspond to local weighted counts of the possible cubic algebras that can arise over $\mathbb{Q}_p$ and over $\mathbb{Q}_\infty = \mathbb{R}$. Theorem 4 is deduced by letting Σ_p consist of all maximal cubic orders over $\mathbb{Z}_p$ that are not totally ramified at p, and then applying class field theory (see Sect. 8.1 and Sect. 8.5).

Meanwhile, the case where Σ_p consists of all orders in étale cubic algebras over $\mathbb{Q}_p$ yields Theorem 6, and again also yields the analogous interpretation of the constants in Theorem 6. Theorem 7 thus simultaneously generalizes Theorems 3, 4, 5, and 6 in a natural way, and moreover, it yields a natural interpretation of the various constants $\frac{\pi^2}{72}$, $\frac{\pi^2}{24}$, $\frac{1}{12\zeta(3)}$, $\frac{1}{4\zeta(3)}$, $4/3$, 2, etc. that appear in the asymptotics of these theorems.

If we are only interested in the first main term, then we have the following stronger result:

Theorem 8 *Let $(\Sigma_p) \cup \Sigma_\infty$ be an acceptable collection of local specifications, and let Σ denote the set of all isomorphism classes of orders R in cubic fields for which $R \otimes \mathbb{Q}_p \in \Sigma_p$ for all p and $R \otimes \mathbb{R} \in \Sigma_\infty$. Let $N_3(\Sigma; X)$ denote the number of cubic orders $R \in \Sigma$ that satisfy $|\mathrm{Disc}(R)| < X$. Then*

$$N_3(\Sigma; X) = \left(\frac{1}{2}\sum_{R\in\Sigma_\infty}\frac{1}{|\mathrm{Aut}(R)|}\right) \cdot \prod_p\left(\frac{p-1}{p}\cdot\sum_{R\in\Sigma_p}\frac{1}{\mathrm{Disc}_p(R)}\cdot\frac{1}{|\mathrm{Aut}(R)|}\right)\cdot X + o(X). \quad (8)$$

The case where, for all p, the set Σ_p consists of all maximal cubic rings is Theorem 1, while the case where it consists of all maximal cubic rings that are not totally ramified at p yields Theorem 2.

Our proofs of Theorems 1–8 and particularly Theorem 7, though perhaps similar in spirit to the original arguments of Davenport and Heilbronn, involve a number of new ideas and refinements both on the algebraic and the analytic side. First, we begin in Sects. 2 and 3 by giving a much shorter and more elementary derivation of the "Davenport–Heilbronn correspondence" between maximal cubic orders and appropriate sets of binary cubic forms.

Second, we obtain the main term of the asymptotics of Theorem 5 in Sect. 5 by counting points not in a single fundamental domain, but on average in a continuum of fundamental domains, using a technique of [7]. This leads, in particular, to a uniform treatment of the cases of positive and negative discriminants. It also leads directly to stronger error terms; most notably, we obtain immediately an error term of $O(X^{5/6})$ for the number of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of integral binary cubic forms of discriminant less than X, improving on Davenport's original $O(X^{15/16})$. The $O(X^{5/6})$ term is seen to come from the "cusps" or "tentacles" of the fundamental regions.

Third, to more efficiently count points in the cusps of these fundamental regions, we introduce a "slicing and smoothing" technique in Sect. 6, which then allows us to keep track of precise second order terms and thus also prove the second main term of Theorem 5. The technique works equally well when counting points satisfying any finite set of congruence conditions (see Theorem 27).

Fourth, our use of the Delone–Faddeev correspondence (cf. Sect. 2) allows us to give an elementary treatment of the analogue of Theorem 3 for orders, rather than just fields, as in Theorem 6 and the cases of Theorem 7 where only finitely many local conditions are involved. We prove the main terms of Theorems 1–8 in Sect. 8, using a simplified computation of p-adic densities that is carried out in Sect. 4.

Finally—in order to treat the second term in cases where infinitely many local conditions are involved—we introduce a sieving method that allows one to preserve the second main terms even when certain natural infinite sets of congruence conditions are applied. This is accomplished in Sect. 9, using a computation of "second order p-adic densities" that is carried out in Sect. 7.

Remark 1 We note that an alternative proof of Theorems 3 and 4 has recently been obtained by Taniguchi and Thorne [31], using quite different methods. Although our proof here is more elementary, the work of Taniguchi–Thorne connects with the theory of Shintani zeta functions, and may thus have further interesting consequences in that realm. In fact, it seems clear that the methods here in conjunction with those of [31] should together yield even stronger results, e.g., better error terms, than either method alone! We hope to pursue this in future work.

Remark 2 Readers interested mainly in our new simpler proofs of the main terms of the Davenport–Heilbronn theorems may safely skip Sects. 6, 7 and 9, which constitute about a half of this paper. On the other hand, those interested in the new results on second main terms may wish to concentrate primarily on these sections.

2 The Delone–Faddeev correspondence

A *cubic ring* is any commutative ring with unit that is free of rank 3 as a $\mathbb{Z}$-module. We begin with a theorem of Delone–Faddeev [17] (as refined by Gan–Gross–Savin [21]) parametrizing cubic rings by $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of integral binary cubic forms.[1] Throughout this paper, we always use the "twisted" action of $\mathrm{GL}_2(\mathbb{Z})$ on binary cubic forms, i.e., an element $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ acts on a binary cubic form $f(x, y)$ by

$$(\gamma f)(x, y) = \frac{1}{\det(\gamma)} f\big((x, y)\gamma\big). \tag{9}$$

[1]We thank Franz Lemmermeyer for pointing out to us that the basic ideas of this correspondence were already essentially contained in the work of Levi [24] in 1914! See also the 1926 work of Delone [16].

Theorem 9 [17, 21] *There is a natural bijection between the set of* $\mathrm{GL}_2(\mathbb{Z})$*-equivalence classes of integral binary cubic forms and the set of isomorphism classes of cubic rings.*

Proof Given a cubic ring R, let $\langle 1, \omega, \theta\rangle$ be a $\mathbb{Z}$-basis for R. Translating ω and θ by the appropriate elements of $\mathbb{Z}$, we may assume that $\omega\theta \in \mathbb{Z}$. In the terminology of [17], a basis satisfying the latter condition is called *normal*. If $\langle 1, \omega, \theta\rangle$ is a normal basis, then there exist constants $a, b, c, d, \ell, m, n \in \mathbb{Z}$ such that

$$\begin{aligned} \omega\theta &= n \\ \omega^2 &= m - b\omega + a\theta \\ \theta^2 &= \ell - d\omega + c\theta. \end{aligned} \tag{10}$$

To the cubic ring R, we associate the binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$.

In more coordinate-free terms, the form $f(x, y)$ represents the cubic map $R/\mathbb{Z} \to \bigwedge^2(R/\mathbb{Z}) \cong \mathbb{Z}$ given by $r \mapsto r \wedge r^2$. To see this, set $r = x\omega + y\theta$; then

$$r \wedge r^2 = (x\omega + y\theta) \wedge \left[x^2(b\omega - a\theta) + y^2(d\omega - c\theta)\right] = f(x, y)(\omega \wedge \theta)$$

as elements of $\bigwedge^2(R/\mathbb{Z})$. In particular, changing the $\mathbb{Z}$-basis $\langle \omega, \theta\rangle$ of $R/\mathbb{Z}$ by an element $\gamma \in \mathrm{GL}_2(\mathbb{Z})$, and then renormalizing the basis in R, transforms the corresponding binary cubic form $f(x, y)$ by that same element of $\mathrm{GL}_2(\mathbb{Z})$.

Conversely, given a binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$, form a potential cubic ring having multiplication laws (10). The values of ℓ, m, n are subject to the associative law relations $(\omega\theta)\theta = \omega(\theta^2)$ and $(\omega^2)\theta = \omega(\omega\theta)$, which when multiplied out using (10), yield a system of equations which possesses a unique solution for n, m, ℓ, namely

$$\begin{aligned} n &= -ad \\ m &= -ac \\ \ell &= -bd. \end{aligned} \tag{11}$$

If follows that any binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$, via the recipe (10) and (11), leads to a unique cubic ring $R = R(f)$. This is the desired conclusion. □

The map $f \mapsto R(f)$ has many desirable properties. First, it is *discriminant-preserving*. More precisely, if R is a cubic ring, then we may define the *trace* $\mathrm{Tr}(\alpha) \in \mathbb{Z}$ of an element $\alpha \in R$ as the trace of the $\mathbb{Z}$-linear mapping

$\times\alpha : R \to R$. The *discriminant* $\mathrm{Disc}(R)$ of a cubic ring R is then the determinant of the bilinear pairing $\mathrm{Tr}(\alpha\beta)_{\alpha,\beta\in R}$ on R. It turns out that this discriminant coincides with the discriminant of the corresponding binary cubic form:

Proposition 10 *The discriminant of an integral binary cubic form f is equal to the discriminant of the corresponding cubic ring $R(f)$.*

Proof An explicit calculation using (10) and (11) easily verifies Proposition 10. The proposition can also be deduced more conceptually as follows. We observe that the discriminant of $R(f)$ must be an $\mathrm{SL}_2(\mathbb{Z})$-invariant polynomial in a, b, c, d of degree 4. It is well-known (see, e.g., [22]) that a binary cubic form f possesses, up to scaling, only one $\mathrm{SL}_2(\mathbb{Z})$-invariant polynomial of degree 4, namely the discriminant $\mathrm{Disc}(f)$. We conclude that $\mathrm{Disc}(R(f)) = c \cdot \mathrm{Disc}(f)$ for some constant c. To determine c, let $f(x, y) = xy(x - y)$. Then by (10), we have $R(f) \cong \mathbb{Z}^3$ (with the identification $\omega \mapsto (-1, 0, 0)$ and $\theta \mapsto (0, -1, 0)$). Since $\mathrm{Disc}(xy(x - y)) = 1$ with the usual normalization of the discriminant, and $\mathrm{Disc}(R(f)) = \mathrm{Disc}(\mathbb{Z}^3) = 1$, we conclude that $c = 1$. □

Explicitly, the discriminant of the binary cubic form f (and thus of the corresponding cubic ring $R(f)$) is given by

$$\mathrm{Disc}\big(R(f)\big) = \mathrm{Disc}(f) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd. \quad (12)$$

Next, we may determine whether $R(f)$ is an integral domain simply by checking the reducibility/irreducibility of f over $\mathbb{Q}$:

Proposition 11 *For an integral binary cubic form f, the cubic ring $R(f)$ is an integral domain if and only if f is irreducible as a polynomial over $\mathbb{Q}$.*

Proof If $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ is reducible, then it has a linear factor, which (by a change of variable in $\mathrm{GL}_2(\mathbb{Z})$) we may assume is y; i.e., $a = 0$. In this case, (10) and (11) show that $\omega\theta = 0$, so $R(f)$ has zero divisors.

Conversely, if a cubic ring R has zero divisors, then there exists some element $\omega \in R$ such that $\langle 1, \omega\rangle$ spans a quadratic subring of R. Such an ω can be constructed as follows. Let α and β be two nonzero elements of R with $\alpha\beta = 0$, and let $\alpha^3 + c_1\alpha^2 + c_2\alpha + c_3 = 0$ be the characteristic equation of the $\mathbb{Z}$-linear mapping $\times\alpha : R \to R$. Multiplying both sides by β, we see that $c_3 = 0$, so that $\alpha(\alpha^2 + c_1\alpha + c_2) = 0$. If $\alpha^2 + c_1\alpha + c_2 = 0$, then we may let $\omega = \alpha$. Otherwise, note that $(\alpha^2 + c_1\alpha + c_2)^2 = c_2(\alpha^2 + c_1\alpha + c_2)$, so in that case we may set $\omega = \alpha^2 + c_1\alpha + c_2$, and $\omega^2 = c_2\omega$. Either way, we see that $\langle 1, \omega\rangle$ spans a quadratic subring of R.

Scaling ω by an integer if necessary, we may assume that ω is a primitive vector in the lattice $R \cong \mathbb{Z}^3$, and then extend $\langle 1, \omega\rangle$ to a basis $\langle 1, \omega, \theta\rangle$ of R. Normalizing this basis if needed, we then see in (10) that we must have $a = 0$, implying that the associated binary cubic form is reducible. We conclude that, under the Delone–Faddeev correspondence, integral domains correspond to irreducible binary cubic forms. □

Other important properties of the cubic ring $R(f)$ can also be read off easily from the binary cubic form f. For example, we have

Proposition 12 *For an integral binary cubic form f, the group of ring automorphisms of $R(f)$ is naturally isomorphic to the stabilizer of f in* $\mathrm{GL}_2(\mathbb{Z})$.

Proof This follows directly from the proof of Theorem 9: any automorphism of $R(f)$ results in a $\mathrm{GL}_2(\mathbb{Z})$-transformation on the chosen normal basis ω, θ of $R/\mathbb{Z}$ (which is then automatically still normal), thus giving an element of the stabilizer of the binary cubic form f in $\mathrm{GL}_2(\mathbb{Z})$; the converse is similarly trivial. □

Finally, we note that the correspondence of Theorem 9, and the analogues of Propositions 10–12, also hold for cubic algebras and binary cubic forms over other base rings such as $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Q}_p$, $\mathbb{Z}_p$, and $\mathbb{F}_p$. Indeed, let T denote any one of these rings. Then a *cubic ring over* T can be defined analogously as any ring with unit that is free of rank 3 as a T-module. Similarly, a *binary cubic form over* T is any binary cubic form with coefficients in T. Again, $\mathrm{GL}_2(T)$ acts on the space of binary cubic forms over T via (9). With these definitions, Theorem 9 and Propositions 10–12 all hold when "$\mathrm{GL}_2(\mathbb{Z})$" is replaced by "$\mathrm{GL}_2(T)$", "integral binary cubic form" is replaced by "binary cubic form over T", and "cubic ring" is replaced by "cubic ring over T"; the proofs are identical. This observation will also be very useful to us in later sections.

3 The Davenport–Heilbronn correspondence

A cubic ring is said to be *maximal* if it is not a subring of any other cubic ring. The first part of the Davenport–Heilbronn theorem [15] describes a bijection (known as the "Davenport–Heilbronn correspondence") between maximal cubic rings and certain special classes of binary cubic forms. In this section, we give a simple derivation of this bijection.

By the work of the previous section, in order to obtain the Davenport–Heilbronn correspondence we must simply determine which binary cubic forms f yield maximal rings $R(f)$ in the bijection given by (10) and (11).

Now a cubic ring R is maximal if and only if the cubic $\mathbb{Z}_p$-algebra $R_p = R \otimes \mathbb{Z}_p$ is maximal for every p (this is because R is a maximal ring if and only if it is isomorphic to a product of rings of integers in number fields). The condition on R that $R \otimes \mathbb{Z}_p$ be a maximal cubic algebra over $\mathbb{Z}_p$ is called "maximality at p". The following lemma illustrates the ways in which a ring R can fail to be maximal at p:

Lemma 13 *Suppose R is not maximal at p. Then there is a $\mathbb{Z}$-basis $\langle 1, \omega, \theta \rangle$ of R such that at least one of the following is true*:

- $\mathbb{Z} + \mathbb{Z} \cdot (\omega/p) + \mathbb{Z} \cdot \theta$ *forms a ring*
- $\mathbb{Z} + \mathbb{Z} \cdot (\omega/p) + \mathbb{Z} \cdot (\theta/p)$ *forms a ring.*

Proof Let $R' \supset R$ be any ring strictly containing R such that the index of R in R' is a multiple of p, and let $R_1 = R' \cap (R \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{p}])$. Then the ring R_1 also strictly contains R, and the index of R in R_1 is a power of p. By the theory of elementary divisors, there exist nonnegative integers $i \geq j$ and a basis $\langle 1, \omega, \theta \rangle$ of R such that

$$R_1 = \mathbb{Z} + \mathbb{Z}\big(\omega/p^i\big) + \mathbb{Z}\big(\theta/p^j\big). \tag{13}$$

If $i = 1$, we are done. Hence we assume $i > 1$.

We normalize the basis $\langle 1, \omega, \theta \rangle$ if necessary; this does not affect the truth of (13). Now suppose the multiplicative structure of R is given by (10) and (11). That the right side of (13) is a ring translates into the following congruence conditions on a, b, c, d:[2]

$$\begin{aligned} a &\equiv 0 \pmod{p^{2i-j}}, \qquad & b &\equiv 0 \pmod{p^i}, \\ c &\equiv 0 \pmod{p^j}, \qquad & d &\equiv 0 \pmod{p^{2j-i}}. \end{aligned} \tag{14}$$

If $j = 0$, then replacing (i, j) by $(i - 1, j)$ maintains the truth of the above congruences, and R_1 as defined by (13) remains a ring. If $j > 0$, then we may replace (i, j) instead by $(i - 1, j - 1)$. Thus in a finite sequence of such moves, we arrive at $i = 1$, as desired. □

The lemma implies that a cubic ring $R(f)$ can fail to be maximal at p in two ways: either (i) f is a multiple of p, or (ii) there is some $\mathrm{GL}_2(\mathbb{Z})$-transformation of $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ such that a is a multiple of p^2 and b is a multiple of p.

Let $\mathcal{U}_p$ be the set of all binary cubic forms f not satisfying either of the latter two conditions. Then we have proven

[2] We follow here the convention that, for $e \leq 0$, we have $a \equiv 0 \pmod{p^e}$ for any integer a.

Theorem 14 (Davenport–Heilbronn [15]) *The cubic ring $R(f)$ is maximal at p if and only if $f \in \mathcal{U}_p$. The cubic ring $R(f)$ is maximal if and only if $f \in \mathcal{U}_p$ for all p.*

Note that our definition of $\mathcal{U}_p$ is somewhat simpler than that used by Davenport–Heilbronn (but is easily seen to be equivalent).

The discussion above can also be used to deduce a number of other consequences. For example, we may use it to determine the number of index p subrings of a given cubic ring $R(f)$ as well as the number of cubic rings containing a given cubic ring $R(f)$ with index p:

Proposition 15 *For an integral binary cubic form f, the number of index p subrings of $R(f)$ is equal to $\omega_p(f)$, the number of zeroes in $\mathbb{P}^1(\mathbb{F}_p)$ of f modulo p.*

Proposition 16 *For an integral binary cubic form f, the number of cubic rings in $R(f) \otimes \mathbb{Q}$ containing $R(f)$ with index p is equal to the number of double zeroes $\alpha \in \mathbb{P}^1(\mathbb{F}_p)$ of f modulo p such that $f(\alpha') \equiv 0 \pmod{p^2}$ for all $\alpha' \equiv \alpha \bmod p$.*

Proof If $R \subset R'$ with $[R' : R] = p$, then we may write $R = \mathbb{Z} + pR' + \mathbb{Z}\theta$, where θ is a well-defined element of $(R'/\mathbb{Z})/p(R'/\mathbb{Z})$. Extending θ to a $\mathbb{Z}$-basis $1, \omega, \theta$ of R', and renormalizing if necessary, we see that $1, \omega, \theta$ is a $\mathbb{Z}$-basis for R' and $1, p\omega, \theta$ is a $\mathbb{Z}$-basis for R. Regardless of these choices, note that θ is well-defined in $(R'/\mathbb{Z})/p(R'/\mathbb{Z})$, while $p\omega$ is well-defined in $(R/\mathbb{Z})/p(R/\mathbb{Z})$.

Now if $f'(x, y) = a'x^3 + b'x^2y + c'xy^2 + d'y^3$ is the binary cubic form corresponding to the normal basis $1, \omega, \theta$ of the ring R', then by (10) we see that $R = \mathbb{Z} + pR' + \mathbb{Z}\theta$ is also a ring if and only if $d' \equiv 0 \pmod{p}$, i.e., the image of θ in $R'/\mathbb{Z}$ is a root of $f' \pmod{p}$, when f' is viewed as a cubic map $R'/\mathbb{Z} \to \bigwedge^2(R'/\mathbb{Z}) \cong \mathbb{Z}$ given by $r \mapsto r \wedge r^2$. In that case, $f(x, y) = a'p^2x^3 + b'px^2y + c'xy^2 + (d'/p)y^3$ is the binary cubic form corresponding to the basis $1, p\omega, \theta$ of R, and this gives the desired bijection between roots of $f' \pmod{p}$ and subrings of R' of index p, as stated in Proposition 15.

Similarly, if $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ is the binary cubic form corresponding to the normal basis $1, p\omega, \theta$ of the ring R, then by (10) we see that the $\mathbb{Z}$-module R' spanned by $1, \omega, \theta$ is also a ring if and only if $a \equiv 0 \pmod{p^2}$ and $b \equiv 0 \pmod{p}$, i.e., the image of $p\omega$ in $R/\mathbb{Z}$ is a double root of $f \pmod{p}$ and f takes a value at $p\omega$ that is a multiple of p^2, when f is viewed as a cubic map $R/\mathbb{Z} \to \bigwedge^2(R/\mathbb{Z}) \cong \mathbb{Z}$ given by $r \mapsto r \wedge r^2$. In that case, $f'(x, y) = (a/p^2)x^3 + (b/p)x^2y + cxy^2 + dpy^3$ is the binary cubic form corresponding to the basis $1, \omega, \theta$ of R', and this gives the desired bijection between roots α of f (mod p) such that $f(\alpha) \equiv 0 \pmod{p^2}$, and rings R' containing R with index p, as stated in Proposition 16. □

4 Local behavior and p-adic densities

In this section, we consider elements f in the spaces of binary cubic forms over the integers $\mathbb{Z}$, the p-adic ring $\mathbb{Z}_p$, and the residue field $\mathbb{Z}/p\mathbb{Z}$. We denote these spaces by $V_{\mathbb{Z}}$, $V_{\mathbb{Z}_p}$, and $V_{\mathbb{F}_p}$ respectively. The results in this section are also contained in [15]; however, we give here slightly simpler and more direct proofs.

Aside from the degenerate case $f \equiv 0 \pmod{p}$, any form $f \in V_{\mathbb{Z}}$ (resp. $V_{\mathbb{Z}_p}$, $V_{\mathbb{F}_p}$) determines exactly three points in $\mathbb{P}^1_{\bar{\mathbb{F}}_p}$, obtained by taking the roots of f reduced modulo p. For such a form f, define the symbol (f, p) by setting

$$(f, p) = \left(f_1^{e_1} f_2^{e_2} \cdots\right),$$

where the f_i's indicate the degrees of the fields of definition over $\mathbb{F}_p$ of the roots of f, and the e_i's indicate the respective multiplicities of these roots. There are thus five possible values of the symbol (f, p), namely, (111), (12), (3), (1^21), and (1^3). Furthermore, it is clear that if two binary cubic forms f_1, f_2 over $\mathbb{Z}$ (resp. $\mathbb{Z}_p$, $\mathbb{F}_p$) are equivalent under a transformation in $\mathrm{GL}_2(\mathbb{Z})$ (resp. $\mathrm{GL}_2(\mathbb{Z}_p)$, $\mathrm{GL}_2(\mathbb{F}_p)$), then $(f_1, p) = (f_2, p)$. By $T_p(111)$, $T_p(12)$, etc., let us denote the set of f such that $(f, p) = (111)$, $(f, p) = (12)$, etc.

By the definition of $R(f)$, the ring structure of the quotient ring $R(f)/(p)$ depends only on the $\mathrm{GL}_2(\mathbb{F}_p)$-orbit of f modulo p; hence the symbol (f, p) indicates something about the structure of the ring $R(f)$ when reduced modulo p. In fact, writing down the multiplication laws at one point of each of the five aforementioned $\mathrm{GL}_2(\mathbb{F}_p)$-orbits demonstrates that

$$\begin{aligned} &(f, p) = \left(f_1^{e_1} f_2^{e_2} \cdots\right) \\ &\iff \quad R(f)/(p) \cong \mathbb{F}_{p^{f_1}}[t_1]/\left(t_1^{e_1}\right) \oplus \mathbb{F}_{p^{f_2}}[t_2]/\left(t_2^{e_2}\right) \oplus \cdots . \end{aligned}$$

In particular, it follows that for $f \in \mathcal{U}_p$, the symbol (f, p) conveys precisely the splitting behavior of $R(f)$ at p. For example, if $(f, p) = (1^3)$ for $f \in \mathcal{U}_p$, then this means the maximal cubic ring $R(f)$ is totally ramified at p.

Now, for any set S in $V_{\mathbb{Z}}$ (resp. $V_{\mathbb{Z}_p}$, $V_{\mathbb{F}_p}$) that is definable by congruence conditions, let us denote by $\mu(S) = \mu_p(S)$ the p-adic density of the p-adic closure of S in $V_{\mathbb{Z}_p}$, where we normalize the additive measure μ on $V_{\mathbb{Z}_p} = \mathbb{Z}_p^4$ so that $\mu(V_{\mathbb{Z}_p}) = 1$ (i.e., we have taken the product of the usual additive measures on $\mathbb{Z}_p$). The following lemma determines the p-adic densities of the sets $T_p(\cdot)$.

Lemma 17 *We have*

$$\mu\big(T_p(111)\big) = \frac{1}{6}(p-1)^2 p(p+1)/p^4$$
$$\mu\big(T_p(12)\big) = \frac{1}{2}(p-1)^2 p(p+1)/p^4$$
$$\mu\big(T_p(3)\big) = \frac{1}{3}(p-1)^2 p(p+1)/p^4$$
$$\mu\big(T_p(1^2 1)\big) = (p-1)p(p+1)/p^4$$
$$\mu\big(T_p(1^3)\big) = (p-1)(p+1)/p^4.$$

Proof Since the criteria for membership of f in a $T_p(\cdot)$ depend only on the residue class of f modulo p, it suffices to consider the situation over $\mathbb{F}_p$. We examine first $\mu(T_p(111))$. The number of unordered triples of distinct points in $\mathbb{P}^1_{\mathbb{F}_p}$ is $\frac{1}{6}(p+1)p(p-1)$. Furthermore, given such a triple of points, there is a unique binary cubic form, up to scaling, having this triple of points as its roots. Since the total number of binary cubic forms over $\mathbb{F}_p$ is p^4, it follows that $\mu(T_p(111)) = \frac{1}{6}[(p+1)p(p-1)](p-1)/p^4$, as given by the lemma.

Similarly, the number of unordered triples of points, one member of which is in $\mathbb{P}^1_{\mathbb{F}_p}$ while the other two are $\mathbb{F}_p$-conjugate in $\mathbb{P}^1_{\mathbb{F}_{p^2}}$, is given by $\frac{1}{2}(p+1)(p^2-p)$. We thus have $\mu(T_p(12)) = \frac{1}{2}[(p+1)(p^2-p)](p-1)/p^4$. Also, the number of unordered $\mathbb{F}_p$-conjugate triples of distinct points in $\mathbb{P}^1_{\mathbb{F}_{p^3}}$ is $(p^3-p)/3$, and hence $\mu(T_p(3)) = \frac{1}{3}[(p^3-p)](p-1)/p^4$.

Meanwhile, the number of pairs (x, y) of distinct points in $\mathbb{P}^1_{\mathbb{F}_p}$ is given by $(p+1)p$, so that the number of binary cubic forms over $\mathbb{F}_p$ having a double root at some point x and a single root at another point y is $[(p+1)p](p-1)$. Thus $\mu(T_p(1^2 1)) = [(p+1)p](p-1)]/p^4$. Finally, the number of binary cubic forms over $\mathbb{F}_p$ having a triple root in $\mathbb{P}^1_{\mathbb{F}_p}$ is $(p+1)(p-1)$, yielding $\mu(T_p(1^3)) = (p+1)(p-1)/p^4$ as desired. □

We next wish to determine the p-adic densities of the sets $\mathcal{U}_p$. Let $\mathcal{U}_p(\cdot)$ denote the subset of elements $f \in T_p(\cdot)$ such that $R(f)$ is maximal at p. If f is an element of $T_p(111)$, $T_p(12)$, or $T_p(3)$, then $R(f)$ is clearly maximal at p, as its discriminant is coprime to p. Thus $\mathcal{U}_p(111) = T_p(111)$, $\mathcal{U}_p(12) = T_p(12)$, and $\mathcal{U}_p(3) = T_p(3)$. If a binary cubic form f is in $T_p(1^2 1)$ or $T_p(1^3)$, then it can clearly be brought into the form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ with $a \equiv b \equiv 0 \pmod p$, namely, by sending the unique multiple root of f in $\mathbb{P}^1_{\mathbb{F}_p}$ to the point $(1, 0)$ via a transformation in $\mathrm{GL}_2(\mathbb{Z})$. Of all $f \in T_p(1^2 1)$ or $T_p(1^3)$ that have been rendered in such a form, a proportion of

$1/p$ actually satisfy the congruence $a \equiv 0 \pmod{p^2}$ of condition (ii). Thus a proportion of $(p-1)/p$ of forms in $T_p(1^21)$ and in $T_p(1^3)$ correspond to cubic rings maximal at p. We have proven:

Lemma 18 *We have*

$$\begin{aligned}
\mu\big(\mathcal{U}_p(111)\big) &= \frac{1}{6}(p-1)^2 p(p+1)/p^4\\
\mu\big(\mathcal{U}_p(12)\big) &= \frac{1}{2}(p-1)^2 p(p+1)/p^4\\
\mu\big(\mathcal{U}_p(3)\big) &= \frac{1}{3}(p-1)^2 p(p+1)/p^4\\
\mu\big(\mathcal{U}_p\big(1^21\big)\big) &= (p-1)^2(p+1)/p^4\\
\mu\big(\mathcal{U}_p\big(1^3\big)\big) &= (p-1)^2(p+1)/p^5.
\end{aligned}$$

Following [15] let $\mathcal{V}_p$ denote the set of elements $f \in \mathcal{U}_p$ such that $(f,p) \neq (1^3)$. Then it is clear from the above arguments that the elements of $\mathcal{V}_p$ correspond to orders in étale cubic algebras over $\mathbb{Q}$ that are maximal at p and in which p does not totally ramify. The set $\mathcal{V}_p$ plays an important role in understanding the 3-torsion in the class groups of cubic fields (see Sect. 8).

Using the fact that $\mathcal{U}_p$ is simply the union of the $\mathcal{U}_p(\sigma)$'s, while $\mathcal{V}_p$ is the union of the $\mathcal{U}_p(\sigma)$'s where $\sigma \neq (1^3)$, we obtain from Lemma 18:

Lemma 19 *We have*

$$\begin{aligned}
\mu(\mathcal{U}_p) &= \big(p^3-1\big)\big(p^2-1\big)/p^5\\
\mu(\mathcal{V}_p) &= \big(p^2-1\big)^2/p^4.
\end{aligned}$$

5 The number of binary cubic forms of bounded discriminant

Let $V_{\mathbb{R}}$ denote the vector space of binary cubic forms over $\mathbb{R}$. Then the action of $\mathrm{GL}_2(\mathbb{R})$ on $V_{\mathbb{R}}$ has two nondegenerate orbits, namely the orbit $V_{\mathbb{R}}^{(0)}$ consisting of elements having positive discriminant, and $V_{\mathbb{R}}^{(1)}$ consisting of those having negative discriminant. In this section we wish to understand the number $N(V_{\mathbb{Z}}^{(i)};X)$ of *irreducible* $\mathrm{GL}_2(\mathbb{Z})$-orbits on $V_{\mathbb{Z}}^{(i)} := V_{\mathbb{Z}} \cap V_{\mathbb{R}}^{(i)}$ having absolute discriminant less than X ($i=0,1$), where we say that a $\mathrm{GL}_2(\mathbb{Z})$-orbit on $V_{\mathbb{Z}}$ is *irreducible* if it consists of binary cubic forms that are irreducible over $\mathbb{Q}$. In particular, we prove the following strengthening of Davenport's theorem on the number of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of irreducible binary cubic forms having bounded discriminant:

Theorem 20 *We have*

$$N\big(V_{\mathbb{Z}}^{(0)};X\big)=\frac{\pi^2}{72}\cdot X+O\big(X^{5/6}\big);$$
$$N\big(V_{\mathbb{Z}}^{(1)};X\big)=\frac{\pi^2}{24}\cdot X+O\big(X^{5/6}\big).$$

In [13] and [14], Davenport had obtained the main terms of the above theorem with an error bound of $O(X^{15/16})$.

5.1 Reduction theory

Define the usual subgroups K_1, A_+, N, and Λ of $\mathrm{GL}_2(\mathbb{R})$ as follows:

$$K_1=\{\text{orthogonal transformations in } \mathrm{GL}_2(\mathbb{R})\};$$
$$A_+=\{a(t):t\in\mathbb{R}_+\},\quad \text{where } a(t)=\begin{pmatrix}t^{-1}&\\&t\end{pmatrix};$$
$$N=\big\{n(u):u\in\mathbb{R}\big\},\quad \text{where } n(u)=\begin{pmatrix}1&\\u&1\end{pmatrix};$$
$$\Lambda=\left\{\begin{pmatrix}\lambda&\\&\lambda\end{pmatrix}\right\}\quad \text{where } \lambda>0.$$

It is well-known (see [23, Theorem 6.46]) that the natural product map $K_1\times A_+\times N\to \mathrm{GL}_2(\mathbb{R})$ is an analytic diffeomorphism. In fact, for any $g\in\mathrm{GL}_2(\mathbb{R})$, there exist unique $k\in K_1$, $a=a(t)\in A_+$, $n=n(u)\in N$, and $\lambda\in\Lambda$ such that $g=k\,a\,n\,\lambda$; this is the Iwasawa decomposition of $\mathrm{GL}_2(\mathbb{R})$.

Let $\mathcal{F}$ denote Gauss's usual fundamental domain for $\mathrm{GL}_2(\mathbb{Z})\backslash\mathrm{GL}_2(\mathbb{R})$ in $\mathrm{GL}_2(\mathbb{R})$. Then $\mathcal{F}$ may be expressed in the form $\mathcal{F}=\{nak\lambda:n\in N'(a),\ a\in A',k\in K,\lambda\in\Lambda\}$, where

$$N'(a)=\left\{\begin{pmatrix}1&\\n&1\end{pmatrix}:n\in\nu(a)\right\},$$
$$A'=\left\{\begin{pmatrix}t^{-1}&\\&t\end{pmatrix}:t\geq\sqrt[4]{3}/\sqrt{2}\right\},\tag{15}$$
$$\Lambda=\left\{\begin{pmatrix}\lambda&\\&\lambda\end{pmatrix}:\lambda>0\right\},$$

and K is as usual the (compact) real special orthogonal group $\mathrm{SO}_2(\mathbb{R})$; here $\nu(a)$ is the union of either one or two subintervals of $[-\frac{1}{2},\frac{1}{2}]$ depending only on the value of $a\in A'$. Furthermore, if a is such that $t\geq1$, then $\nu(a)=[-\frac{1}{2},\frac{1}{2}]$. (See, e.g., [28, Ch. 7, Th. 1].)

For $i \in \{0, 1\}$, let n_i denote the cardinality of the stabilizer in $\mathrm{GL}_2(\mathbb{R})$ of any element $v \in V_{\mathbb{R}}^{(i)}$ (by the correspondence of Theorems 9 and 12 over $\mathbb{R}$, we have $n_1 = \mathrm{Aut}_{\mathbb{R}}(\mathbb{R}^3) = 6$ and $n_2 = \mathrm{Aut}_{\mathbb{R}}(\mathbb{R} \oplus \mathbb{C}) = 2$). Then for any $v \in V_{\mathbb{R}}^{(i)}$, $\mathcal{F}v$ will be the union of n_i fundamental domains for the action of $\mathrm{GL}_2(\mathbb{Z})$ on $V_{\mathbb{R}}^{(i)}$. Since this union is not necessarily disjoint, $\mathcal{F}v$ is best viewed as a multiset, where the multiplicity of a point x in $\mathcal{F}v$ is given by the cardinality of the set $\{g \in \mathcal{F} \mid gv = x\}$. Evidently, this multiplicity is a number between 1 and n_i.

Even though the multiset $\mathcal{F}v$ is the union of n_i fundamental domains for the action of $\mathrm{GL}_2(\mathbb{Z})$ on $V_{\mathbb{R}}^{(i)}$, not all elements in $\mathrm{GL}_2(\mathbb{Z})\backslash V_{\mathbb{Z}}$ will be represented in $\mathcal{F}v$ exactly n_i times. In general, the number of times the $\mathrm{GL}_2(\mathbb{Z})$-equivalence class of an element $x \in V_{\mathbb{Z}}$ will occur in the multiset $\mathcal{F}v$ is given by $n_i/m(x)$, where $m(x)$ denotes the size of the stabilizer of x in $\mathrm{GL}_2(\mathbb{Z})$. Now the stabilizer in $\mathrm{GL}_2(\mathbb{Z})$ of an irreducible element $x \in V_{\mathbb{Z}}$ is the group of ring automorphisms of the order corresponding to x under the Delone–Faddeev correspondence (see Sect. 2), and is thus either trivial or C_3. We conclude that, for any $v \in V_{\mathbb{R}}^{(i)}$, the product $n_i \cdot N(V_{\mathbb{Z}}^{(i)}; X)$ is exactly equal to the number of irreducible integer points in $\mathcal{F}v$ having absolute discriminant less than X, with the slight caveat that the (relatively rare—see Lemma 22) C_3-points are to be counted with weight $1/3$

Now the number of such integer points can be difficult to count in a single such fundamental domain. The main technical obstacle is that the fundamental region $\mathcal{F}v$ is not bounded, but rather has a cusp going off to infinity which in fact contains infinitely many integer points, including many irreducible points. We simplify the counting of such points by “thickening” the cusp; more precisely, we compute the number of points in the fundamental region $\mathcal{F}v$ by averaging over lots of such fundamental domains, i.e., by averaging over points v lying in a certain compact subset B of $V_{\mathbb{R}}$.

5.2 Estimates on reducibility

We first consider the reducible elements in the multiset

$$\mathcal{R}_X(v) := \left\{ w \in \mathcal{F}v : |\mathrm{Disc}(w)| < X \right\},$$

where v is any vector in a fixed compact subset B of $V_{\mathbb{R}}$. Note that if a binary cubic form $ax^3 + bx^2y + cxy^2 + dy^3$ satisfies $a = 0$, then it is reducible over $\mathbb{Q}$, since y is a factor. The following lemma, proved in [13, Lem. 3] and [14, Lem. 2], shows that for binary cubic forms in $\mathcal{R}_X(v)$, reducibility with $a \neq 0$ does not occur very often.

Lemma 21 *Let $v \in B$ be any point of nonzero discriminant, where B is any fixed compact subset of $V_{\mathbb{R}}$ containing only elements having discriminant* *greater than* 1. *Then the number of integral binary cubic forms* $ax^3+bx^2y+cxy^2+dy^3 \in \mathcal{R}_X(v)$ *that are reducible with* $a \neq 0$ *is* $O(X^{3/4+\epsilon})$, *where the implied constant depends only on* B.

Proof For an element $f(x,y)=ax^3+bx^2y+cxy^2+dy^3 \in \mathcal{R}_X(v)$, we have $f \in N'A'K\Lambda v$ where $0<\lambda<X^{1/4}$, since $\mathrm{Disc}(\lambda\cdot v)=\lambda^4\mathrm{Disc}(v)$. It follows that $a=O(\lambda/t^3)=O(X^{1/4})$, $ab=O(\lambda^2/t^4)=O(X^{1/2})$, $ac=O(\lambda^2/t^2)=O(X^{1/2})$, $ad=O(\lambda^2)=O(X^{1/2})$, $abc=O(\lambda^3/t^3)=O(X^{3/4})$, and $abd=O(\lambda^3/t)=O(X^{3/4})$. In particular, the latter estimates clearly imply that the total number of forms $f \in \mathcal{R}_X(v)$ with $a\neq 0$ and $d=0$ is $O(X^{3/4+\epsilon})$.

Let us now assume $a\neq 0$ and $d\neq 0$. Then the above estimates show that the total number of possibilities for the triple (a,b,d) is $O(X^{3/4+\epsilon})$. Suppose the values a,b,d $(d\neq 0)$ are now fixed, and consider the possible number of values of c such that the resulting form $f(x,y)$ is reducible. For $f(x,y)$ to be reducible, it must have some linear factor $rx+sy$, where $r,s\in\mathbb{Z}$ are relatively prime. Then r must be a factor of a, while s must be a factor of d; they are thus both determined up to $O(X^\epsilon)$ possibilities. Once r and s are determined, computing $f(-s,r)$ and setting it equal to zero then uniquely determines c (if it is an integer at all) in terms of a,b,d,r,s. Thus the total number of reducible forms $f\in\mathcal{R}_X(v)$ with $a\neq 0$ is $O(X^{3/4+\epsilon})$, as desired. □

We shall need the following lemma, which also follows from [13, Lemma 2], bounding the number of integral points in $\mathcal{R}_X(v)$ that have stabilizer C_3 in $\mathrm{GL}_2(\mathbb{Z})$, when v has positive discriminant. No integral binary cubic form having negative discriminant has stabilizer C_3 in $\mathrm{GL}_2(\mathbb{Z})$.

Lemma 22 *Let* $v\in V_\mathbb{R}$ *be any point of positive discriminant. Then the number of points in* $V_\mathbb{Z}\cap\mathcal{R}_X(v)$ *having stabilizer* C_3 *in* $\mathrm{GL}_2(\mathbb{Z})$ *is* $O(X^{3/4+\epsilon})$, *where the implied constant is independent of* v.

Proof The number of integral points in $\mathcal{R}_X(v)$ having stabilizer C_3 in $\mathrm{GL}_2(\mathbb{Z})$ is equal to the number of isomorphism classes of cubic rings having automorphism group C_3 and discriminant less than X. This number is thus independent of v, and so it suffices to prove the lemma for any single v.

We choose v to be the binary cubic form x^3-3xy^2. The reason for this choice is as follows. Every binary cubic form $f(x,y)=ax^3+bx^2y+cxy^2+dy^3$ has a naturally associated binary quadratic form, namely, the "Hessian covariant" $H_f(x,y)=(b^2-3ac)x^2+(bc-9ad)xy+(c^2-3bd)y^2$. It is easy to see that if a binary cubic form f is acted upon by an element $\gamma\in\mathrm{SL}_2(\mathbb{Z})$, then H_f is also acted upon by the same transformation. Now $H_v(x,y)=9(x^2+y^2)$, and so $\mathcal{F}H_v$ consists of the usual reduced (positive-definite) binary quadratic forms $A_1x^2+A_2xy+A_3y^2$, where $|A_2|\le A_1\le A_3$. Thus $\mathcal{F}v$ consists of binary cubic forms satisfying $|bc-9ad|\le b^2-3ac\le c^2-3bd$.

Now if a binary cubic form f in $\mathcal{F}v$ has a nontrivial stabilizing element γ of order 3 in $\mathrm{SL}_2(\mathbb{Z})$, then γ will also stabilize its Hessian H_f. But the only reduced binary quadratic form, up to multiplication by scalars, having a nontrivial stabilizing element of order 3 is x^2+xy+y^2. Therefore, any such C_3-type binary cubic form $f(x,y)=ax^3+bx^2y+cxy^2+dy^3$ in $\mathcal{F}v$ must satisfy

$$b^2-3ac=bc-9ad=c^2-3bd.$$

From this we see that, if a,b,d are fixed, then there is at most one solution for c. As in the proof of Lemma 21, the total number of possibilities for the triple (a,b,d) in $\mathcal{F}v$ is $O(X^{3/4+\epsilon})$, and the lemma follows. □

In fact, by refining the proof of Lemma 22, it can be shown that the number of C_3-points in $\mathcal{R}_X(v)$ of discriminant less than X is asymptotic to $cX^{1/2}$, where $c=\pi\sqrt{3}/18$; see [8].

Thus, as far as Theorem 20 is concerned, the C_3-points in $V_\mathbb{Z}$ are negligible in number and are absorbed in the error term.

5.3 Averaging

Let dv denote the usual Euclidean measure on $V_\mathbb{R}$ (normalized so that $V_\mathbb{Z}$ has co-volume 1) and let $dg=t^{-2}dn\,d^\times t\,dk\,d^\times\lambda$ be the Haar measure of $\mathrm{GL}_2(\mathbb{R})$ obtained from its Iwasawa decomposition (see the beginning of Sect. 5.1), where dk is normalized to have measure 1 on $\mathrm{SO}_2(\mathbb{R})$. We start with a proposition implying that $|\mathrm{Disc}(v)|^{-1}dv$ is a $\mathrm{GL}_2(\mathbb{R})$-invariant measure on $V_\mathbb{R}$.

Proposition 23 *For $i=0$ or 1, let $f\in C_0(V_\mathbb{R}^{(i)})$ and let v_i be any element of $V_\mathbb{R}^{(i)}$. Then*

$$\int_{g\in\mathrm{GL}_2(\mathbb{R})} f(g\cdot v_i)\,dg=\frac{1}{2\pi}\int_{v\in\mathrm{GL}_2(\mathbb{R})\cdot v_i} f(v)\bigl|\mathrm{Disc}(v)\bigr|^{-1}dv$$
$$=\frac{n_i}{2\pi}\int_{v\in V_\mathbb{R}^{(i)}} f(v)\bigl|\mathrm{Disc}(v)\bigr|^{-1}dv.$$

The first equality in Proposition 23 is simply a Jacobian calculation for the change of variable for the map which sends $g\in\mathrm{GL}_2(\mathbb{R})$ to $v=g\cdot v_i$ in $V_\mathbb{R}$, where the coordinates for g are (k,t,n,λ), while for v they are the usual Euclidean coordinates (a,b,c,d) with $dv=da\,db\,dc\,dd$. The second follows from the fact that the multiset $\mathrm{GL}_2(\mathbb{R})\cdot v_i$ is an n_i-fold cover of the set $V_\mathbb{R}^{(i)}$.

For a constant $C\geq 1$, let $B=B(C)=\{w=(a,b,c,d)\in V_\mathbb{R}:3a^2+b^2+c^2+3d^2\leq C,\ |\mathrm{Disc}(w)|\geq 1\}$; then one easily checks that B is K-invariant.

Let $V_{\mathbb{Z}}^{\mathrm{irr}}$ denote the subset of irreducible points of $V_{\mathbb{Z}}$. It then follows from the discussion in Sect. 5.1 that

$$N\big(V_{\mathbb{Z}}^{(i)};X\big)=\frac{\int_{v\in B\cap V_{\mathbb{R}}^{(i)}}\#\{x\in\mathcal{F}v\cap V_{\mathbb{Z}}^{\mathrm{irr}}:|\mathrm{Disc}(x)|<X\}|\mathrm{Disc}(v)|^{-1}dv}{n_i\cdot\int_{v\in B\cap V_{\mathbb{R}}^{(i)}}|\mathrm{Disc}(v)|^{-1}dv},\tag{16}$$

where points $x\in\mathcal{F}v\cap V_{\mathbb{Z}}^{\mathrm{irr}}$ whose stabilizer in $\mathrm{GL}_2(\mathbb{Z})$ is C_3 are counted with multiplicity $1/3$. The denominator of the latter expression is, by construction, a finite absolute constant greater than zero. We have chosen the measure $|\mathrm{Disc}(v)|^{-1}\,dv$ because it is a $\mathrm{GL}_2(\mathbb{R})$-invariant measure.

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

$$N(S;X)=\frac{\int_{v\in B\cap V_{\mathbb{R}}^{(i)}}\#\{x\in\mathcal{F}v\cap S^{\mathrm{irr}}:|\mathrm{Disc}(x)|<X\}|\mathrm{Disc}(v)|^{-1}dv}{n_i\cdot\int_{v\in B\cap V_{\mathbb{R}}^{(i)}}|\mathrm{Disc}(v)|^{-1}dv},\tag{17}$$

where, as before, points $x\in\mathcal{F}v\cap S^{\mathrm{irr}}$ whose stabilizer in $\mathrm{GL}_2(\mathbb{Z})$ is C_3 are counted with multiplicity $1/3$. We shall use this as a definition of $N(S;X)$ for any $S\subset V_{\mathbb{Z}}$, even if S is not $\mathrm{GL}_2(\mathbb{Z})$-invariant. Note that for disjoint $S_1,S_2\subset V_{\mathbb{Z}}$, we have $N(S_1\cup S_2;X)=N(S_1;X)+N(S_2;X)$.

Fix $v_i\in V_{\mathbb{R}}^{(i)}$ and maximal subsets $H^{(i)}\subset\mathrm{GL}_2(\mathbb{R})$ such that $H^{(i)}\cdot v_i=B\cap V_{\mathbb{R}}^{(i)}$. Thus, the multiset $H^{(i)}\cdot v_i$ is an n_i-fold cover of $B\cap V_{\mathbb{R}}^{(i)}$. The numerator of the right hand side of (17) is equal to

$$\begin{aligned}&\sum_{\substack{x\in S^{\mathrm{irr}}\\|\mathrm{Disc}(x)|<X}}\int_{v\in B\cap V_{\mathbb{R}}^{(i)}}\#\{g\in\mathcal{F}:x=gv\}|\mathrm{Disc}(v)|^{-1}dv\\&\quad=\frac{2\pi}{n_i}\sum_{\substack{x\in S^{\mathrm{irr}}\\|\mathrm{Disc}(x)|<X}}\int_{h\in H^{(i)}}\#\{g\in\mathcal{F}:x=ghv_i\}dh,\end{aligned}\tag{18}$$

where the equality in (18) follows from Proposition 23. The right hand side of (18) is equal to

$$\begin{aligned}&\frac{2\pi}{n_i}\sum_{\substack{x\in S^{\mathrm{irr}}\\|\mathrm{Disc}(x)|<X}}\int_{g\in\mathcal{F}}\#\{h\in H^{(i)}:x=ghv_i\}dg\\&\quad=\frac{2\pi}{n_i}\int_{g\in\mathcal{F}}\#\{x\in S^{\mathrm{irr}}\cap gH^{(i)}v_i:|\mathrm{Disc}(x)|<X\}\,dg.\end{aligned}\tag{19}$$

Therefore, we have

$$\begin{aligned} N(S;X) &= \frac{1}{M_i}\int_{g\in\mathcal{F}} \#\big\{x\in S^{\mathrm{irr}}\cap gB\cap V_{\mathbb{R}}^{(i)} : |\mathrm{Disc}(x)|<X\big\}\,dg \qquad (20)\\ &= \frac{1}{M_i}\int_{g\in N'(a)A'\Lambda K} \#\big\{x\in S^{\mathrm{irr}}\cap n\big(\begin{smallmatrix} t^{-1} & \\ & t\end{smallmatrix}\big)\lambda k B\cap V_{\mathbb{R}}^{(i)} : |\mathrm{Disc}(x)|<X\big\}\\ &\qquad\times t^{-2}dn\,d^{\times}t\,d^{\times}\lambda\,dk. \qquad (21)\end{aligned}$$

where

$$M_i = \frac{n_i}{2\pi}\cdot\int_{v\in B\cap V_{\mathbb{R}}^{(i)}} |\mathrm{Disc}(v)|^{-1}dv. \qquad (22)$$

Let us write $B(n,t,\lambda,X) = n\big(\begin{smallmatrix} t^{-1} & \\ & t\end{smallmatrix}\big)\lambda B\cap\{v\in V_{\mathbb{R}}^{(i)} : |\mathrm{Disc}(v)|<X\}$. As $KB=B$ and $\int_K dk = 1$, we have

$$N(S;X) = \frac{1}{M_i}\int_{g\in N'(a)A'\Lambda} \#\big\{x\in S^{\mathrm{irr}}\cap B(n,t,\lambda,X)\big\}t^{-2}dn\,d^{\times}t\,d^{\times}\lambda. \quad (23)$$

To estimate the number of lattice points in $B(n,t,\lambda,X)$, we have the following elementary proposition from the geometry-of-numbers. The form we state is essentially due to Davenport [12]. To state the proposition, we require the following simple definitions. A multiset $\mathcal{R}\subset\mathbb{R}^n$ is said to be *measurable* if $\mathcal{R}_k$ is measurable for all k, where $\mathcal{R}_k$ denotes the set of those points in $\mathcal{R}$ having a fixed multiplicity k. Given a measurable multiset $\mathcal{R}\subset\mathbb{R}^n$, we define its volume in the natural way, that is, $\mathrm{Vol}(\mathcal{R}) = \sum_k k\cdot\mathrm{Vol}(\mathcal{R}_k)$, where $\mathrm{Vol}(\mathcal{R}_k)$ denotes the usual Euclidean volume of $\mathcal{R}_k$.

Proposition 24 *Let $\mathcal{R}$ be a bounded, semi-algebraic multiset in $\mathbb{R}^n$ having maximum multiplicity m, and which is defined by at most k polynomial inequalities each having degree at most ℓ. Let $\mathcal{R}'$ denote the image of $\mathcal{R}$ under any (upper or lower) triangular, unipotent transformation of $\mathbb{R}^n$. Then the number of integer lattice points (counted with multiplicity) contained in the region $\mathcal{R}'$ is*

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

where $\mathrm{Vol}(\bar{\mathcal{R}})$ 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.

Although Davenport states the above lemma only for compact semi-algebraic sets $\mathcal{R} \subset \mathbb{R}^n$, his proof adapts without essential change to the more general case of a bounded semi-algebraic multiset $\mathcal{R} \subset \mathbb{R}^n$, with the same estimate applying also to any image $\mathcal{R}'$ of $\mathcal{R}$ under a unipotent triangular transformation.

We now have the following lemma on the number of lattice points in $B(n, t, \lambda, X)$ with $a \neq 0$:

Lemma 25 *The number of lattice points* (a, b, c, d) *in* $B(n, t, \lambda, X)$ *with* $a \neq 0$ *is*

$$\begin{cases} 0 & \text{if } \frac{C\lambda}{t^3} < 1; \\ \mathrm{Vol}(B(n,t,\lambda,X)) + O(\max\{C^3 t^3 \lambda^3, 1\}) & \text{otherwise.} \end{cases}$$

Proof From our description of B, it follows that the x^3-coefficient of any binary cubic form in B is bounded by C. Thus, if $C\lambda/t^3 < 1$, then $a = 0$ is the only possibility for an integral binary cubic form $ax^3 + bx^2y + cy^2 + dy^3$ in $B(n, t, \lambda, X)$. If $C\lambda/t^3 \geq 1$, then λ and t are positive numbers bounded from below by $(\sqrt[4]{3}/\sqrt{2})^3/C$ and $\sqrt[4]{3}/\sqrt{2}$ respectively. In this case, one sees that the projection of $B(n, t, \lambda, X)$ onto $a = 0$ has volume $O(C^3 t^3 \lambda^3)$, while all other projections are also bounded by a constant times this. The lemma now follows from Proposition 24. □

In (23), observe that the integrand will be nonzero only if $t^3 \leq C\lambda$ and $\lambda \leq X^{1/4}$, since B consists only of points having discriminant at least 1. Thus we may write, up to an error of $O(X^{3/4+\epsilon})$ due to Lemma 21, that

$$N\big(V_{\mathbb{R}}^{(i)}; X\big) = \frac{1}{M_i} \int_{\lambda=(\sqrt[4]{3}/\sqrt{2})^3/C}^{X^{1/4}} \int_{t=\sqrt[4]{3}/\sqrt{2}}^{C^{1/3}\lambda^{1/3}} \int_{N'(t)} \big(\mathrm{Vol}\big(B(n,t,\lambda,X)\big) + O\big(\max\big\{C^3 t^3 \lambda^3, 1\big\}\big)\big) t^{-2} dn\, d^\times t\, d^\times \lambda. \tag{24}$$

The integral of the first summand is

$$\frac{1}{2\pi M_i} \int_{v \in B \cap V_{\mathbb{R}}^{(i)}} \mathrm{Vol}\big(\mathcal{R}_X(v)\big) |\mathrm{Disc}(v)|^{-1} dv - \frac{1}{M_i} \int_{\lambda=(\sqrt[4]{3}/\sqrt{2})^3/C}^{X^{1/4}} \int_{C^{1/3}\lambda^{1/3}}^{\infty} \int_{N'(t)} \mathrm{Vol}\big(B(n,t,\lambda,X)\big) t^{-2} dn d^\times t d^\times \lambda. \tag{25}$$

Since $\mathrm{Vol}(\mathcal{R}_X(v))$ does not depend on the choice of $v \in V_{\mathbb{R}}^{(i)}$ (by Proposition 23), the first term of (25) is simply $\mathrm{Vol}(\mathcal{R}_X(v))/n_i$; meanwhile, the integral of the second term is easily evaluated to be $O(C^{10/3} X^{5/6}/M_i(C))$, since $\mathrm{Vol}(B(n,t,\lambda,X)) \ll C^4\lambda^4$. On the other hand, since $C^3t^3\lambda^3 \gg 1$ one immediately computes the integral of the second summand in (24) to be $O(C^{10/3}X^{5/6}/M_i(C))$. We thus obtain, for any $v \in V_{\mathbb{R}}^{(i)}$, that

$$N\big(V_{\mathbb{Z}}^{(i)};X\big) = \frac{1}{n_i}\cdot \mathrm{Vol}\big(\mathcal{R}_X(v)\big) + O\big(C^{10/3}X^{5/6}/M_i(C)\big). \tag{26}$$

To prove Theorem 20, it remains to compute the fundamental volume $\mathrm{Vol}(\mathcal{R}_X(v))$ for $v \in V_{\mathbb{R}}^{(i)}$.

5.4 Computation of the fundamental volume

Let $\mathrm{GL}_2^{\pm1}(\mathbb{R})$ denote the subgroup of elements in $\mathrm{GL}_2(\mathbb{R})$ having determinant ±1. It is known [23] (or readily computed using Gauss's explicit fundamental domain for $\mathrm{SL}_2(\mathbb{Z})\backslash\mathrm{SL}_2(\mathbb{R})$) that $\mathrm{Vol}(\mathrm{GL}_2^{\pm1}(\mathbb{Z})\backslash\mathrm{GL}_2^{\pm1}(\mathbb{R})) = \zeta(2)/\pi$, where this volume is computed with respect to the measure dh obtained from the Iwasawa decomposition of $\mathrm{GL}_2^{\pm1}(\mathbb{R})$. Then we obtain using Proposition 23 that

$$\begin{aligned}\frac{1}{n_i}\cdot \mathrm{Vol}\big(\mathcal{R}_X(v_i)\big) &= \frac{2\pi}{n_i}\int_0^{X^{1/4}} \lambda^4 d^\times\lambda \int_{\mathrm{GL}_2(\mathbb{Z})\backslash\mathrm{GL}_2^{\pm1}(\mathbb{R})} dh\\ &= \frac{2\pi}{n_i}\cdot\frac{X}{4}\cdot\frac{\zeta(2)}{\pi} = \frac{\pi^2}{12n_i}X.\end{aligned}$$

This proves Theorem 20, and thus the main term of Theorem 5. Together with the Delone-Faddeev correspondence, this also proves the main term of Theorem 6.

5.5 Congruence conditions

We may prove a version of Theorem 20 for a set in $V_{\mathbb{Z}}^{(i)}$ defined by a finite number of congruence conditions.

Theorem 26 *Suppose S is a subset of $V_{\mathbb{Z}}^{(i)}$ defined by finitely many congruence conditions modulo prime powers. Then we have*

$$\lim_{X\to\infty}\frac{N(S\cap V_{\mathbb{Z}}^{(i)};X)}{X} = \frac{\pi^2}{12n_i}\prod_p \mu_p(S), \tag{27}$$

where $\mu_p(S)$ denotes the p-adic density of S in $V_{\mathbb{Z}}$, and $n_i = 6$ or 2 for $i = 0$ or 1, respectively.

To obtain Theorem 26, suppose $S \subset V_{\mathbb{Z}}^{(i)}$ is defined by congruence conditions modulo some integer m. Then S may be viewed as the intersection of $V_{\mathbb{Z}}^{(i)}$ with the union U of (say) k translates $L_1, \ldots, L_k$ of the lattice $m \cdot V_{\mathbb{Z}}$. For each such lattice translate L_j, we may use formula (23) and the discussion following that formula to compute $N(L_j \cap V_{\mathbb{Z}}^{(i)}; X)$, where each d-dimensional volume is scaled by a factor of $1/m^d$ to reflect the fact that our new lattice has been scaled by a factor of m. With these scalings, the volumes of the d-dimensional projections of $B(n,t,\lambda,X)$, for $d = 3$, 2, and 1 are seen to be at most $O(m^{-3}C^3t^3\lambda^3)$, $O(m^{-2}C^2t^4\lambda^2)$, and $O(m^{-1}Ct^3\lambda)$, respectively. Let $a \geq 1$ be the smallest nonzero first coordinate of any point in L_j. Then, analogous to Lemma 25, the number of lattice points in $B(n,t,\lambda,X) \cap L_j$ with first coordinate nonzero is

$$\begin{cases} 0 & \text{if } \frac{C\lambda}{t^3} < a; \\ \frac{\mathrm{Vol}(B(n,t,\lambda,X))}{m^4} + O(\frac{C^3t^3\lambda^3}{m^3} + \frac{C^2t^4\lambda^2}{m^2} + \frac{Ct^3\lambda}{m} + 1) & \text{otherwise.} \end{cases} \tag{28}$$

Carrying out the integral for $N(L_j; X)$ as in (24), we obtain, up to an error of $O(X^{3/4+\epsilon})$ corresponding to the reducible points in Lemma 21, that

$$\begin{aligned} &N\big(L_j \cap V_{\mathbb{Z}}^{(i)}; X\big) \\ &\quad = \frac{\mathrm{Vol}(\mathcal{R}_X(v))}{m^4} + O\bigg(\frac{1}{M_i(C)}\bigg[\frac{C^{10/3}X^{5/6}}{a^{1/3}m^3} + \frac{C^{8/3}X^{2/3}}{a^{2/3}m^2} \\ &\qquad + \frac{C^{4/3}X^{1/3}}{a^{1/3}m} + \log X\bigg]\bigg). \end{aligned} \tag{29}$$

Assuming $m = O(X^{1/6})$, this gives (up to the $O(X^{3/4+\epsilon})$ reducible points of Lemma 21):

$$N(L_j; X) = m^{-4}\mathrm{Vol}\big(\mathcal{R}_X(v)\big) + O\big(m^{-3}X^{5/6}\big), \tag{30}$$

where the implied constant is again independent of m. Summing over j, we thus obtain

$$N(S; X) = km^{-4}\mathrm{Vol}\big(\mathcal{R}_X(v)\big) + O\big(km^{-3}X^{5/6}\big) + O\big(X^{3/4}\big). \tag{31}$$

Finally, the identities $km^{-4} = \prod_p \mu_p(S)$ and $\mathrm{Vol}(\mathcal{R}_X(v)) = \pi^2/(12n_i) \cdot X$ yield (27).

Note that (29)–(31) also give some information on the rate of convergence of (27) for various S, which will indeed be of use when studying second order terms.

6 Slicing and second order terms

In Sect. 5, we proved that $N(V_{\mathbb{Z}}^{(i)}; X) = c_1^{(i)} X + O(X^{5/6})$, where $c_1^{(0)} = \pi^2/72$ and $c_1^{(1)} = \pi^2/24$. Let $c_2^{(0)} = \sqrt{3}r/30$ and $c_2^{(1)} = r/10$ where $r = \frac{\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{\Gamma(2/3)}$. In this section, we prove that

$$N\big(V_{\mathbb{Z}}^{(i)}; X\big) = c_1^{(i)} X + c_2^{(i)} X^{5/6} + O\big(X^{3/4}\big),$$

thereby proving Theorems 5 and 6.

6.1 Proofs of Theorems 5 and 6

In (20) of the previous section (with $S = V_{\mathbb{Z}}^{(i)}$), we obtained a formula for the number $N(V_{\mathbb{Z}}^{(i)}; X)$ in terms of an integral over a chosen fundamental domain $\mathcal{F}$ for the left action of $\mathrm{GL}_2(\mathbb{Z})$ on $\mathrm{GL}_2(\mathbb{R})$. Evaluating this integral required us to evaluate the number of integral points in $B(n, t, \lambda, X)$ for various n, t, λ, X. Using Proposition 24, we concluded that the number of integral points in $B(n, t, \lambda, X)$ is equal to the volume of $B(n, t, \lambda, X)$ with an error of $O(t^3\lambda^3)$.

In this section, we count points in dyadic ranges of the discriminant. Let $B(n, t, \lambda, X/2, X)$ be the subset of $B(n, t, \lambda, X)$ that contains points having discriminant greater than $X/2$ in absolute value. We again estimate the number of integer points in $B(n, t, \lambda, X/2, X)$ to be equal to its volume, again with an error of $O(t^3\lambda^3)$. To obtain a more precise count for the number of lattice points in $B(n, t, \lambda, X/2, X)$ when t is large, we *slice* the set $B(n, t, \lambda, X/2, X)$ by the coefficient of x^3. More precisely, for $a \in \mathbb{Z}$, let $B_a(n, t, \lambda, X/2, X)$ denote the set of binary cubic forms in $B(n, t, \lambda, X/2, X)$ whose x^3-coefficient is equal to a. Then we have:

$$\#\big\{x \in V_{\mathbb{Z}}^{\mathrm{irr}} \cap B(n, t, \lambda, X/2, X)\big\} = \sum_{\substack{a \in \mathbb{Z} \\ a \neq 0}} \#\big\{x \in V_{\mathbb{Z}}^{\mathrm{irr}} \cap B_a(n, t, \lambda, X/2, X)\big\}. \tag{32}$$

We then again use Proposition 24 to estimate the right hand side of (32). We shall slice the set $B(n, t, \lambda, X/2, X)$ when t is "large". We separate the large t from the small as follows.

Let Ψ be a smooth function on $\mathbb{R}_{\geq 0}$ such that $\Psi(x) = 1$ for $x \leq 2$ and $\Psi(x) = 0$ for $x \geq 3$. Let Ψ_0 denote the function $1 - \Psi$. Let $N(V_{\mathbb{Z}}^{(i)}; X/2, X)$ denote the number of $\mathrm{GL}_2(\mathbb{Z})$-orbits on $V_{\mathbb{Z}}^{(i),\mathrm{irr}}$ having discriminant between $X/2$ and X in absolute value. Then for any $\kappa > 0$, we have just as in (23) that

$$\begin{aligned} &N\big(V_{\mathbb{Z}}^{(i)}; X/2, X\big) \\ &\quad= \frac{1}{M_i}\int_{N'(a)A'\Lambda} \Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right)\#\big\{x \in V_{\mathbb{Z}}^{(i),\mathrm{irr}} \cap B(n,t,\lambda,X/2,X)\big\} \\ &\qquad\times t^{-2} dn\, d^\times t\, d^\times\lambda \\ &\qquad+ \frac{1}{M_i}\int_{N'(a)A'\Lambda} \Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right)\#\big\{x \in V_{\mathbb{Z}}^{(i),\mathrm{irr}} \cap B(n,t,\lambda,X/2,X)\big\} \\ &\qquad\times t^{-2} dn\, d^\times t\, d^\times\lambda. \end{aligned} \tag{33}$$

Note that the first summand of the right hand side of (33) is non-zero only when $t < 3\lambda^{1/3}/\kappa$, while the second summand is non-zero only when $t > 2\lambda^{1/3}/\kappa$. We will choose κ later to minimize our error term. For now, we merely insist $\lim_{X\to\infty}\kappa = \infty$ and $\kappa < X^{3/4}$.

Let D_0 be a constant that bounds the discriminant of every point in B. Since the absolute value of the discriminant of every point in B is bounded below by 1 and above by D_0, we see that $B(n,t,\lambda,X/2,X)$ is empty unless $(\frac{X}{D_0})^{1/4} < \lambda < X^{1/4}$. Also, note that $\Psi(\frac{t\kappa}{\lambda^{1/3}})$ vanishes whenever $\lambda < 27t^3\kappa^3$. Thus, by Proposition 24, we see that the first summand of the right hand side of (33) is

$$\begin{aligned} &\frac{1}{M_i}\int_{\lambda=(\frac{X}{D_0})^{1/4}}^{X^{1/4}} \int_{t=\sqrt[4]{3}/\sqrt{2}}^{3\lambda^{1/3}/\kappa} \int_{N'(t)} \Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right)\big(\mathrm{Vol}\big(B(n,t,\lambda,X/2,X)\big) \\ &\quad+ O\big(\max\{t^3\lambda^3, 1\}\big)\big)t^{-2} dn\, d^\times t\, d^\times\lambda. \end{aligned} \tag{34}$$

The integral of the error term in (34) is easily seen to be

$$O\left(\int_{(\frac{X}{D_0})^{1/4}}^{X^{1/4}} \int_{t=\sqrt[4]{3}/\sqrt{2}}^{\lambda^{1/3}/\kappa} \lambda^3 t\, d^\times t\, d^\times\lambda\right) = O\left(\frac{X^{5/6}}{\kappa}\right).$$

Therefore, the first summand of the right hand side of (33) is equal to

$$\begin{aligned} &\frac{1}{M_i}\int_{\lambda=(\frac{X}{D_0})^{1/4}}^{X^{1/4}} \int_{t=\sqrt[4]{3}/\sqrt{2}}^{\infty} \int_{N'(t)} \Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right)\lambda^4 \\ &\quad\times \mathrm{Vol}\big(B\big(X/\big(2\lambda^4\big), X/\lambda^4\big)\big)t^{-2} dn\, d^\times t\, d^\times\lambda + O\left(\frac{X^{5/6}}{\kappa}\right), \end{aligned} \tag{35}$$

where $B(d_1, d_2)$ denotes the set of all points in B with discriminant between d_1 and d_2.

To evaluate the second summand on the right hand side of (33), we break up the integrand into a sum over points with fixed x^3-coefficient. Indeed, we see that it is equal to

$$\frac{1}{M_i}\sum_{\substack{a\in\mathbb{Z}\\ a\neq 0}}\int_{g\in\mathcal{F}}\Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right)\#\left\{x\in V_{\mathbb{Z}}^{(i),\mathrm{irr}}\cap B_a(n,t,\lambda,X/2,X)\right\}dg. \tag{36}$$

Since B is K-invariant, the number of points in $B_a(n,t,\lambda,X/2,X)$ is equal to the number of points in $B_{-a}(n,t,\lambda,X/2,X)$. Note that the integrand vanishes for $a>O(\kappa^3)$ where the implied constant depends only on B. We again use Proposition 24 to see that (36) is equal to

$$\begin{aligned}\frac{2}{M_i}\sum_{a=1}^{O(\kappa^3)}\int_{\lambda=(\frac{X}{D_0})^{1/4}}^{X^{1/4}}\int_{t=\sqrt[4]{3}/\sqrt{2}}^{\infty}\int_{N'(t)}\Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right)\bigl(\mathrm{Vol}\bigl(B_a(n,t,\lambda,X/2,X)\bigr)\\ +O\bigl(\max\{\lambda^2t^4,1\}\bigr)\bigr)t^{-2}dnd^\times td^\times\lambda.\end{aligned} \tag{37}$$

Again, we can estimate the integral of the error in (37) to be on the order of

$$\begin{aligned}&\sum_{a=1}^{O(\kappa^3)}\int_{\lambda=(\frac{X}{D_0})^{1/4}}^{X^{1/4}}\int_{t=\sqrt[4]{3}/\sqrt{2}}^{\lambda^{1/3}/a^{1/3}}\lambda^2t^4t^{-2}d^\times t\,d^\times\lambda\\ &\quad=X^{2/3}\sum_{a=1}^{O(\kappa^3)}O\bigl(a^{-2/3}\bigr)=O\bigl(\kappa X^{2/3}\bigr).\end{aligned} \tag{38}$$

We assume from now on that $\kappa\leq\frac{1}{3}X^{1/12}$. For sufficiently large values of X, it follows that if $\Psi_0(t\kappa/\lambda^{1/3})$ is nonzero, then $t>\frac{2\lambda^{1/3}}{\kappa}>1$ since $\lambda>(\frac{X}{D_0})^{1/4}$. Thus, the integral over N' in (37) always goes between $-1/2$ and $1/2$. The integral of the main term in (37) is now computed to be

$$\begin{aligned}&\frac{2}{M_i}\sum_{a=1}^{\infty}\int_{\lambda=(\frac{X}{D_0})^{1/4}}^{X^{1/4}}\int_{t>0}\Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right)\bigl(\mathrm{Vol}\bigl(B_a(0,t,\lambda,X/2,X)\bigr)\bigr)t^{-2}d^\times td^\times\lambda\\ &\quad=\frac{2}{M_i}\sum_{a=1}^{\infty}\int_{\lambda=(\frac{X}{D_0})^{1/4}}^{X^{1/4}}\int_{t>0}\Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right)\lambda^3t^3\\ &\qquad\times\mathrm{Vol}\bigl(B_{\frac{at^3}{\lambda}}\bigl(X/\bigl(2\lambda^4\bigr),X/\lambda^4\bigr)\bigr)t^{-2}d^\times td^\times\lambda,\end{aligned} \tag{39}$$

where $B_a(d_1,d_2)$ denotes the set of forms in B having x^3-coordinate equal to a and discriminant between d_1 and d_2 in absolute value. We change variables to compute the right hand side of (39); let $u=t^3a/\lambda$ so that $d^\times u=3d^\times t$. The main term in (37) is therefore equal to

$$\frac{2}{3M_i}\sum_{a=1}^{\infty}\int_{\lambda=(\frac{X}{D_0})^{1/4}}^{X^{1/4}}\int_{u>0}\Psi_0\Big(\frac{u^{1/3}\kappa}{a^{1/3}}\Big)\frac{\lambda^{10/3}u^{1/3}}{a^{1/3}} \\ \times \mathrm{Vol}\big(B_u\big(X/\big(2\lambda^4\big),X/\lambda^4\big)\big)d^\times u d^\times\lambda. \tag{40}$$

To compute the expression above, we first sum over a. Let $\Phi(z)$ be equal to $\Psi_0(u^{1/3}/z^{1/3})$. For a function F defined on the positive reals, let $\widetilde{F}(s)$ denote the Mellin transforms of F. Since the first derivative Ψ_0' is smooth and Schwartz class, the Mellin transform $\widetilde{\Psi_0'}(s)$ is holomorphic, entire, and rapidly decaying on any vertical line $\sigma+it$ as $|t|\to\infty$. Moreover, by standard properties of the Mellin transform, we have the equality $\widetilde{\Psi_0'}(s+1)=s\widetilde{\Psi_0}(s)$. Thus the functions $\widetilde{\Psi_0}(s)$ and $\widetilde{\Phi}(s)$ are entire except for a possible simple pole at 0 and rapidly decreasing on vertical lines. Moreover, the residue at 0 of $\widetilde{\Psi_0}(s)$ is equal to

$$\widetilde{\Psi_0'}(1)=\int_0^\infty \Psi_0'(y)dy=1.$$

Therefore,

$$\begin{aligned}\sum_{a=1}^{\infty}&a^{-\frac{1}{3}}\Psi_0\Big(\frac{u^{1/3}\kappa}{a^{1/3}}\Big)\\ &=\int_{\mathrm{Re}\,s=2}\zeta(s+1/3)\widetilde{\Phi}(s)\kappa^{3s}ds\\ &=3\int_{\mathrm{Re}\,s=2}\zeta(s+1/3)\widetilde{\Psi_0}(-3s)\big(\kappa^3u\big)^s ds\\ &=\zeta(1/3)+3\widetilde{\Psi_0}(-2)\big(\kappa^3u\big)^{2/3}+O_M\big(\min\big\{\big(\kappa^3u\big)^{-M},1\big\}\big)\end{aligned} \tag{41}$$

for any integer M, where we obtain the last equality by moving the line of integration to $\mathrm{Re}\,s=-M$ and computing the residues at $s=0$ and $s=\frac{2}{3}$. Therefore, (40) is equal to

$$\frac{2}{3M_i}\int_{\lambda=(\frac{X}{D_0})^{1/4}}^{X^{1/4}}\int_{u>0}\big[\zeta(1/3)+3\widetilde{\Psi_0}(-2)\big(\kappa^3u\big)^{2/3}\big] \\ \times\lambda^{10/3}u^{1/3}\mathrm{Vol}\big(B_u\big(X/\big(2\lambda^4\big),X/\lambda^4\big)\big)d^\times u d^\times\lambda, \tag{42}$$

with an error of

$$O\left(\int_{\lambda=(\frac{X}{D_0})^{1/4}}^{X^{1/4}}\int_{u>0}\min\{(\kappa^3u)^{-1},1\}\lambda^{10/3}u^{1/3}\right.$$
$$\left.\times\operatorname{Vol}\big(B_u\big(X/(2\lambda^4),X/\lambda^4\big)\big)d^\times u\,d^\times\lambda\right). \tag{43}$$

We shall eventually choose κ to be equal to $\frac{1}{3}X^{1/12}$. Therefore, (43) can be bounded above by

$$O\left(\int_{\lambda=(\frac{X}{D_0})^{1/4}}^{X^{1/4}}\int_{u=0}^{\kappa^{-3}}\lambda^{10/3}u^{1/3}d^\times u\,d^\times\lambda\right)=O\left(\frac{X^{5/6}}{\kappa}\right). \tag{44}$$

We now evaluate the integral of the two summands in the integrand of (42) separately. Evaluating the integral of the second summand, we obtain

$$\frac{2}{M_i}\int_{\lambda=(\frac{X}{D_0})^{1/4}}^{X^{1/4}}\int_{u>0}\widetilde{\Psi_0}(-2)\kappa^2\lambda^{10/3}u\operatorname{Vol}\big(B_u\big(X/(2\lambda^4),X/\lambda^4\big)\big)d^\times u\,d^\times\lambda$$
$$=\frac{1}{M_i}\int_{\lambda=(\frac{X}{D_0})^{1/4}}^{X^{1/4}}\widetilde{\Psi_0}(-2)\kappa^2\lambda^{10/3}\operatorname{Vol}\big(B\big(X/(2\lambda^4),X/\lambda^4\big)\big)d^\times\lambda,$$

which is simply equal to

$$\frac{1}{M_i}\int_{\lambda=(\frac{X}{D_0})^{1/4}}^{X^{1/4}}\int_{t=0}^{\infty}\Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right)\lambda^{\frac{10}{3}+\frac{2}{3}}\operatorname{Vol}\big(B\big(X/(2\lambda^4),X/\lambda^4\big)\big)t^{-2}d^\times t\,d^\times\lambda. \tag{45}$$

Adding (45) to the main term of (35) gives us the following.

$$\frac{1}{M_i}\int_{\lambda=(\frac{X}{D_0})^{1/4}}^{X^{1/4}}\int_{t=\sqrt[4]{3}/\sqrt{2}}^{\infty}\int_{N'(t)}\left(\Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right)+\Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right)\right)$$
$$\times\lambda^4\operatorname{Vol}\big(B\big(X/(2\lambda^4),X/\lambda^4\big)\big)t^{-2}dn\,d^\times t\,d^\times\lambda$$
$$=\frac{1}{M_i}\int_{\lambda=(\frac{X}{D_0})^{1/4}}^{X^{1/4}}\int_{t=\sqrt[4]{3}/\sqrt{2}}^{\infty}\int_{N'(t)}\big(\operatorname{Vol}\big(B(n,t,\lambda,X/2,X)\big)\big)t^{-2}dn\,d^\times t\,d^\times\lambda,$$

which can be evaluated, as in Sect. 5, to be equal to $c_1^{(i)}X/2$.

Now the integral of the first summand in (42) is

$$\frac{2}{3M_i}\int_{\lambda=(\frac{X}{D_0})^{1/4}}^{X^{1/4}}\int_{u>0}\zeta(1/3)\lambda^{10/3}u^{1/3}\mathrm{Vol}\big(B_u\big(X/\big(2\lambda^4\big),\,X/\lambda^4\big)\big)d^\times u d^\times\lambda. \tag{46}$$

Let $a(v)$, $b(v)$, $c(v)$, and $d(v)$ denote the four coordinates of points $v \in B$. Then (46) is equal to

$$\begin{aligned}&\frac{1}{3M_i}\zeta(1/3)\int_{\lambda=(\frac{X}{D_0})^{1/4}}^{X^{1/4}}\int_{B(X/(2\lambda^4),X/\lambda^4)}\lambda^{10/3}a(v)^{1/3}\frac{dv}{a(v)}d^\times\lambda\\ &=\frac{1}{3M_i}\zeta(1/3)\int_{\lambda=(\frac{X}{D_0})^{1/4}}^{X^{1/4}}\int_{B(X/(2\lambda^4),X/\lambda^4)}\lambda^{10/3}a(v)^{-2/3}dv d^\times\lambda.\end{aligned}$$

Carrying out the integral over λ, we see that (46) is equal to

$$\frac{1}{10M_i}\zeta(1/3)\big(1-2^{-5/6}\big)X^{5/6}\int_B|\mathrm{Disc}(v)|^{-5/6}a(v)^{-2/3}dv. \tag{47}$$

Recalling the definition of M_i in (22), we then see that (46) is equal to

$$\frac{2\pi}{10n_i}\zeta(1/3)\big(1-2^{-5/6}\big)X^{5/6}\frac{\int_B|\mathrm{Disc}(v)|^{-5/6}a(v)^{-2/3}dv}{\int_B|\mathrm{Disc}(v)|^{-1}dv}.$$

We now evaluate the ratio

$$\frac{\int_B|\mathrm{Disc}(v)|^{-5/6}a(v)^{-2/3}dv}{\int_B|\mathrm{Disc}(v)|^{-1}dv}. \tag{48}$$

The ratio in (48) is independent of the K-invariant set B. Thus, for any $f \in V_{\mathbb{R}}^{(i)}$, (48) is equal to

$$\begin{aligned}&|\mathrm{Disc}(f)|^{1/6}\int_K a(\gamma\cdot f)^{-2/3}d\gamma\\ &=|\mathrm{Disc}(f)|^{1/6}\int_K f\big((1,0)\cdot\gamma\big)^{-2/3}d\gamma\\ &=\frac{|\mathrm{Disc}(f)|^{1/6}}{2\pi}\int_0^{2\pi}f\big(\cos(\theta),\sin(\theta)\big)^{-2/3}d\theta.\end{aligned}$$

We now choose convenient points $f \in V_{\mathbb{R}}^{(i)}$ for $i = 0, 1$. For $i = 1$ we choose $f(x, y) = x^3 + xy^2$ which has discriminant -4. Then

$$\frac{|\mathrm{Disc}(f)|^{1/6}}{2\pi} \int_0^{2\pi} f\big(\cos(\theta), \sin(\theta)\big)^{-2/3} d\theta$$
$$= \frac{2^{1/3}}{2\pi} \int_0^{2\pi} \cos(\theta)^{-2/3} d\theta = \frac{2^{4/3}}{\pi} \int_0^{\pi/2} \cos(\theta)^{-2/3} d\theta.$$

The substitution $y = \cos(\theta)$ yields

$$\frac{2^{4/3}}{\pi} \int_0^{\pi/2} \cos(\theta)^{-2/3} d\theta = \frac{2^{4/3}}{\pi} \int_0^1 y^{-2/3}(1 - y^2)^{-1/2} dy.$$

The substitution $z = y^2$ then gives

$$\frac{2^{4/3}}{\pi} \int_0^1 y^{-2/3}\big(1 - y^2\big)^{-1/2} dy = \frac{2^{1/3}}{\pi} \int_0^1 z^{-5/6}(1 - z)^{-1/2} dz$$
$$= \frac{2^{1/3}\Gamma(1/6)\Gamma(1/2)}{\pi \Gamma(2/3)},$$

where the final equality follows from evaluating the beta function $\mathrm{B}(\frac{1}{2}, \frac{1}{6})$. Using the standard identities

$$\begin{aligned} \Gamma(1/6) &= 2^{5/3} 3^{-1/2} \pi^{3/2} / \Gamma(2/3)^2, \\ \Gamma(2/3) &= 3^{-1/2} 2\pi / \Gamma(1/3), \\ \zeta(1/3) &= (2\pi)^{-2/3} \Gamma(2/3) \zeta(2/3), \end{aligned} \tag{49}$$

we finally see that (47) is equal to $(1 - 2^{-5/6}) c_2^{(1)} X^{5/6}$.

Similarly, for $i = 0$ we choose the form $f(x, y) = x^3 - 3xy^2 \in V_{\mathbb{R}}^{(0)}$. Using the identity $\cos(3\theta) = \cos^3(\theta) - 3\cos(\theta)\sin^2(\theta)$ we see, exactly as above, that (47) is equal to $(1 - 2^{-5/6}) c_2^{(0)} X^{5/6}$. Therefore,

$$N\big(V_{\mathbb{Z}}^{(i)}; X/2, X\big) = c_1^{(i)} X/2 + c_2^{(i)}\big(1 - 2^{-5/6}\big) X^{5/6} + O\big(X^{2/3}\kappa\big)$$
$$+ O\big(X^{5/6}/\kappa\big),$$

and choosing κ to be equal to $\frac{1}{3} X^{1/12}$ proves Theorems 5 and 6.

6.2 Congruence conditions

Let $S \subset V_{\mathbb{Z}}^{(i)}$ be a $\mathrm{GL}_2(\mathbb{Z})$-invariant set. We define $N(S; X/2, X)$ to be the number of irreducible $\mathrm{GL}_2(\mathbb{Z})$-orbits on S having discriminant between $X/2$

and X in absolute value. Identically as in (33), we then have

$$\begin{aligned} &N(S; X/2, X) \\ &= \frac{1}{M_i} \int_{N'(a)A'\Lambda} \Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right) \#\{x \in S^{\mathrm{irr}} \cap B(n, t, \lambda, X/2, X)\} \\ &\quad \times t^{-2} dn\, d^\times t\, d^\times \lambda \\ &\quad + \frac{1}{M_i} \int_{N'(a)A'\Lambda} \Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right) \#\{x \in S^{\mathrm{irr}} \cap B(n, t, \lambda, X/2, X)\} \\ &\quad \times t^{-2} dn\, d^\times t\, d^\times \lambda. \end{aligned}$$

We use this as a definition of $N(S; X/2, X)$ even when the set $S \subset V_{\mathbb{Z}}^{(i)}$ is not $\mathrm{GL}_2(\mathbb{Z})$-invariant.

Suppose $\mathcal{L} \subset V_{\mathbb{Z}}$ is any sublattice of index T in $V_{\mathbb{Z}}$ that is defined by congruence conditions modulo m, so that $mV_{\mathbb{Z}} \subset L$. In what follows, we compute $N(\mathcal{L} \cap V_{\mathbb{Z}}^{(i)}; X/2, X)$ and $N(\mathcal{L} \cap V_{\mathbb{Z}}^{(i)}; X)$, for $i = 0, 1$. The computation is very similar to that of $N(V_{\mathbb{Z}}^{(i)}; X/2, X)$ and $N(V_{\mathbb{Z}}^{(i)}; X)$, and we highlight the differences that occur.

We have

$$\begin{aligned} &N\left(\mathcal{L} \cap V_{\mathbb{Z}}^{(i)}; X/2, X\right) \\ &= \frac{1}{M_i} \int_{N'(a)A'\Lambda} \Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right) \#\{x \in \mathcal{L} \cap V_{\mathbb{Z}}^{(i),\mathrm{irr}} \cap B(n, t, \lambda, X/2, X)\} \\ &\quad \times t^{-2} dn\, d^\times t\, d^\times \lambda \\ &\quad + \frac{1}{M_i} \int_{N'(a)A'\Lambda} \Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right) \#\{x \in \mathcal{L} \cap V_{\mathbb{Z}}^{(i),\mathrm{irr}} \cap B(n, t, \lambda, X/2, X)\} \\ &\quad \times t^{-2} dn\, d^\times t\, d^\times \lambda. \end{aligned} \tag{50}$$

Analogously to (28), we see that the first summand of the right hand side of (50) is equal to

$$\begin{aligned} &\frac{1}{TM_i} \int_{\lambda=(\frac{X}{D_0})^{1/4}}^{X^{1/4}} \int_{t=\sqrt[4]{3}/\sqrt{2}}^{\infty} \int_{N'(t)} \Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right) \lambda^4 \mathrm{Vol}\left(B\left(X/(2\lambda^4), X/\lambda^4\right)\right) \\ &\quad \times t^{-2} dn d^\times t d^\times \lambda \\ &\quad + \frac{m^4}{TM_i} \int_{\lambda=(\frac{X}{D_0})^{1/4}}^{X^{1/4}} \int_{t=\sqrt[4]{3}/\sqrt{2}}^{\infty} \int_{N'(t)} \Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right) \end{aligned}$$

$$\times\, O\left(\frac{t^3\lambda^3}{m^3}+\frac{t^4\lambda^2}{m^2}+\frac{t^3\lambda}{m}+1\right)t^{-2}dnd^\times td^\times\lambda.$$

We evaluate the second term above to be

$$O\left(\frac{mX^{5/6}}{T\kappa}+\frac{m^2X^{2/3}}{T\kappa^2}+\frac{m^2X^{1/3}}{T\kappa}+\frac{m^4}{T}\right). \tag{51}$$

As in (36), we see that the second summand of the right hand side of (50) is equal to

$$\frac{1}{M_i}\sum_{\substack{a\in\mathbb{Z}\\ a\neq 0}}\int_{\mathcal{F}}\Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right)\#\left\{x\in\mathcal{L}^{\mathrm{irr}}\cap V_{\mathbb{Z}}^{(i)}\cap B_a(n,t,\lambda,X/2,X)\right\}dg. \tag{52}$$

We write $T=T_1T_2$, where the x^3-coefficient of every element in $\mathcal{L}$ is a multiple of T_1 and the index of $\mathcal{L}_a$ in V_a is equal to T_2; here $\mathcal{L}_a$ (resp. V_a) denotes the set of all forms in $\mathcal{L}$ (resp. $V_{\mathbb{Z}}$) whose x^3-coefficient is equal to a. As in (36)–(40), we estimate (52) to be

$$\begin{aligned}&\frac{2}{3T_2M_i}\sum_{\substack{a=1\\ T_1|a}}^{\infty}\int_{\lambda=(\frac{X}{D_0})^{1/4}}^{X^{1/4}}\int_{u>0}\Psi_0\left(\frac{u^{1/3}\kappa}{a^{1/3}}\right)\frac{\lambda^{10/3}u^{1/3}}{a^{1/3}}\\ &\quad\times \mathrm{Vol}\big(B_u\big(X/(2\lambda^4),X/\lambda^4\big)\big)d^\times ud^\times\lambda\\ &\quad+\sum_{\substack{a=1\\ T_1|a}}^{O(\kappa^3)}\int_{\lambda=(\frac{X}{D_0})^{1/4}}^{X^{1/4}}\int_{t=\lambda^{1/3}/\kappa}^{\lambda^{1/3}/a^{1/3}}\frac{m^3}{T_2}\cdot O\left(\frac{\lambda^2t^4}{m^2}+\frac{\lambda t^2}{m}+1\right)t^{-2}d^\times t\,d^\times\lambda.\end{aligned}$$

The error term is easily integrated to give

$$O\left(\frac{m\kappa X^{2/3}}{T}+\frac{m^2X^{1/4}\kappa}{T}+\frac{m^3X^{1/4}}{T}\right). \tag{53}$$

Analogously to the computations in (41) and (42), we have

$$\begin{aligned}\sum_{\substack{a=1\\ T_1|a}}^{\infty}a^{-\frac13}\Psi_0\left(\frac{u^{1/3}\kappa}{a^{1/3}}\right)&=T_1^{-1/3}\int_{\mathrm{Re}\,s=2}\zeta(s+1/3)\widetilde{\Phi}(s)\big(T_1^{-1/3}\kappa\big)^{3s}ds\\ &=3T_1^{-1/3}\int_{\mathrm{Re}\,s=2}\zeta(s+1/3)\widetilde{\Psi_0}(-3s)\big(\big(T_1^{-1/3}\kappa\big)^3u\big)^s ds\\ &=T_1^{-1/3}\zeta(1/3)+3\widetilde{\Psi_0}(-2)T_1^{-1}\big(\kappa^3u\big)^{2/3}\end{aligned}$$

$$+ O_M\big(T_1^{-1/3}\min\{\big(T_1^{-1}\kappa^3 u\big)^{-M}, 1\}\big)$$

for any integer M. Identically as in (44), the error coming from the term $O_M(T_1^{-1/3}\min\{(T_1^{-1}\kappa^3 u)^{-M}, 1\})$ is equal to $O(X^{5/6}/(\kappa T_2))$. The total error is thus

$$O\left(\frac{m\kappa X^{2/3}}{T} + \frac{m^2 X^{1/4}\kappa}{T} + \frac{m^3 X^{1/4}}{T} + \frac{mX^{5/6}}{T\kappa} + \frac{m^2 X^{2/3}}{T\kappa^2} + \frac{m^2 X^{1/3}}{T\kappa} + \frac{m^4}{T}\right).$$

We will only be interested in the range where $m \le X^{1/4}$. In this range, we optimize the above by taking $\kappa = X^{1/12}$ to get an error of

$$O\left(\frac{mX^{3/4}}{T} + \frac{m^2 X^{1/2}}{T} + \frac{m^3 X^{1/4}}{T}\right) = O\left(\frac{mX^{3/4}}{T}\right).$$

We thus have the following theorem:

Theorem 27 *Let $\mathcal{L} \subset V_{\mathbb{Z}}$ be a sublattice of index T in $V_{\mathbb{Z}}$, containing $mV_{\mathbb{Z}}$. Write $T = T_1T_2$, where the x^3-coefficient of each element in $\mathcal{L}$ is a multiple of T_1 and the corresponding index of $\mathcal{L}_a$ in V_a is equal to T_2. Assume further that $m^4 \le X$. Then*

$$N\big(\mathcal{L} \cap V_{\mathbb{Z}}^{(i)}; X/2, X\big) = \frac{c_1^{(i)}}{T}\frac{X}{2} + \big(1 - 2^{-5/6}\big)\frac{c_2^{(i)}}{T_1^{1/3}T_2}X^{5/6} + O\left(\frac{m}{T}X^{3/4}\right). \tag{54}$$

Summing over dyadic ranges of the discriminant, we also then obtain

$$N\big(\mathcal{L} \cap V_{\mathbb{Z}}^{(i)}; X\big) = \frac{c_1^{(i)}}{T}X + \frac{c_2^{(i)}}{T_1^{1/3}T_2}X^{5/6} + O\left(\frac{m}{T}X^{3/4}\right). \tag{55}$$

Remark 3 Note that our proof shows that the analogue of Theorem 27 also holds for translates of the lattice $\mathcal{L}$, although the constant $\frac{c_2^{(i)}}{T_1^{1/3}T_2}$ would get replaced with something rather more complicated. However, the error term would remain the same.

7 *p*-Adic densities for the second term

Let p be a fixed prime and σ be the splitting type (f, p) at p of an integral binary cubic form f. The methods of the previous section allow us to count the asymptotic number of $\mathrm{GL}_2(\mathbb{Z})$-orbits on $\mathcal{U}_p(\sigma)$ having bounded discriminant.

More precisely, let us define $\mu_1(\sigma, p)$, $\mu_2(\sigma, p)$, $\mu_1(p)$, and $\mu_2(p)$ so that

$$N\big(\mathcal{U}_p(\sigma) \cap V_{\mathbb{Z}}^{(i)}; X\big) = \mu_1(\sigma, p)c_1^{(i)}X + \mu_2(\sigma, p)c_2^{(i)}X^{5/6} + O_\epsilon\big(X^{3/4+\epsilon}\big),$$
$$N(\mathcal{U}_p; X) = \mu_1(p)c_1^{(i)}X + \mu_2(p)c_2^{(i)}X^{5/6} + O_\epsilon\big(X^{3/4+\epsilon}\big).$$

We similarly define $\mu_1'(p)$ and $\mu_2'(p)$ so that

$$N(\mathcal{V}_p; X) = \mu_1'(p)c_1^{(i)}X + \mu_2'(p)c_2^{(i)}X^{5/6} + O_\epsilon\big(X^{3/4+\epsilon}\big).$$

The values of $\mu_1(\sigma, p)$, $\mu_1(p)$ and $\mu_1'(p)$ were computed in Sect. 4 to be equal to $\mu(\mathcal{U}_p(\sigma))$, $\mu(\mathcal{U}_p)$, and $\mu(\mathcal{V}_p)$, respectively. In this section we compute the values of $\mu_2(\sigma, p)$, $\mu_2(p)$ and $\mu_2'(p)$ for all splitting types σ and all primes p. We will require these results to prove Theorems 3 and 4.

From the results of Sect. 4, we see that $\mathcal{U}_p(111) = T_p(111)$, $\mathcal{U}_p(12) = T_p(12)$, and $\mathcal{U}_p(3) = T_p(3)$. For $\sigma = (111), (12), (3)$, we write $T_p(\sigma)$ as a union of lattices in the following way. For $\alpha, \beta, \gamma \in \mathbb{P}^1_{\overline{\mathbb{F}}_p}$, let $T_p(\alpha, \beta, \gamma)$ be the set of all elements $f \in V_{\mathbb{Z}}$ such that the reduction of f modulo p has roots α, β, and γ in $\mathbb{P}^1_{\overline{\mathbb{F}}_p}$. Then

$$T_p(111) = \bigcup_{\alpha,\beta,\gamma\in\mathbb{P}^1_{\mathbb{F}_p}} \big(T_p(\alpha, \beta, \gamma) \setminus p \cdot V_{\mathbb{Z}}\big),$$

$$T_p(12) = \bigcup_{\alpha\in\mathbb{P}^1_{\mathbb{F}_p},\beta_1,\beta_2\in\mathbb{P}^1_{\mathbb{F}_{p^2}}\setminus\mathbb{P}^1_{\mathbb{F}_p}} \big(T_p(\alpha, \beta_1, \beta_2) \setminus p \cdot V_{\mathbb{Z}}\big),$$

$$T_p(3) = \bigcup_{\gamma_1,\gamma_2,\gamma_3\in\mathbb{P}^1_{\mathbb{F}_{p^3}}\setminus\mathbb{P}^1_{\mathbb{F}_p}} \big(T_p(\gamma_1, \gamma_2, \gamma_3) \setminus p \cdot V_{\mathbb{Z}}\big),$$

where α, β, γ are distinct points in $\mathbb{P}^1_{\mathbb{F}_p}$, while β_1, β_2 are $\mathbb{F}_p$-conjugate points in $\mathbb{P}^1(\mathbb{F}_{p^2})$ and $\gamma_1, \gamma_2, \gamma_3$ are $\mathbb{F}_p$-conjugate points in $\mathbb{P}^1(\mathbb{F}_{p^3})$.

Similarly, the set $T_p(1^21)$ (resp. $T_p(1^3)$) can be written as the union over pairs of distinct points $\alpha, \beta \in \mathbb{P}^1_{\mathbb{F}_p}$ (resp. points $\alpha \in \mathbb{P}^1_{\mathbb{F}_p}$) of the sets $T_p(\alpha, \alpha, \beta)$ (resp. $T_p(\alpha, \alpha, \alpha)$) which consist of elements $f \in V_{\mathbb{Z}}$ whose reduction modulo p has a double root at α and a single root at β (resp. a triple root at α). Furthermore, the results of Sect. 4 imply that elements f in $T_p(\alpha, \alpha, \beta)$ or $T_p(\alpha, \alpha, \alpha)$ correspond to rings that are non-maximal at p if and only if $f(\tilde{\alpha})$ is a multiple of p^2, where $\tilde{\alpha}$ is any element in $\mathbb{Z}$ whose reduction modulo p is equal to α.

We can now compute the values of $\mu_2(\sigma, p)$ from Theorem 27. Let $\sigma = (111)$. We apply Theorem 27 to the lattices $T_p(\alpha, \beta, \gamma)$ and $p \cdot V_{\mathbb{Z}}$. For the lattice $T_p([1:0],\beta,\gamma)$ we have $T_1 = p$ and $T_2 = p^2$ in the notation of Theorem 27. Therefore

$$N\bigl(T_p\bigl([1:0],\beta,\gamma\bigr);X\bigr) = \frac{c_1^{(i)}}{p^3}X + \frac{c_2^{(i)}}{p^{7/3}}X^{5/6} + O_\epsilon\bigl(X^{3/4+\epsilon}\bigr).$$

For the lattice $T_p(\alpha,\beta,\gamma)$, where none of α, β, and γ are equal to $[1:0] \in \mathbb{P}^1_{\mathbb{F}_p}$, we have $T_1 = 1$ and $T_2 = p^3$. Therefore

$$N\bigl(T_p(\alpha,\beta,\gamma);X\bigr) = \frac{c_1^{(i)}}{p^3}X + \frac{c_2^{(i)}}{p^3}X^{5/6} + O_\epsilon\bigl(X^{3/4+\epsilon}\bigr).$$

Finally for the lattice $p\cdot V_{\mathbb{Z}}$ we have $T_1 = p$ and $T_2 = p^3$. Therefore,

$$N(p\cdot V_{\mathbb{Z}};X) = \frac{c_1^{(i)}}{p^4}X + \frac{c_2^{(i)}}{p^{10/3}}X^{5/6} + O_\epsilon(X^{3/4+\epsilon}).$$

There are $\binom{p}{2}$ lattices $T_p([1:0],\beta,\gamma)$ and $\binom{p}{3}$ lattices $T_p(\alpha,\beta,\gamma)$ where none of α, β, and γ are equal to $[1:0]$. Thus we have

$$\mu_2\bigl((111),p\bigr) = \binom{p}{2}\bigl(p^{-7/3} - p^{-10/3}\bigr) + \binom{p}{3}\bigl(p^{-3} - p^{-10/3}\bigr).$$

Consider now the splitting type $\sigma = (12)$. Following the above notation, we have $(T_1,T_2) = (p,p^2)$ for the lattice $T_p([1:0],\beta_1,\beta_2)$ and $(T_1,T_2) = (1,p^3)$ for $T_p(\alpha,\beta_1,\beta_2)$ when $\alpha \neq [1:0]$. Since we have $(p^2-p)/2$ choices for the $\mathbb{F}_p$-conjugate points β_1 and β_2, we have

$$\mu_2\bigl((12),p\bigr) = \frac{p^2-p}{2}\bigl(p\bigl(p^{-3} - p^{-10/3}\bigr) + \bigl(p^{-7/3} - p^{-10/3}\bigr)\bigr).$$

For $\mathbb{F}_p$-conjugate points $\gamma_1,\gamma_2,\gamma_3 \in \mathbb{P}^1(\mathbb{F}_{p^3})$, the lattice $T_p(\gamma_1,\gamma_2,\gamma_3)$ has $(T_1,T_2) = (1,p^3)$. Since there are $(p^3-p)/3$ such triples $(\gamma_1,\gamma_2,\gamma_3)$, we see that

$$\mu_2\bigl((3),p\bigr) = \frac{p^3-p}{3}\bigl(p^{-3} - p^{-10/3}\bigr).$$

When $\sigma = (1^21)$, the situation is slightly more complicated. The lattice $T_p(\alpha,\alpha,\beta)$ has $(T_1,T_2) = (p,p^2)$ when α or β equals $[1:0]$, and has $(T_1,T_2) = (1,p^3)$ otherwise. To account for the fact that an element f in $T_p(\alpha,\alpha,\beta)$ corresponds to a ring that is maximal at p if and only if $f(\tilde{\alpha})$ (where $\tilde{\alpha}$ is an integer whose reduction modulo p is α) is not a multiple of

Table 1 Values of p-adic densities for splitting types

σ	$\mu_1(\sigma, p)$	$\mu_2(\sigma, p)$
(111)	$\frac{1}{6}(p-1)^2p(p+1)/p^4$	$p^{-3}(\binom{p}{3}(1-p^{-1/3})+\frac{p(p-1)}{2}(p-1)p^{-1/3})$
(12)	$\frac{1}{2}(p-1)^2p(p+1)/p^4$	$p^{-3}(p(\frac{p^2-p}{2})(1-p^{-1/3})+\frac{p^2-p}{2}(p-1)p^{-1/3})$
(3)	$\frac{1}{3}(p-1)^2p(p+1)/p^4$	$p^{-3}((\frac{p^3-p}{3})(1-p^{-1/3}))$
(1^21)	$(p-1)^2(p+1)/p^4$	$p^{-3}(p(p-1)(1-p^{-1})+p(p-1)(1-p^{-1/3})p^{-1/3})$
(1^3)	$(p-1)^2(p+1)/p^5$	$p^{-3}(p(1-p^{-1/3})(1-p^{-1})+(p-1)(1-p^{-1/3})p^{-1/3})$

p^2, we must multiply the density of each lattice $T_p(\alpha, \alpha, \beta)$ by $1 - p^{-1/3}$ if $\alpha = [1:0]$ and by $1 - p^{-1}$ if $\alpha \neq [1:0]$. Therefore,

$$\mu_2\big((1^21), p\big) = p\big(p^{-7/3} - p^{-10/3}\big)\big(1 - p^{-1/3}\big) + \big(p\big(p^{-7/3} - p^{-10/3}\big) + p(p-1)\big(p^{-3} - p^{-10/3}\big)\big)\big(1 - p^{-1}\big).$$

Finally, let σ equal (1^3). The lattice $T_p(\alpha, \alpha, \alpha)$ has $(T_1, T_2) = (p, p^2)$ when $\alpha = [1:0]$ and $(T_1, T_2) = (1, p^3)$ otherwise. Therefore, as before,

$$\mu_2\big((1^3), p\big) = \big(p^{-7/3} - p^{-10/3}\big)\big(1 - p^{-1/3}\big) + p\big(p^{-3} - p^{-10/3}\big)\big(1 - p^{-1}\big).$$

We list the values of $\mu_1(\sigma, p)$ and $\mu_2(\sigma, p)$ in Table 1.

Adding up the values of the $\mu_1(\sigma, p)$ and the $\mu_2(\sigma, p)$, both over all σ and over all $\sigma \neq (1^3)$, we obtain the following lemma.

Lemma 28 *We have*:

$$\begin{aligned} \mu_1(p) &= \left(1 - \frac{1}{p^2}\right)\left(1 - \frac{1}{p^3}\right), \\ \mu_1'(p) &= \left(1 - \frac{1}{p^2}\right)^2, \\ \mu_2(p) &= \left(1 - \frac{1}{p^2}\right)\left(1 - \frac{1}{p^{5/3}}\right), \\ \mu_2'(p) &= \left(1 - \frac{1}{p^2}\right)\left(1 - \frac{p^{1/3}+1}{p(p+1)}\right). \end{aligned} \tag{56}$$

8 Proofs of the main terms of Theorems 1–8

In this section, we use the results of Sects. 1–5 to complete the proofs of the main terms of Theorems 1–8.

We have already proven the main term (indeed even the second main term) of Theorems 5 and 6, which give counts for the number of isomorphism classes of integral binary cubic forms and cubic orders, respectively, having bounded discriminant. In fact, Theorem 26 gives the main term for the count of integral binary cubic forms satisfying any specified finite set of congruence conditions.

We recall from Sect. 3, however, that the set of elements in $V_{\mathbb{Z}}$ corresponding to maximal orders is defined by infinitely many congruence conditions. Similarly, we show in Sect. 8.1 that the count in Theorem 2 of 3-torsion elements in class groups of quadratic fields is equal to the count of integer binary cubic forms in another set that too is defined by infinitely many congruence conditions. To prove that (27) still holds for such sets, we require a uniform estimate on the error term when only finitely many factors are taken in (27). This uniformity estimate is proven in Sect. 8.2.

In Sects. 8.3, 8.4, and 8.5, we then carry out a sieve, using this uniformity estimate, to prove Theorems 1, 8, and 2 which imply the first main terms of Theorems 3, 7, and 4, respectively.

8.1 Cubic fields with no totally ramified primes

To prove Theorem 2, we consider those cubic fields in which no prime is totally ramified. The significance of being "nowhere totally ramified" is as follows. Given an S_3-cubic field K_3, let K_6 denote its Galois closure. Let K_2 denote the quadratic field contained in K_6 (the "quadratic resolvent field"). Then one checks that the Galois cubic extension K_6/K_2 is unramified precisely when the cubic field K_3 is nowhere totally ramified. Conversely, if K_2 is a quadratic field, and K_6 is any unramified cubic extension of K_2, then as an extension of the base field $\mathbb{Q}$, the field K_6 is Galois with Galois group S_3, and any cubic subfield K_3 of K_6 is then nowhere totally ramified.

8.2 A uniformity estimate

As in Sect. 4, let us denote by $\mathcal{V}_p$ the set of all $f \in V_{\mathbb{Z}}$ corresponding to cubic rings R that are maximal at p and in which p is not totally ramified. Furthermore, let $\mathcal{Z}_p = V_{\mathbb{Z}} - \mathcal{V}_p$ (thus $\mathcal{Z}_p$ consists of those binary cubic forms whose discriminants are not fundamental). In order to apply a simple sieve to obtain Theorems 1, 2, and 8, we require the following proposition:

Proposition 29 $N(\mathcal{Z}_p; X) = O(X/p^2)$, *where the implied constant is independent of* p.

Proof The set $\mathcal{Z}_p$ may be naturally partitioned into two subsets: $\mathcal{W}_p$, the set of forms $f \in V_{\mathbb{Z}}$ corresponding to cubic rings not maximal at p; and $\mathcal{Y}_p$, the set of forms $f \in V_{\mathbb{Z}}$ corresponding to cubic rings that are maximal at p but also totally ramified at p.

We first treat $\mathcal{W}_p$. Recall that the *content* $\mathrm{ct}(R)$ of a cubic ring R is defined as the maximal integer n such that $R = \mathbb{Z} + nR'$ for some cubic ring R'. It follows from (10) that the content of R is simply the content (i.e., the greatest common divisor of the coefficients) of the corresponding binary cubic form f. We say R is *primitive* if $\mathrm{ct}(R) = 1$, and R is *primitive at* p if $\mathrm{ct}(R)$ is not a multiple of p. The following lemma follows immediately from Proposition 15. □

Lemma 30 *Suppose R is a cubic ring that is primitive at p. Then the number of subrings of index p in R is at most* 3.

To prove the proposition, suppose R is a cubic ring of absolute discriminant less than X that is not maximal at p. By Lemma 13, the cubic ring R has a $\mathbb{Z}$-basis $\langle 1, \omega, \theta\rangle$ such that either (i) $R' = \mathbb{Z} + \mathbb{Z}\cdot(\omega/p) + \mathbb{Z}\cdot\theta$ forms a cubic ring, or (ii) $R'' = \mathbb{Z} + \mathbb{Z}\cdot(\omega/p) + \mathbb{Z}\cdot(\theta/p)$ forms a cubic ring.

Assume we are in case (i), i.e., R' is a ring. If R' is primitive at p, then we have that $\mathrm{Disc}(R') = \mathrm{Disc}(R)/p^2 < X/p^2$; thus the total number of possible rings R' that can arise is $O(X/p^2)$ by Theorem 6. By Lemma 30, the number of R that can correspond to such R' is at most three times that, which is also $O(X/p^2)$. On the other hand, if R' is not primitive at p, then let S be the ring such that $R' = \mathbb{Z} + pS$. Then $\mathrm{Disc}(S) = \mathrm{Disc}(R)/p^6 < X/p^6$, so the number of possibilities for S is $O(X/p^6)$, which is thus the number of possibilities for R' (since $R' = \mathbb{Z} + pS$). The number of possibilities for R is then $p+1$ (the number of index p submodules of a free $\mathbb{Z}$-module of rank 2) times the number of possibilities for R', yielding $O((p+1)X/p^6)$ possibilities. We conclude that in case (i), the number of possibilities for R is $O(X/p^2) + O((p+1)X/p^6) = O(X/p^2)$.

Assume we are now in case (ii), i.e., R'' is a ring. Then $R = \mathbb{Z} + pR''$ where $\mathrm{Disc}(R'') = \mathrm{Disc}(R)/p^4 < X/p^4$. The number of possible R'' in this case is $O(X/p^4)$ by Theorem 6, and so the number of possible cubic rings $R = \mathbb{Z} + pR''$ arising from case (ii) is $O(X/p^4)$. Thus the total number $N(\mathcal{W}_p; X)$ of cubic rings R that are not maximal at p and have absolute discriminant less than X is $O(X/p^2) + O(X/p^4) = O(X/p^2)$, as desired.

Finally, that $N(\mathcal{Y}_p; X) = O(X/p^2)$ follows easily from class field theory. A nice, short exposition of this may be found in, e.g., [11, p. 15].

8.3 Density of discriminants of cubic fields (Proof of Theorem 1)

We may now prove Theorem 1. Let $\mathcal{U} = \bigcap_p \mathcal{U}_p$. Then $\mathcal{U}$ is the set of $v \in V_{\mathbb{Z}}$ corresponding to maximal cubic rings R. By Lemma 19, the p-adic density of $\mathcal{U}_p$ is given by $\mu(\mathcal{U}_p) = (1 - p^{-2})(1 - p^{-3})$. Suppose Y is any positive integer. It follows from (27) that

$$\lim_{X\to\infty} \frac{N(\bigcap_{p<Y} \mathcal{U}_p \cap V_{\mathbb{Z}}^{(i)}; X)}{X} = \frac{\pi^2}{12n_i} \prod_{p<Y} \big[\big(1 - p^{-2}\big)\big(1 - p^{-3}\big)\big].$$

Letting Y tend to ∞, we obtain immediately that

$$\limsup_{X\to\infty} \frac{N(\mathcal{U} \cap V_{\mathbb{Z}}^{(i)}; X)}{X} \le \frac{\pi^2}{12n_i} \prod_{p} \big[\big(1 - p^{-2}\big)\big(1 - p^{-3}\big)\big] = \frac{1}{2n_i\zeta(3)}.$$

To obtain a lower bound for $N(\mathcal{U} \cap V_{\mathbb{Z}}^{(i)}; X)$, we note that

$$\bigcap_{p<Y} \mathcal{U}_p \subset \Big(\mathcal{U} \cup \bigcup_{p\ge Y} \mathcal{W}_p\Big).$$

Hence by Proposition 29,

$$\lim_{X\to\infty} \frac{N(\mathcal{U} \cap V_{\mathbb{Z}}^{(i)}; X)}{X} \ge \frac{\pi^2}{12n_i} \prod_{p<Y} \big[\big(1 - p^{-2}\big)\big(1 - p^{-3}\big)\big] - O\Big(\sum_{p\ge Y} p^{-2}\Big).$$

Letting Y tend to infinity completes the proof.

We note that the same arguments also apply when counting cubic fields with specified local behavior at finitely many primes.

8.4 A simultaneous generalization (Proof of Theorem 8)

We now prove Theorem 8, which gives the density of discriminants of cubic orders or fields satisfying any finite number (or in many natural cases, an infinite number) of local conditions. To this end, for each prime p let Σ_p be a set of isomorphism classes of nondegenerate cubic rings over $\mathbb{Z}_p$. (By *nondegenerate*, we mean having nonzero discriminant over $\mathbb{Z}_p$, so that it can arise as $R \otimes \mathbb{Z}_p$ for some cubic order R over $\mathbb{Z}$.) We denote the collection (Σ_p) of these local specifications over all primes p by Σ. We say that the collection $\Sigma = (\Sigma_p)$ is *acceptable* if, for all sufficiently large p, the set Σ_p contains at least the maximal cubic rings over $\mathbb{Z}_p$ that are not totally ramified at p.

For a cubic order R over $\mathbb{Z}$, we write "$R \in \Sigma$" (or say that "R is a Σ-order") if $R \otimes \mathbb{Z}_p \in \Sigma_p$ for all p. We wish to determine the number of Σ-orders R of bounded discriminant, for any acceptable collection Σ of local specifications.

To this end, fix an acceptable $\Sigma = (\Sigma_p)$ of local specifications, and also fix any $i \in \{0, 1\}$. Let $S = S(\Sigma, i)$ denote the set of all irreducible $f \in V_{\mathbb{Z}}^{(i)}$ such that the corresponding cubic ring $R(f) \in \Sigma$. Then the number of Σ-orders with discriminant at most X is given by $N(S; X)$. We prove the following asymptotics for $N(S; X)$.

Theorem 31 *We have*

$$\lim_{X\to\infty} \frac{N(S(\Sigma, i); X)}{X} = \frac{1}{2n_i} \prod_p \left(\frac{p-1}{p} \cdot \sum_{R\in\Sigma_p} \frac{1}{\mathrm{Disc}_p(R)} \cdot \frac{1}{|\mathrm{Aut}(R)|} \right).$$

Although $S = S(\Sigma, i)$ might again be defined by infinitely many congruence conditions, the estimate provided in Proposition 29 (and the fact that Σ is acceptable) shows that (27) continues to hold for the set S; the argument is identical to that in the proof of Theorem 1.

We now evaluate $\mu_p(S)$ in terms of the cubic rings lying in Σ_p.

Lemma 32 *We have*

$$\mu_p\big(S(\Sigma, i)\big) = \frac{\#\mathrm{GL}_2(\mathbb{F}_p)}{p^4} \cdot \sum_{R\in\Sigma_p} \frac{1}{\mathrm{Disc}_p(R)} \cdot \frac{1}{|\mathrm{Aut}(R)|}.$$

Proof The proof of Theorem 9, with $\mathbb{Z}_p$ in place of $\mathbb{Z}$, shows that for any cubic $\mathbb{Z}_p$-algebra R there is a unique element $v \in V_{\mathbb{Z}_p}$ up to $\mathrm{GL}_2(\mathbb{Z}_p)$-equivalence satisfying $R_{\mathbb{Z}_p}(v) = R$. Moreover, the automorphism group of such a cubic $\mathbb{Z}_p$-algebra R is simply the size of the stabilizer in $\mathrm{GL}_2(\mathbb{Z}_p)$ of the corresponding element $v \in V_{\mathbb{Z}_p}$ (cf. Prop. 12).

We normalize the Haar measure dg on the p-adic group $\mathrm{GL}_2(\mathbb{Z}_p)$ so that $\int_{g\in\mathrm{GL}_2(\mathbb{Z}_p)} dg = \#\mathrm{GL}_2(\mathbb{F}_p)$. Since $|\mathrm{Disc}(x)|_p^{-1} \cdot dx$ is a $\mathrm{GL}_2(\mathbb{Q}_p)$-invariant measure on $V_{\mathbb{Z}_p}$, we must have for any cubic $\mathbb{Z}_p$-algebra $R = R(v_0)$ that

$$\begin{aligned}\int_{\substack{x\in V_{\mathbb{Z}_p}\\ R(x)=R}} dx &= c \cdot \int_{g\in\mathrm{GL}_2(\mathbb{Z}_p)/\mathrm{Stab}(v_0)} |\mathrm{Disc}(gv_0)|_p \cdot dg \\ &= c \cdot \frac{|\mathrm{Disc}(R)|_p \cdot \#\mathrm{GL}_2(\mathbb{F}_p)}{\#\mathrm{Aut}_{\mathbb{Z}_p}(R)},\end{aligned}$$

for some constant c. A Jacobian calculation using an indeterminate v_0 satisfying $\mathrm{Disc}(v_0) \neq 0$ shows that $c = p^{-4}$, independent of v_0. The lemma follows. □

Finally, we observe that $\#\mathrm{GL}_2(\mathbb{F}_p) = (p^2-1)(p^2-p)$, and so

$$\begin{aligned}\frac{\pi^2}{12n_i}\prod_p \mu_p\big(S(\Sigma,i)\big) \\ = \frac{\pi^2}{12n_i}\prod_p\left(1-\frac{1}{p^2}\right)\left(\frac{p-1}{p}\right)\cdot\sum_{R\in\Sigma_p}\frac{1}{\mathrm{Disc}_p(R)}\cdot\frac{1}{|\mathrm{Aut}(R)|},\end{aligned}$$

proving Theorem 31. Noting that $n_1 = \mathrm{Aut}_{\mathbb{R}}(\mathbb{R}^3)$ and $n_2 = \mathrm{Aut}_{\mathbb{R}}(\mathbb{R}\oplus\mathbb{C})$ then yields Theorem 8.

Remark 4 Lemma 32, together with the identities $\mu_p(V_{\mathbb{Z}_p}) = 1$ and $\mu_p(\mathcal{U}_p) = (p^3-1)(p^2-1)/p^5$ of Lemma 19, give the interesting formulae

$$\sum_{R \text{ nondeg. cubic ring}/\mathbb{Z}_p}\frac{1}{\mathrm{Disc}_p(R)}\cdot\frac{1}{|\mathrm{Aut}(R)|} = \left(1-\frac{1}{p}\right)^{-1}\left(1-\frac{1}{p^2}\right)^{-1} \tag{57}$$

and

$$\sum_{K \text{ etale cubic extension of } \mathbb{Q}_p}\frac{1}{\mathrm{Disc}_p(K)}\cdot\frac{1}{|\mathrm{Aut}(K)|} = 1+\frac{1}{p}+\frac{1}{p^2}. \tag{58}$$

(Note that (57) is an infinite sum!) What is remarkable about these formulae is that their statements are independent of p. Such "mass formulae" for local fields and orders in fact hold in far more generality (in particular, for degrees other than 3); see [6, 29], and [9].

8.5 The mean size of the 3-torsion subgroups of class groups of quadratic fields

In this section we prove Davenport and Heilbronn's theorem on the average size of the 3-torsion subgroups of class groups of quadratic fields. This is accomplished using class field theory, as in Davenport and Heilbronn's original arguments. This will prove Theorem 2.

Let $\mathcal{V} = \bigcap_p \mathcal{V}_p$ be the set of all $v \in V_{\mathbb{Z}}$ corresponding to maximal cubic rings that are nowhere totally ramified (as in Sect. 4). Then by Lemma 19, we have $\mu(\mathcal{V}_p) = (1-p^{-2})^2$. By the same argument as in the proof of the main term of Theorem 3,

$$\lim_{X\to\infty}\frac{N(\mathcal{V}\cap V_{\mathbb{Z}}^{(i)};X)}{X} = \frac{\pi^2}{12n_i}\prod\big[\big(1-p^{-2}\big)^2\big] = \frac{3}{n_i\pi^2}.$$

Now given a nowhere totally ramified cubic field K_3, we have observed earlier that in the Galois closure K_6 is contained a quadratic field K_2 and K_6/K_2 is unramified. In addition, the discriminant of K_2 is equal to the discriminant of K_3. Furthermore, by class field theory the number of triplets of cubic fields K_3 corresponding to a given K_2 in this way equals $(h_3^*(K_2)-1)/2$, where $h_3^*(K_2)$ denotes the number of 3-torsion elements in the class group of K_2. Therefore,

$$\begin{aligned}\sum_{0<\mathrm{Disc}(K_2)<X}\big(h_3^*(K_2)-1\big)/2 &= N\big(\mathcal{V}\cap V_{\mathbb{Z}}^{(0)};X\big),\\ \sum_{-X<\mathrm{Disc}(K_2)<0}\big(h_3^*(K_2)-1\big)/2 &= N\big(\mathcal{V}\cap V_{\mathbb{Z}}^{(1)};X\big).\end{aligned}\tag{59}$$

Since it is known that

$$\begin{aligned}\lim_{X\to\infty}\frac{\sum_{0<\mathrm{Disc}(K_2)<X}1}{X}&=\frac{3}{\pi^2},\\ \lim_{X\to\infty}\frac{\sum_{-X<\mathrm{Disc}(K_2)<0}1}{X}&=\frac{3}{\pi^2},\end{aligned}\tag{60}$$

we conclude

$$\begin{aligned}\lim_{X\to\infty}\frac{\sum_{0<\mathrm{Disc}(K_2)<X}h_3^*(K_2)}{\sum_{0<\mathrm{Disc}(K_2)<X}1}&=1+2\lim_{X\to\infty}\frac{N(\mathcal{V}\cap V_{\mathbb{Z}}^{(0)};X)}{\sum_{0<\mathrm{Disc}(K_2)<X}1}\\ &=1+\frac{2\cdot 3/6\pi^2}{3/\pi^2}=\frac{4}{3},\\ \lim_{X\to\infty}\frac{\sum_{-X<\mathrm{Disc}(K_2)<0}h_3^*(K_2)}{\sum_{-X<\mathrm{Disc}(K_2)<0}1}&=1+2\lim_{X\to\infty}\frac{N(\mathcal{V}\cap V_{\mathbb{Z}}^{(1)};X)}{\sum_{-X<\mathrm{Disc}(K_2)<0}1}\\ &=1+\frac{2\cdot 3/2\pi^2}{3/\pi^2}=2.\end{aligned}$$

9 A refined sieve, and proofs of Theorems 3, 4, and 7

As we have seen, an integral binary cubic form corresponds to a maximal ring if and only if its coefficients satisfy certain congruence conditions modulo p^2 for each prime p. To prove Theorem 3 using Theorem 27, we require a suitable sieve as follows. Recall that for each prime p, we defined $\mathcal{W}_p$ to be the set of binary cubic forms corresponding to cubic rings that are non-maximal at p, and $\mathcal{Z}_p$ to be the set of binary cubic forms corresponding to cubic rings that are non-maximal at p, or are maximal at p but in which p is totally ramified. For a squarefree integer n, define $\mathcal{W}_n = \bigcap_{p|n} \mathcal{W}_p$ and $\mathcal{Z}_n = \bigcap_{p|n} \mathcal{Z}_p$. Then the number of isomorphism classes of maximal cubic orders having absolute discriminant in the dyadic range $X/2$ to X is equal to

$$N\big(\mathcal{U} \cap V_{\mathbb{Z}}^{(i)}; X/2, X\big) = \sum_{n \in \mathbb{N}} \mu(n) N\big(\mathcal{W}_n \cap V_{\mathbb{Z}}^{(i)}; X/2, X\big) \tag{61}$$

and the number of isomorphism classes of nowhere totally ramified maximal cubic orders in the range $X/2$ to X is equal to

$$N(\mathcal{V} \cap V_{\mathbb{Z}}^{(i)}; X/2, X) = \sum_{n \in \mathbb{N}} \mu(n) N(\mathcal{Z}_n \cap V_{\mathbb{Z}}^{(i)}; X/2, X). \tag{62}$$

We focus our discussion on the first sieve, the second sieve being treated in an analogous manner. In order to prove Theorem 3, we need to estimate the individual terms on the right hand side of (61) accurately. The difficulty lies in the fact that the sets $\mathcal{W}_n$ are defined by congruence conditions modulo n^2. We are then not able to directly apply Theorem 27, due to the fact that the $\mathcal{W}_n$ is the union of a large number of lattices modulo n^2. In Sect. 9.1, we show how to transform this count to one over fewer lattices defined by congruence conditions modulo n, thus enabling us to use Theorem 27 more effectively.

We then split (61) into three ranges for n and use a different method on each range. We use the splitting of the discriminant range into dyadic ranges so that we may choose the three ranges for n depending on the dyadic range of the discriminant. When n is small, we use Theorem 27 together with an identity proven in Sect. 9.1 to evaluate $N(\mathcal{W}_n; X/2, X)$ with two main terms and a smaller error term. Meanwhile, when n gets very large we apply the uniformity estimates from [4, Lemma 2.7] to bound the size of $|N(\mathcal{W}_n; X/2, X)|$. Lastly, when n is around $X^{1/6}$ it turns out that Theorem 27 and [4, Lemma 2.7] do not suffice, and so we require a different argument. We use again the correspondence of Sect. 9.1 to reduce the problem to one of determining the main term for the weighted count of binary cubic forms having bounded discriminant, where each binary cubic form is weighted by the number of its roots in $\mathbb{P}^1(\mathbb{Z}/n\mathbb{Z})$. To accomplish this count, we us an equidistribution argument, carried out in Sect. 9.4. We then complete the proof of Theorem 3 in Sect. 9.5.

In Sect. 9.6, we prove Theorem 4 in a very similar manner to the proof of Theorem 3. Finally, in Sect. 9.7, we prove Theorem 7 by expressing the second terms that arise in the count of isomorphism classes of cubic rings of bounded discriminant satisfying specified local conditions in terms of local masses of cubic rings.

9.1 Two useful identities

For $\alpha \in \mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$, define $V_{p,\alpha}$ to be the set of all integer binary cubic forms $f \in V_{\mathbb{Z}}$ such that $f \pmod p$ has a root at α, and $V_{p,\alpha}^2$ the set of all integer binary cubic forms $f \in V_{\mathbb{Z}}$ such that $f \pmod p$ has at least a double root at α. Note that although $V_{p,\alpha}$ and $V_{p,\alpha}^2$ are not $\mathrm{GL}_2(\mathbb{Z})$-invariant, the unions $\bigcup_\alpha V_{p,\alpha}$ and $\bigcup_\alpha V_{p,\alpha}^2$ are each $\mathrm{GL}_2(\mathbb{Z})$-invariant.

Our sieve makes use of the following proposition which contains two essential identities:

Proposition 33 *We have*

$$N(\mathcal{W}_p; X) = \sum_{\alpha \in \mathbb{P}^1(\mathbb{F}_p)} N\big(V_{p,\alpha}; X/p^2\big) - \sum_{\alpha \in \mathbb{P}^1(\mathbb{F}_p)} N\big(V_{p,\alpha}; X/p^4\big) + N\big(V_{\mathbb{Z}}; X/p^4\big); \tag{63}$$

$$N(\mathcal{Z}_p; X) = \sum_{\alpha \in \mathbb{P}^1(\mathbb{F}_p)} N\big(V_{p,\alpha}; X/p^2\big) + N\big(T_p(1^3); X\big) - \sum_{\alpha \in \mathbb{P}^1(\mathbb{F}_p)} N\big(V_{p,\alpha}^2; X/p^2\big) + N\big(V_{\mathbb{Z}}; X/p^4\big). \tag{64}$$

Proof To prove (63), we count isomorphism classes of pairs (R, R') of cubic rings such that $R \subset R'$ with $[R' : R] = p$ and $\mathrm{Disc}(R) < X$. We count these in two ways, namely, by R and by R'.

First, in order to count pairs (R, R') by R, recall from Proposition 16 that, for any integral binary cubic form $f \in \mathcal{W}_p \setminus p \cdot V_{\mathbb{Z}}$, the ring $R = R(f)$ is contained in a unique ring $R' \subset R \otimes \mathbb{Q}$ such that $[R' : R] = p$. Meanwhile, if $f = pg \in p \cdot V_{\mathbb{Z}}$, then R sits inside $\omega_p(g)$ rings $R' \subset R \otimes \mathbb{Q}$ with $[R' : R] = p$, where we use $\omega_p(g)$ to denote the number of roots in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ of $g \pmod p$. It follows that the total number of pairs (R, R') is

$$N(\mathcal{W}_p; X) - N\big(V_{\mathbb{Z}}; X/p^4\big) + \sum_{\alpha \in \mathbb{P}^1(\mathbb{F}_p)} N\big(V_{p,\alpha}; X/p^4\big). \tag{65}$$

The third term on the right hand side of the above expression counts those pairs $(R = R(f), R')$ that correspond to integer binary cubic forms $f = pg \in pV_{\mathbb{Z}}$.

We now count the number of pairs (R, R') by R'. Recall by Proposition 15 that for any binary cubic form f, the cubic ring $R' = R(f)$ has precisely $\omega_p(f)$ subrings R of index p. Therefore, since R' is constrained by $\mathrm{Disc}(R') = \mathrm{Disc}(R)/p^2 < X/p^2$, we see then that the total number of pairs

(R, R') is given by

$$\sum_{\alpha\in\mathbb{P}^1(\mathbb{F}_p)} N\big(V_{p,\alpha}; X/p^2\big). \tag{66}$$

Equating (65) and (66) yields the identity (63).

To prove (64), we begin by deriving a formula for $N(\mathcal{W}_p \cap T_p(1^3); X)$. To this end, we count now isomorphism classes of pairs (R, R') of cubic rings such that $R \subset R'$ with $[R' : R] = p$ and $\mathrm{Disc}(R) < X$, where furthermore R has splitting type $(1^2 1)$ at p. We again count these in two ways, namely, by R and by R'.

First, we note that if R has splitting type $(1^2 1)$ at p, and $R = R(f)$, then $R' \subset R \otimes \mathbb{Q}$ is uniquely determined and is primitive at p; moreover, if we write $R' = R(f')$, then f' (mod p) has a distinguished simple root in $\mathbb{P}^1(\mathbb{F}_p)$. Conversely, if $R' = R(f)$, where f (mod p) has a simple root in $\mathbb{P}^1(\mathbb{F}_p)$, then any subring R of index p will have splitting type $(1^2 1)$ at p. It follows that the number of desired pairs (R, R') is

$$N\big(\mathcal{W}_p \cap T_p\big(1^2 1\big); X\big) = \sum_{\alpha\in\mathbb{P}^1(\mathbb{F}_p)} N\big(V_{p,\alpha}; X/p^2\big) - \sum_{\alpha\in\mathbb{P}^1(\mathbb{F}_p)} N\big(V^2_{p,\alpha}; X/p^2\big) \tag{67}$$

where we have counted such pairs (R, R') by R on the left and by R' on the right. Noting that

$$N(\mathcal{W}_p; X) = N\big(\mathcal{W}_p \cap T_p\big(1^2 1\big); X\big) + N\big(\mathcal{W}_p \cap T_p\big(1^3\big); X\big) + N(pV_{\mathbb{Z}}; X), \tag{68}$$

together with (63) and (67), yields the following identity:

$$N\big(\mathcal{W}_p \cap T_p\big(1^3\big); X\big) = \sum_{\alpha\in\mathbb{P}^1(\mathbb{F}_p)} N\big(V^2_{p,\alpha}; X/p^2\big) - \sum_{\alpha\in\mathbb{P}^1(\mathbb{F}_p)} N\big(V_{p,\alpha}; X/p^4\big). \tag{69}$$

Since we know that

$$N(\mathcal{Z}_p; X) = N(\mathcal{W}_p; X) + N\big(T_p\big(1^3\big); X\big) - N\big(\mathcal{W}_p \cap T_p\big(1^3\big); X\big),$$

we obtain (64). □

For any squarefree $n \in \mathbb{N}$ and $\alpha \in \mathbb{P}^1(\mathbb{Z}/n\mathbb{Z})$, let $V_{n,\alpha}$ denote the set of all integral binary cubic forms $f \in V_{\mathbb{Z}}$ such that the reduction of f (mod n) has a root at α, and $V^2_{n,\alpha}$ the set of all integral binary cubic forms $f \in V_{\mathbb{Z}}$ such that the reduction of f (mod p) has at least a double root at the reduction of α (mod p) for all primes p dividing n.

Then the above analysis generalizes in a straightforward way to squarefree integers n to give

$$N(\mathcal{W}_n; X) = \sum_{\substack{k,\ell,m\in\mathbb{Z}_{\geq 0}\\ k\ell m=n\\ \alpha\in\mathbb{P}^1(\mathbb{Z}/k\ell\mathbb{Z})}} \mu(\ell) N\left(V_{k\ell,\alpha}; \frac{X}{k^2\ell^4 m^4}\right)$$

$$= \sum_{\substack{k,\ell\in\mathbb{Z}_{\geq 0}\\ k\ell\mid n\\ \alpha\in\mathbb{P}^1(\mathbb{Z}/k\ell\mathbb{Z})}} \mu(\ell) N\left(V_{k\ell,\alpha}; \frac{Xk^2}{n^4}\right); \tag{70}$$

$$N(\mathcal{Z}_n; X) = \sum_{\substack{k,\ell,m,q\in\mathbb{Z}_{\geq 0}\\ k\ell mq=n\\ \alpha\in\mathbb{P}^1(\mathbb{Z}/k\ell\mathbb{Z})}} \mu(\ell) N\left(V_{k,\alpha}\cap V_{\ell,\alpha}^2 \cap T_q\big(1^3\big); \frac{X}{k^2\ell^2 m^4}\right). \tag{71}$$

9.2 Back to the sieve

Let us define the error functions $E_n^{(i)}(X)$ and $E_n^{(i)}(X/2, X)$ for squarefree n by

$$E_n^{(i)}(X) = N\big(\mathcal{W}_n \cap V_{\mathbb{Z}}^{(i)}; X\big) - \big(\gamma_1(n) c_1^{(i)} X + \gamma_2(n) c_2^{(i)} X^{5/6}\big),$$

$$E_n^{(i)}(X/2, X) = N\big(\mathcal{W}_n \cap V_{\mathbb{Z}}^{(i)}; X/2, X\big) - \left(\frac{\gamma_1(n)}{2} c_1^{(i)} X + \big(1 - 2^{-5/6}\big)\gamma_2(n) c_2^{(i)} X^{5/6}\right), \tag{72}$$

where $\gamma_1(n)$ and $\gamma_2(n)$ are defined by the conditions $\gamma_1(p) + \mu_1(p) = \gamma_2(p) + \mu_2(p) = 1$ for $n = p$ prime, and $\gamma_1(n) = \prod_{p\mid n} \gamma_1(p)$ and $\gamma_2(n) = \prod_{p\mid n} \gamma_2(p)$ for general squarefree n. Returning to (61), we write

$$N\big(\mathcal{U} \cap V_{\mathbb{Z}}^{(i)}; X/2, X\big) = \sum_{n\in\mathbb{N}} \mu(n) N\big(\mathcal{W}_n \cap V_{\mathbb{Z}}^{(i)}; X/2, X\big)$$

$$= \sum_{n\in\mathbb{N}} \mu(n) \left(\frac{\gamma_1(n)}{2} c_1^{(i)} X + \big(1 - 2^{-5/6}\big)\gamma_2(n) c_2^{(i)} X^{5/6}\right)$$

$$+ \sum_{n\in\mathbb{N}} \mu(n) E_n^{(i)}(X/2, X)$$

$$= \frac{c_1^{(i)} X}{2\zeta(2)\zeta(3)} + \big(1 - 2^{-5/6}\big) \frac{c_2^{(i)} X^{5/6}}{\zeta(2)\zeta(5/3)}$$

$$+\sum_{n\in\mathbb{N}}\mu(n)E_n^{(i)}(X/2,X).$$

Thus to prove Theorem 3, it is sufficient prove the estimate

$$\sum_{n\in\mathbb{N}}\big|E_n^{(i)}(X/2,X)\big| = O_\epsilon\big(X^{5/6-1/48+\epsilon}\big). \tag{73}$$

Fix small numbers $\delta_1, \delta_2 > 0$ to be determined later. We break up (73) into the three different ranges

$$0 \le n \le X^{1/6-\delta_1}, \qquad X^{1/6-\delta_1} \le n \le X^{1/6+\delta_2}, \quad \text{and} \quad X^{1/6+\delta_2} \le n$$

and estimate $\sum_n |E_n^{(i)}(X/2,X)|$ for n in each range separately.

9.3 The small and large ranges

Suppose n is a fixed positive integer. Let k, ℓ be positive integers such that $k\ell \mid n$ and let $\alpha \in \mathbb{P}^1(\mathbb{Z}/k\ell\mathbb{Z})$. Then, by Theorem 27, there exist constants $c_1^{(i)}(\alpha)$ and $c_2^{(i)}(\alpha)$ such that

$$N\left(V_{k\ell,\alpha}\cap V_{\mathbb{Z}}^{(i)}; \frac{Xk^2}{2n^4}, \frac{Xk^2}{n^4}\right) = c_1^{(i)}(\alpha)\frac{Xk^2}{2n^4} + \big(1-2^{-5/6}\big)c_2^{(i)}(\alpha)\left(\frac{Xk^2}{n^4}\right)^{5/6} + O_\epsilon\left(\frac{T_1^{1/3}X^{3/4+\epsilon}k^{3/2}}{n^3}\right) \tag{74}$$

where, in the notation of Theorem 27, $T_1 = T_1(k,\ell,\alpha)$ is an integer dividing $k\ell$ which depends only on the lattice $V_{k\ell,\alpha}$. Now, if a lattice $V_{k\ell,\alpha}$ satisfies $T_1(k,\ell,\alpha) = d$, then by the definition of T_1, the image of α in $\mathbb{P}^1(\mathbb{Z}/d\mathbb{Z})$ must be 0. Hence, the number of choices for α is $O((k\ell/d)^{1+\epsilon})$. Since the total number of (k,ℓ) such that $k\ell$ divides n is $O(n^\epsilon)$, we conclude that the number of lattices $V_{k\ell,\alpha}$ satisfying $T_1(k,\ell,\alpha) = d$ is bounded by $O(n^{1+\epsilon}/d)$. Therefore, from (70), (72), and (74), we see that

$$|E_n^{(i)}(X/2,X)| = O_\epsilon\left(\sum_{d\mid n}\frac{n^{1+\epsilon}d^{1/3}X^{3/4+\epsilon}}{dn^{3/2}}\right) = O_\epsilon\left(\frac{X^{3/4+\epsilon}}{n^{1/2-\epsilon}}\right).$$

Summing over n, we conclude that

$$\sum_{n=0}^{X^{1/6-\delta_1}} |E_n^{(i)}(X/2,X)| = O_\epsilon\big(X^{5/6-\delta_1/2+\epsilon}\big). \tag{75}$$

From the definitions of γ_1 and γ_2, and from (56), we have the estimates

$$\gamma_1(n) = O_\epsilon\bigl(n^{-2+\epsilon}\bigr) \quad \text{and} \quad \gamma_2(n) = O_\epsilon\bigl(n^{-5/3+\epsilon}\bigr). \tag{76}$$

Let $q(n)$ denote the number of prime divisors of n. The next lemma follows from [4, Lemmas 2.7 and 3.3]:

Lemma 34 *For a square-free integer n, we have*

$$N(\mathcal{Z}_n; X) = O\bigl(3^{q(n)} X/n^2\bigr).$$

Thus we also have the estimate

$$N(\mathcal{W}_n; X) = O_\epsilon\bigl(X/n^{2-\epsilon}\bigr).$$

We deduce that

$$|E_n^{(i)}(X/2, X)| = O_\epsilon\bigl(X/n^{2-\epsilon}\bigr) + O_\epsilon\bigl(X^{5/6}/n^{5/3-\epsilon}\bigr),$$

and summing up over n we obtain

$$\sum_{n \geq X^{1/6+\delta_2}} \bigl|E_n^{(i)}(X/2, X)\bigr| = O_\epsilon\bigl(X^{5/6-\delta_2+\epsilon}\bigr) + O_\epsilon\bigl(X^{13/18-2\delta_2/3+\epsilon}\bigr). \tag{77}$$

In the next section, we estimate the sum of $|E_n^{(i)}(X/2, X)|$ over the range $X^{1/6-\delta_1} \leq n \leq X^{1/6+\delta_2}$.

9.4 An equidistribution argument

We now concentrate on the middle range $X^{1/6-\delta_1} \leq n \leq X^{1/6+\delta_2}$. Let us write

$$N\bigl(\mathcal{W}_n \cap V_{\mathbb{Z}}^{(i)}; X\bigr) = \sum_{k\ell \mid n} \mu(m) S_{k\ell}^{(i)}\bigl(Xk^2/n^4\bigr), \tag{78}$$

where

$$S_n^{(i)}(X) = \sum_{\alpha \in \mathbb{P}^1(\mathbb{Z}/n\mathbb{Z})} N\bigl(V_{n,\alpha} \cap V_{\mathbb{Z}}^{(i)}, X\bigr).$$

In this section, we estimate $S_n^{(i)}(X)$, and then use (72) and (78) to obtain a corresponding estimate on $E_n^{(i)}(X/2, X)$. Given a form f, let $w_n(f)$ denote as before the number of roots in $\mathbb{P}^1(\mathbb{Z}/n\mathbb{Z})$ of f (mod n). Then the number $S_n^{(i)}(X)$ counts the number of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of irreducible binary cubic forms in $V_{\mathbb{Z}}^{(i)}$, weighted by $w_n(f)$, having discriminant bounded by X. Thus

$$S_n^{(i)}(X) = \sum_{\substack{f \in \mathrm{GL}_2(\mathbb{Z}) \backslash V_{\mathbb{Z}}^{\mathrm{irr}} \\ |\mathrm{Disc}(f)| \leq X}} w_n(f). \tag{79}$$

We now consider $w_n(f)$ as a function on $V_{\mathbb{Z}/n\mathbb{Z}}$ and bound its Fourier transform pointwise. This in turn will allow us to count the number of binary cubic forms f, weighted by $w_n(f)$, in small boxes (boxes with each side length at least $n^{3/4+\epsilon}$). We then can count this weighted number of binary cubic forms in fundamental domains using the ideas of Sect. 5, yielding the desired estimate for $S_n^{(i)}(X)$, and therefore for $|E_n^{(i)}(X/2, X)|$.

Define $\widehat{V_{\mathbb{Z}}/nV_{\mathbb{Z}}}$ to be the space of additive characters $\chi : V_{\mathbb{Z}}/nV_{\mathbb{Z}} \to \mathbb{C}^{\times}$. Then we define the Fourier transform $\widehat{g} : \widehat{V_{\mathbb{Z}}/nV_{\mathbb{Z}}} \to \mathbb{C}$ of a function $g : V_{\mathbb{Z}}/nV_{\mathbb{Z}} \to \mathbb{C}$ via

$$\widehat{g}(\chi) := n^{-4} \sum_{v \in V_{\mathbb{Z}}/nV_{\mathbb{Z}}} g(v)\chi(v).$$

Fourier inversion then states that

$$g(v) = \sum_{\chi \in \widehat{V_{\mathbb{Z}}/nV_{\mathbb{Z}}}} \hat{g}(\chi)\bar{\chi}(v).$$

We focus now on computing $\widehat{w_n}(\chi)$. Assume first that $n = p$ is prime. We start with the trivial character which maps all of $V_{\mathbb{Z}}/pV_{\mathbb{Z}}$ to 1, which we denote by **Id**. Then

$$\widehat{w_p}(\mathbf{Id}) = p^{-4} \sum_{v \in V_{\mathbb{Z}}/pV_{\mathbb{Z}}} w_p(v) = 1 + p^{-1}.$$

Now for any $\chi \neq \mathbf{Id}$, we compute

$$\begin{aligned} \widehat{w_p}(\chi) &= p^{-4} \sum_{v \in V_{\mathbb{Z}}/pV_{\mathbb{Z}}} \chi(v) w_p(v) \\ &= p^{-4} \sum_{v:\chi(v)=1} w_p(v) + p^{-4} \sum_{v:\chi(v)\neq 1} w_p(v)\chi(v). \end{aligned} \tag{80}$$

Since $\chi(v) = 1$ for p^3 values of v and $w_p(v) \leq 3$ for $v \neq 0$, we have the estimate

$$\sum_{v:\chi(v)=1} w_p(v) \leq 3\big(p^3 - 1\big) + (p+1) = 3p^3 + p - 2. \tag{81}$$

Because $w_p(\lambda v) = w_p(v)$ for any $\lambda \in \mathbb{F}_p^\times$, we see that if $\chi(v) \neq 1$ then

$$\sum_{\lambda \in \mathbb{F}_p^\times} w_p(\lambda v)\chi(\lambda v) = -w_p(v),$$

implying

$$\sum_{v:\chi(v)\neq 1} w_p(v)\chi(v) = -(p-1)^{-1} \sum_{v:\chi(v)\neq 1} w_p(v). \tag{82}$$

Combining (81) with (82), we see that (80) implies that

$$\widehat{w_p}(\chi) \ll p^{-1} \tag{83}$$

uniformly for $\chi \neq 0$.

Now let n be a general squarefree integer. Then $\widehat{V_{\mathbb{Z}}/nV_{\mathbb{Z}}} \cong \bigoplus_{p|n} \widehat{V_{\mathbb{Z}}/pV_{\mathbb{Z}}}$ and $w_n(f) = \prod_{p|n} w_p(f)$. From this we conclude that $\widehat{w_n}(\chi) = \prod_{p|n} \widehat{w_p}(\chi_p)$, where χ_p is the p-part of χ. Using this and (83) implies that

$$\widehat{w_n}(\chi) \ll \prod_{\substack{p|n \\ \chi_p \neq \mathbf{Id}}} p^{-1} \tag{84}$$

and also

$$\widehat{w_n}(\mathbf{Id}) = \prod_{p|n} \left(1 + p^{-1}\right) = \sigma(n)/n, \tag{85}$$

where $\sigma(n) = \sum_{d|n} d$ denotes as usual the sum-of-divisors function.

We now run through the argument in Sect. 5, counting integer binary cubic forms f weighted by $w_n(f)$. Identically as in (23), we have the following identity.

$$S_n^{(i)}(X) = \frac{1}{M_i} \int_{g \in N'(t)A'\Lambda} S_n^{(i)}(m, t, \lambda, X) t^{-2} dm\, d^\times t\, d^\times \lambda, \tag{86}$$

where

$$S_n^{(i)}(m, t, \lambda, X) := \sum_{x \in B(m,t,\lambda,X)} w_n(x).$$

To estimate $S_n^{(i)}(m, t, \lambda, X)$, we tile the set $B(m, t, \lambda, X)$ with boxes and count weighted integer cubic forms inside each box. We have the following two lemmas.

Lemma 35 *Suppose R is a region in $\mathbb{R}^4$ having volume C_1 and surface area C_2. Let N be a positive integer. Then there exists a set $R' \subset R$ having volume equal to $C_1 + O(N \cdot C_2)$ such that R' can be tiled with 4-dimensional boxes with all sides having length N.*

Proof We first tile $\mathbb{R}^4$ with boxes having side length equal to N. Then we place R inside $\mathbb{R}^4$ and take R' to be the union of those boxes which lie entirely inside R. The region $R \setminus R'$ is within distance N of the boundary of R. It is thus clear that the volume of R' is equal to $C_1 + O(N \cdot C_2)$. □

We now use (83) to establish the following quantitative equidistribution statement for $w_n(f)$ inside boxes having small sidelengths relative to n.

Lemma 36 *Let $\mathcal{B} \subset V_{\mathbb{R}}$ be a box with sides parallel to the coordinate axes on $V_{\mathbb{R}}$ formed by the coefficients of the cubic form (a, b, c, d) such that each side has length $N \leq n$. Then*

$$\sum_{v \in \mathcal{B} \cap V_{\mathbb{Z}}} w_n(v) = \frac{\sigma(n)}{n} \mathrm{Vol}(\mathcal{B}) + O_\epsilon\big(n^{3+\epsilon}\big).$$

Proof Since each side length of $\mathcal{B}$ has side length at most n, we can consider the set of lattice points in $\mathcal{B}$ as a subset $\mathcal{B}_n$ of $V_{\mathbb{Z}}/nV_{\mathbb{Z}}$. We then use Fourier inversion to write

$$\sum_{v \in \mathcal{B} \cap V_{\mathbb{Z}}} w_n(v) = \sum_{v \in \mathcal{B}_n} \sum_{\chi \in \widehat{V_{\mathbb{Z}}/nV_{\mathbb{Z}}}} \widehat{w_n}(\chi)\bar{\chi}(v) \tag{87}$$

$$= N^4 \widehat{w_n}(\mathbf{Id}) + \sum_{\substack{\chi \in \widehat{V_{\mathbb{Z}}/nV_{\mathbb{Z}}} \\ \chi \neq \mathbf{Id}}} \widehat{w_n}(\chi) \sum_{v \in \mathcal{B}_n} \chi(-v) + O(N^3). \tag{88}$$

There is a $v_0 \in V_{\mathbb{Z}}/nV_{\mathbb{Z}}$ such that $\mathcal{B}_n = \{(a_1, a_2, a_3, a_4) + v_0 \mid 0 \leq a_1, a_2, a_3, a_4 \leq N - 1\}$. For each χ, there are characters χ_i, for $1 \leq i \leq 4$, such that $\chi(a_1, a_2, a_3, a_4) = \prod_{i=1}^4 \chi_i(a_i)$. Then, up to an error of $O(N^3)$, we see that $\sum_{v \in \mathcal{B}_n} w_n(v)$ is equal to

$$N^4 \widehat{w_n}(\mathbf{Id}) + \sum_{\substack{\chi \in \widehat{V_{\mathbb{Z}}/nV_{\mathbb{Z}}} \\ \chi \neq \mathbf{Id}}} \widehat{w_n}(\chi) \sum_{v \in \mathcal{B}_n} \chi(-v)$$

$$= N^4 \frac{\sigma(n)}{n} + \sum_{\substack{\chi \in \widehat{V_{\mathbb{Z}}/nV_{\mathbb{Z}}} \\ \chi \neq \mathbf{Id}}} \widehat{w_n}(\chi)\chi(-v_0) \prod_{i=1}^{4} \sum_{a_i=0}^{N-1} \chi_i(-a_i). \tag{89}$$

We estimate the sum over each $\chi \neq \mathbf{Id}$ separately. By (84), we know $|\widehat{w_n}(\chi)| \ll \prod_{\substack{p|n \\ \chi_p \neq \mathbf{Id}}} p^{-1}$. Now, for a character ψ of $\mathbb{Z}/n\mathbb{Z}$, we define $A_N(\psi)$ by

$$A_N(\psi) := \sum_{a=0}^{N-1} \psi(a) = \begin{cases} N & \psi = \mathbf{Id} \\ \frac{1-\psi(N)}{1-\psi(1)} & \psi \neq \mathbf{Id} \end{cases}$$

and then define $A_N(\chi) := \prod_{i=1}^{4} A_N(\chi_i)$. This implies that $\sum_{\psi \in \widehat{\mathbb{Z}/n\mathbb{Z}}} |A_N(\psi)| \ll \sum_{k=1}^{n} \frac{n}{k} \ll n \log n$.

We now estimate the right hand side of (89) as follows:

$$\begin{aligned} &N^4 \frac{\sigma(n)}{n} + \sum_{\substack{\chi \in \widehat{V_{\mathbb{Z}}/nV_{\mathbb{Z}}} \\ \chi \neq \mathbf{Id}}} \widehat{w_n}(\chi)\chi(-v) \prod_{i=1}^{4} \sum_{a_i=0}^{N-1} \chi_i(-a_i) \\ &= N^4 \frac{\sigma(n)}{n} + O\Bigg(\sum_{\substack{\chi \in \widehat{V_{\mathbb{Z}}/nV_{\mathbb{Z}}} \\ \chi \neq \mathbf{Id}}} |A_N(\chi)\widehat{w_n}(\chi)| \Bigg) \\ &= N^4 \frac{\sigma(n)}{n} + O_\epsilon\big(n^{3+\epsilon}\big), \end{aligned}$$

where the last bound follows from

$$\begin{aligned} \sum_{\substack{\chi \in \widehat{V_{\mathbb{Z}}/nV_{\mathbb{Z}}} \\ \chi \neq \mathbf{Id}}} |A_N(\chi)\widehat{w_n}(\chi)| &\leq \sum_{\substack{d|n \\ 1<d}} d^{-1} \sum_{\substack{\chi \\ \chi_p \neq \mathbf{Id}\, \forall p|d \\ \chi_p = \mathbf{Id}\, \forall p\nmid d}} |A_N(\chi)| \\ &\leq \sum_{\substack{d|n \\ 1<d}} d^{-1} \Bigg(\Bigg(\sum_{\psi \in \widehat{\mathbb{Z}/d\mathbb{Z}}} |A_N(\psi)| \Bigg)^4 - N^4 \Bigg) \\ &\leq \sum_{\substack{d|n \\ 1<d}} d^{-1} \big((N + O(d \log d))^4 - N^4 \big) \\ &\leq \sum_{\substack{d|n \\ 1<d}} O_\epsilon\big(\max(d, N)^{3+\epsilon}\big) \\ &\leq O_\epsilon\big(n^{3+\epsilon}\big). \end{aligned}$$

This completes the proof of the lemma. □

We now estimate $S_n^{(i)}(m,t,\lambda,X)$ for $|m| < 1/2$. First, tile $B(m,t,\lambda,X)' \subset B(m,t,\lambda,X)$ with boxes using Lemma 35. Note that the region $B(m,t,\lambda,X)$ is obtained by acting on the region $B(1,1,1,\frac{X}{\lambda^4})$ by $m \cdot t \cdot \lambda \in \mathrm{GL}_2(\mathbb{R})$. So the surface area of $B(m,t,\lambda,X)$ is $O(\lambda^3 t^3)$. We thus have

$$S_n^{(i)}(m,t,\lambda,X) = \frac{\sigma(n)}{n}\mathrm{Vol}\big(B(m,t,\lambda,X)\big) + O_\epsilon\left(\frac{n^{3+\epsilon}\lambda^4}{N^4}\right) + O\big(\lambda^3 t^3 N\big), \tag{90}$$

where the first error term comes from Lemma 36 and the second comes from Lemma 35. We optimize by picking $N = \lambda^{1/5} t^{-3/5} n^{3/5}$. Using (90), as in Sect. 5, we evaluate the right hand side of (86) to obtain

$$S_n^{(i)}(X) = \frac{\sigma(n)}{n} c_1^{(i)} X + O_\epsilon\big(n^{3+\epsilon} + X^{5/6} n^{1/2}\big). \tag{91}$$

Using (70), (72), (76), and (91) we finally arrive at the bound

$$|E_n^{(i)}(X)| \le \gamma_2(n) X^{5/6} + O_\epsilon\big(n^\epsilon\big)\Bigg(\sum_{\substack{k,\ell\in\mathbb{Z}\\ k\ell|n}} (k\ell)^3 + \frac{X^{5/6}k^{5/3}}{n^{17/6}}\Bigg).$$

Therefore, we have

$$|E_n^{(i)}(X)| = O_\epsilon\big(n^\epsilon\big)\left(\frac{X^{5/6}}{n^{7/6}} + n^3\right)$$

implying

$$\sum_{n=X^{1/6-\delta_1}}^{X^{1/6+\delta_2}} |E_n^{(i)}(X)| = O_\epsilon\big(X^{29/36+\delta_1/6+\epsilon} + X^{2/3+4\delta_2+\epsilon}\big). \tag{92}$$

This also implies the estimate

$$\sum_{n=X^{1/6-\delta_1}}^{X^{1/6+\delta_2}} |E_n^{(i)}(X/2,X)| = O_\epsilon\big(X^{29/36+\delta_1/6+\epsilon} + X^{2/3+4\delta_2+\epsilon}\big). \tag{93}$$

9.5 Putting it together

We combine (75), (77) and (93) to obtain

$$\sum_{n\in\mathbb{Z}} |E_n^{(i)}(X/2,X)| \ll_\epsilon X^{5/6-\delta_1/2+\epsilon} + X^{5/6-\delta_2+\epsilon} + X^{13/18-2\delta_2/3+\epsilon}$$

$$+ X^{29/36+\delta_1/6+\epsilon} + X^{2/3+4\delta_2+\epsilon}.$$

We optimize by picking $\delta_1 = \frac{1}{24}$ and $\delta_2 = \frac{1}{30}$ to get

$$\sum_{n\in\mathbb{Z}} |E_n^{(i)}(X/2, X)| \ll_\epsilon X^{5/6-1/48+\epsilon},$$

which proves Theorem 3.

Finally, note that the values of $\mu_1(\sigma, p)$ and $\mu_2(\sigma, p)$ that we list in Table 1 are the same as the values of C_{p,α_p} and K_{p,α_p}, respectively, in [26, (5.1)]. We thus also obtain Roberts' refined conjecture (see [26, Sect. 5]); the proof is identical to the proof of Theorem 3.

9.6 Proof of Theorem 4

The proof of Theorem 4 is very similar to that of Theorem 3. This time, we define the error function $F_n^{(i)}(X/2, X)$ for squarefree n by

$$F_n^{(i)}(X/2, X) = N\big(\mathcal{Z}_n \cap V_{\mathbb{Z}}^{(i)}; X/2, X\big) - \left(\frac{\gamma_1'(n)}{2} c_1^{(i)} X + \big(1 - 2^{-5/6}\big)\gamma_2'(n) c_2^{(i)} X^{5/6}\right), \quad (94)$$

where $\gamma_1'(n)$ and $\gamma_2'(n)$ are defined by the conditions $\gamma_1'(p) + \mu_1'(p) = \gamma_2'(p) + \mu_2'(p) = 1$ for $n = p$ prime, and $\gamma_1'(n) = \prod_{p|n} \gamma_1'(p)$ and $\gamma_2'(n) = \prod_{p|n} \gamma_2'(p)$ for general squarefree n. We can write

$$\begin{aligned}
N\big(\mathcal{V} \cap V_{\mathbb{Z}}^{(i)}; X/2, X\big) &= \sum_{n\in\mathbb{N}} \mu(n) N\big(\mathcal{Z}_n \cap V_{\mathbb{Z}}^{(i)}; X/2, X\big) \\
&= \sum_{n\in\mathbb{N}} \mu(n) \left(\frac{\gamma_1'(n)}{2} c_1^{(i)} X + \big(1 - 2^{-5/6}\big)\gamma_2'(n) c_2^{(i)} X^{5/6}\right) \\
&\quad + \sum_{n\in\mathbb{N}} \mu(n) F_n^{(i)}(X/2, X) \\
&= \frac{c_1^{(i)} X}{2\zeta(2)\zeta(3)} + \big(1 - 2^{-5/6}\big)\frac{c_2^{(i)} X^{5/6}}{\zeta(2)\zeta(5/3)} \\
&\quad + \sum_{n\in\mathbb{N}} \mu(n) F_n^{(i)}(X/2, X).
\end{aligned}$$

Thus, to prove Theorem 4, it is sufficient prove the estimate

$$\sum_{n\in\mathbb{N}} |F_n^{(i)}(X/2, X)| = O_\epsilon\big(X^{5/6-1/48+\epsilon}\big). \quad (95)$$

Let $\delta_1, \delta_2 > 0$ be as in the previous subsection. Again, we break up (95) into the three different ranges

$$0 \le n \le X^{1/6-\delta_1}, \qquad X^{1/6-\delta_1} \le n \le X^{1/6+\delta_2}, \quad \text{and} \quad X^{1/6+\delta_2} \le n$$

and estimate $\sum_n |F_n^{(i)}(X/2, X)|$ for n in each range separately.

In (71), we write $N(\mathcal{Z}_n \cap V_{\mathbb{Z}}^{(i)}; X/2, X)$ as a sum over positive integers k, ℓ, m, q with $k\ell mq = n$. Let $k, \ell \in \mathbb{Z}_{>0}$ such that $k\ell|n$. Then, for $\alpha \in \mathbb{P}^1(\mathbb{Z}/k\ell\mathbb{Z})$, we may write $V_{k,\alpha} \cap V_{\ell,\alpha}^2 \cap T_q(1^3)$ as a union of $O(q^2)$ translates of lattices, each of which has index $k\ell^2q^4$ in $V_{\mathbb{Z}}$ and is defined via congruence conditions modulo $k\ell q$. The remark following Theorem 27 implies that for each of these lattice-translates $\mathcal{L}$ there exist constants $c_1^{(i)}(\mathcal{L})$ and $c_2^{(i)}(\mathcal{L})$ such that

$$\begin{aligned} N\left(\mathcal{L}; \frac{Xk^2\ell^2q^4}{2n^4}, \frac{Xk^2\ell^2q^4}{n^4}\right) &= c_1^{(i)}(\mathcal{L})\frac{Xk^2\ell^2q^4}{2n^4} \\ &\quad + \left(1-2^{-5/6}\right)c_2^{(i)}(\mathcal{L})\left(\frac{Xk^2\ell^2q^4}{n^4}\right)^{5/6} \\ &\quad + O_\epsilon\left(\frac{X^{3/4}k^{3/2}\ell^{1/2}}{n^3}\right). \end{aligned} \tag{96}$$

Since there are $O_\epsilon(n^\epsilon k\ell q^2)$ such lattices, we see that

$$|F_n^{(i)}(X/2, X)| = O_\epsilon\left(\sum_{n=kn_1} n^\epsilon \frac{X^{3/4}}{k^{1/2}\ell^{3/2}m^3q}\right) = O_\epsilon\left(\frac{X^{3/4}}{n^{1/2-\epsilon}}\right).$$

Summing over $n = kn_1$ in the small range, we conclude that

$$\sum_{n=1}^{X^{\frac{1}{6}-\delta_1}} |F_n^{(i)}(X/2, X)| = O_\epsilon\left(X^{5/6-\delta_1/2+\epsilon}\right). \tag{97}$$

As in Sect. 9.3, we may use Lemma 34 to estimate $\sum_n |F_n^{(i)}(X/2, X)|$ over n lying in the large range:

$$\sum_{n \ge X^{\frac{1}{6}+\delta_2}} |F_n^{(i)}(X/2, X)| = O_\epsilon\left(X^{5/6-\delta_2+\epsilon}\right) + O_\epsilon\left(X^{13/18-2\delta_2/3+\epsilon}\right). \tag{98}$$

We now consider the middle range. Fix k, ℓ, q, m such that $k\ell qm = n$. For $\beta \in \mathbb{P}^1(\mathbb{Z}/\ell\mathbb{Z})$, we may write $V_{\ell,\beta}^2 \cap T_p(1^3)$ as a union of $O(p^2\ell^2)$ translates of $p\ell V_{\mathbb{Z}}$. Let $\mathcal{L}$ be one of them. Identically to Sect. 9.4, using equation (91) we have:

$$\sum_{\alpha \in \mathbb{P}^1(\mathbb{Z}/k\mathbb{Z})} N\left(V_{\mathbb{Z}}^{(i)} \cap V_{k,\alpha} \cap \mathcal{L}; \frac{X}{k^2\ell^2 m^4}\right)$$
$$= c^{(i)}(\mathcal{L})X + O_\epsilon\left(k^{3+\epsilon} + k^{1/2}\left(\frac{X}{k^2\ell^6 m^4 p^4}\right)^{\frac{5}{6}}\right),$$

where $c(\mathcal{L})$ is some explicit constant. It follows, just as in Sect. 9.4, that

$$\sum_{n=X^{1/6-\delta_1}}^{X^{1/6+\delta_2}} |F_n^{(i)}(X/2, X)| \ll_\epsilon X^{29/36+\frac{\delta_1}{6}+\epsilon} + X^{2/3+4\delta_2+\epsilon}. \quad (99)$$

Finally, note that

$$\sum_{0<\mathrm{Disc}(K_2)<X} 1 = \frac{3}{\pi^2} \cdot X + O\left(X^{\frac{1}{2}}\right);$$
$$\sum_{-X<\mathrm{Disc}(K_2)<0} 1 = \frac{3}{\pi^2} \cdot X + O\left(X^{\frac{1}{2}}\right). \quad (100)$$

Theorem 4 may now be deduced from (97), (98), and (99) (together with (59) and (100)) just as Theorem 3 was deduced in Sect. 9.5 from (75), (77), and (93).

9.7 Another simultaneous generalization

In this subsection, we prove Theorem 7.

Proof of Theorem 7 Let p be a fixed finite prime. If $R \in \Sigma_p$ is a cubic ring over $\mathbb{Z}_p$, then we define $V(R) \subset V_{\mathbb{Z}}$ to be the set of all integer binary cubic forms f such that the corresponding cubic ring C satisfies $C \otimes \mathbb{Z}_p \cong R$. As in Sect. 7, we define $\mu_1(R, p)$ and $\mu_2(R, p)$ to be such that

$$N\left(V(R) \cap V_{\mathbb{Z}}^{(i)}; X\right) = \mu_1(R, p)c_1^{(i)}X + \mu_2(R, p)c_2^{(i)}X^{5/6} + O_\epsilon\left(X^{3/4+\epsilon}\right).$$

Using the same techniques as in the proofs of Theorems 3 and 4, we have

$$N(\Sigma; X) = \left(\frac{1}{2}\sum_{R\in\Sigma_\infty} \frac{1}{|\mathrm{Aut}_{\mathbb{R}}(R)|}\right) \cdot \prod_p \left(\sum_{R\in\Sigma_p} \mu_1(R, p)\right) \cdot \zeta(2) \cdot X$$

$$+\Big(\sum_{R\in\Sigma_\infty} c_2(R)\Big)\cdot\prod_p\Big(\sum_{R\in\Sigma_p}\mu_2(R,p)\Big)\cdot X^{5/6} + O_\epsilon\big(X^{5/6-1/48+\epsilon}\big). \tag{101}$$

We now prove the following lemma:

Lemma 37 *With notation as above, we have*

$$\mu_2(R,p)=\big(1-p^{-2}\big)\big(1-p^{-1/3}\big) \times\left(\frac{1}{\mathrm{Disc}_p(R)}\cdot\frac{1}{|\mathrm{Aut}(R)|}\int_{(R/\mathbb{Z}_p)^{\mathrm{Prim}}} i(x)^{2/3}dx\right).$$

Proof Fix a form $f\in V_{\mathbb{Z}_p}$ corresponding to R. Let m be a positive integer such that p^m is larger than $\mathrm{Disc}_p(R)$, so that in particular $\mathrm{Disc}(f)\not\equiv 0 \pmod{p^m}$. Let $F=\{f_1,f_2,\ldots,f_r\}$ be the $\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})$-orbit of the reduction of $f \pmod{p^m}$. By the slicing techniques of Sect. 6, as used in the proof of Theorem 27, we have

$$\mu_2(R,p)=p^{-3m}\cdot\left.\frac{\sum_{i=1}^r\sum_{a\equiv a(f_i)}a^{-s}}{\sum_{a\neq 0}a^{-s}}\right|_{s=1/3},$$

where $a(f_i)$ denotes the x^3-coefficient of f_i and the congruences are taken modulo p^m. Since F is $\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})$-invariant, every value of $a(f_i)$ with the same p-adic valuation occurs equally often in F. Therefore, we have

$$\mu_2(R,p)=(1-p^{-1/3})p^{-3m}\sum_{i=1}^r\begin{cases}\frac{p^{1-m}|a(f_i)|_p^{-2/3}}{p-1} & \text{if } a(f_i)\not\equiv 0 \pmod{p^m}\\ \frac{p^{-m/3}}{1-p^{-1/3}} & \text{if } a(f_i)\equiv 0 \pmod{p^m}.\end{cases} \tag{102}$$

The group $\mathrm{GL}_2(\mathbb{Z}_p)$ acts on f in the natural way. Normalizing the Haar measure so as to give $\mathrm{GL}_2(\mathbb{Z}_p)$ measure 1, we may rewrite (102) as

$$\mu_2(R,p)=\frac{(1-p^{-2})(1-p^{-1/3})}{|\mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})}(f)|}\cdot\int_{\mathrm{GL}_2(\mathbb{Z}_p)}|a(g\cdot f)|_p^{-2/3}dg.$$

The above equality holds since we are in the first case of (102) when m is sufficiently large, and

$$r=\#F=\frac{|\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})|}{|\mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})}(f)|}=\frac{p^{4m}(1-p^{-2})(1-p^{-1})}{|\mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})}(f)|}.$$

Now, by computing the measure of $\mathrm{GL}_2(\mathbb{Z}_p)\cdot f$ using two different methods, we obtain

$$|\mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})}(f)| = |\mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}_p)}(f)|\cdot \mathrm{Disc}_p(f).$$

The first method is by splitting $\mathrm{GL}_2(\mathbb{Z}_p)\cdot f$ into $p^m\cdot V_{\mathbb{Z}_p}$ cosets. The number of such cosets is exactly $|\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})|\cdot|\mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})}(f)|^{-1}$. The second method is by integrating over the group, and using that the left invariant measure on $V_{\mathbb{Z}_p}$ is $|\mathrm{Disc}(v)|^{-1}dv$ and the map $g\to g\cdot f$ is a $|\mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}_p)}(f)|$-to-1 cover.

We thus have

$$\mu_2(R,p)=\frac{(1-p^{-2})(1-p^{-1/3})}{\mathrm{Disc}_p(f)\cdot|\mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}_p)}(f)|}\cdot\int_{\mathrm{GL}_2(\mathbb{Z}_p)}|a(g\cdot f)|_p^{-2/3}dg.$$

Note that $a(g\cdot f)=f(v_0\cdot g)$ where $v_0=(1,0)\in\mathbb{Z}_p\times\mathbb{Z}_p$. Therefore, we have

$$\int_{\mathrm{GL}_2(\mathbb{Z}_p)}|a(g\cdot f)|_p^{-2/3}dg=\int_{(\mathbb{Z}_p^2)^{\mathrm{Prim}}}|f(v)|_p^{-2/3}dv,$$

where dv is normalized to have measure 1 on $(\mathbb{Z}_p^2)^{\mathrm{Prim}}$.

From the correspondence in Sect. 2, we see that the set $(\mathbb{Z}_p^2)^{\mathrm{Prim}}$ corresponds to $(R/\mathbb{Z}_p)^{\mathrm{Prim}}$ and that for $v\in(\mathbb{Z}_p^2)^{\mathrm{Prim}}$ corresponding to $x\in R$, the value of $f(v)$ is equal to the index of $\mathbb{Z}[x]$ in R. The lemma follows. □

Theorem 7 now follows from Theorem 31 and the above lemma. □

Acknowledgements We thank Mohammad Bardestani, Karim Belabas, Andrew Granville, Piper Harris, Carl Pomerance, Peter Sarnak, Christopher Skinner, Frank Thorne, Ila Varma, Melanie Wood, and the anonymous referees for helpful comments on earlier versions of this manuscript. We are also grateful to Boris Alexeev and Sucharit Sarkar for helping us compute the precise values of the second main terms.

References

1. Belabas, K.: A fast algorithm to compute cubic fields. Math. Comput. **66**(219), 1213–1237 (1997)
2. Belabas, K.: On the mean 3-rank of quadratic fields. Compos. Math. **118**(1), 1–9 (1999). Corrigendum: On the mean 3-rank of quadratic fields. Compos. Math. **140**, 1221 (2004)
3. Belabas, K., Fouvry, E.: Sur le 3-rang des corps quadratiques de discriminant premier ou presque premier. Duke Math. J. **98**(2), 217–268 (1999)
4. Belabas, K., Bhargava, M., Pomerance, C.: Error terms for the Davenport-Heilbronn theorems. Duke Math. J. **153**, 173–210 (2010)
5. Bhargava, M.: The density of discriminants of quartic rings and fields. Ann. Math. **162**, 1031–1063 (2005)

6. Bhargava, M.: Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants. Internat. Math. Res. Not. **2007**(17), rnm052 (2007), 20 pp.
7. Bhargava, M.: The density of discriminants of quintic rings and fields. Ann. Math. **172**, 1559–1591 (2010)
8. Bhargava, M., Shnidman, A.: On the number of cubic orders of bounded discriminant having automorphic group C_3, and related problems. Preprint
9. Bhargava, M., Stich, S.: On mass formulae for algebras over $\mathbb{F}_p$ and over $\mathbb{Z}_p$. In preparation
10. Bhargava, M., Wood, M.M.: The density of discriminants of S_3-sextic number fields. Proc. Am. Math. Soc. **136**(5), 1581–1587 (2008)
11. Datskovsky, B., Wright, D.J.: Density of discriminants of cubic extensions. J. Reine Angew. Math. **386**, 116–138 (1988)
12. Davenport, H.: On a principle of Lipschitz. J. Lond. Math. Soc. **26**, 179–183 (1951). Corrigendum: On a principle of Lipschitz. J. Lond. Math. Soc. **39**, 580 (1964)
13. Davenport, H.: On the class-number of binary cubic forms I. J. Lond. Math. Soc. **26**, 183–192 (1951). Corrigendum, ibidem, **27**, 512 (1952)
14. Davenport, H.: On the class-number of binary cubic forms II. J. Lond. Math. Soc. **26**, 192–198 (1951)
15. Davenport, H., Heilbronn, H.: On the density of discriminants of cubic fields II. Proc. R. Soc. Lond. Ser. A, Math. Phys. Sci. **322**(1551), 405–420 (1971)
16. Delone, B.N.: Solution of the problem of equivalence and tabulation of cubic binary forms with negative discriminant. Ž. Leningr. Fiz.-Mat. Obšč. **1**(1), 40–55 (1926). (Russian)
17. Delone, B.N., Faddeev, D.K.: The theory of irrationalities of the third degree. AMS Transl. Math. Monogr. **10** (1964)
18. Duke, W., Kowalski, E.: A problem of Linnik for elliptic curves and mean-value estimates for automorphic representations (with an appendix by Dinakar Ramakrishnan). Invent. Math. **139**(1), 1–39 (2000)
19. Fouvry, E., Katz, N.: A general stratification theorem for exponential sums, and applications. J. Reine Angew. Math. **540**, 115–166 (2001)
20. Fung, G.W., Williams, H.C.: On the computation of a table of complex cubic fields with discriminant $D > -10^6$. Math. Comput. **55**(191), 313–325 (1990)
21. Gan, W.-T., Gross, B.H., Savin, G.: Fourier coefficients of modular forms on G_2. Duke Math. J. **115**, 105–169 (2002)
22. Hilbert, D.: Theory of Algebraic Invariants. Cambridge University Press, Cambridge (1993). (Translated by R. Laubenbacher)
23. Knapp, A.W.: Lie groups beyond an introduction. 2nd edn. Progress in Mathematics, vol. 140. Birkhäuser, Boston (2002)
24. Levi, F.: Kubische Zahlkörper und binäre kubische Formenklassen. Sitz.ber. Sachs. Akad. Wiss. Leipz., Mat.-Nat. Kl. **66**, 26–37 (1914)
25. Llorente, P., Quer, J.: On totally real cubic fields with discriminant $D < 10^7$. Math. Comput. **50**(182), 581–594 (1988)
26. Roberts, D.P.: Density of cubic field discriminants. Math. Comput. **70**(236), 1699–1705 (2001) (electronic)
27. Sato, M., Shintani, T.: On zeta functions associated with prehomogeneous vector spaces. Ann. Math. (2) **100**, 131–170 (1974)
28. Serre, J.-P.: A Course in Arithmetic. Graduate Texts in Mathematics, vol. 7. Springer, New York (1973). (Translated from the French)
29. Serre, J.-P.: Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local. C. R. Acad. Sci. Paris Ser. A-B **286**(22), A1031–A1036 (1978)

30. Shintani, T.: On Dirichlet series whose coefficients are class-numbers of integral binary cubic forms. J. Math. Soc. Jpn. **24**, 132–188 (1972)
31. Taniguchi, T., Thorne, F.: Secondary terms in counting functions for cubic fields. Preprint
32. Vatsal, V.: Rank-one twists of a certain elliptic curve. Math. Ann. **311**, 791–794 (1998)
33. Wong, S.: Elliptic curves and class number divisibility. Internat. Math. Res. Notices **1999**(12), 661–672