Proc. London Math. Soc. (3) 112 (2016) 235–266
doi:10.1112/plms/pdv062

The mean number of 3-torsion elements in the class groups and ideal groups of quadratic orders

Manjul Bhargava and Ila Varma

Abstract

We determine the mean number of 3-torsion elements in the class groups of quadratic orders, where the quadratic orders are ordered by their absolute discriminants. Moreover, for a quadratic order $\mathcal{O}$ we distinguish between the two groups: $\mathrm{Cl}_3(\mathcal{O})$, the group of *ideal classes of order* 3; and $\mathcal{I}_3(\mathcal{O})$, the group of *ideals of order* 3. We determine the mean values of both $|\mathrm{Cl}_3(\mathcal{O})|$ and $|\mathcal{I}_3(\mathcal{O})|$, as $\mathcal{O}$ ranges over any family of orders defined by finitely many (or in suitable cases, even infinitely many) local conditions.

As a consequence, we prove the surprising fact that the mean value of the difference $|\mathrm{Cl}_3(\mathcal{O})| - |\mathcal{I}_3(\mathcal{O})|$ is equal to 1, regardless of whether one averages over the maximal orders in complex quadratic fields or over all orders in such fields or, indeed, over any family of complex quadratic orders defined by local conditions. For any family of real quadratic orders defined by local conditions, we prove similarly that the mean value of the difference $|\mathrm{Cl}_3(\mathcal{O})| - \frac{1}{3}|\mathcal{I}_3(\mathcal{O})|$ is equal to 1, independent of the family.

1. *Introduction*

In their classical paper [**9**], Davenport and Heilbronn proved the following theorem.

Theorem 1. *When quadratic fields are ordered by their absolute discriminants:*

(a) *The average number of* 3*-torsion elements in the class groups of imaginary quadratic fields is* 2*.*

(b) *The average number of* 3*-torsion elements in the class groups of real quadratic fields is* $\frac{4}{3}$*.*

This theorem yields the only two proven cases of the Cohen–Lenstra heuristics for class groups of quadratic fields.

In their paper [**5**, p. 59], Cohen and Lenstra raise the question as to what happens when one looks at class groups over *all orders*, rather than just the maximal orders corresponding to fields. The heuristics formulated by Cohen and Lenstra for class groups of quadratic fields are based primarily on the assumption that, in the absence of any known structure for these abelian groups beyond genus theory, we may as well assume that they are 'random' groups in the appropriate sense.

For orders, however, as pointed out by Cohen and Lenstra themselves [**5**], when an imaginary quadratic order is not maximal, there is an additional arithmetic constraint on the class group coming from the class number formula. Indeed, if $h(d)$ denotes the class number of the imaginary quadratic order of discriminant d, and if D is a (negative) fundamental discriminant,

Received 28 February 2014; revised 17 September 2014.

2010 *Mathematics Subject Classification* 11R11, 11R29, 11R45 (primary).

The first author was supported by the Packard and Simons Foundations and NSF Grant DMS-1001828. The second author was supported by a National Defense Science & Engineering Fellowship and an NSF Graduate Research Fellowship.

then the class number formula gives

$$h(Df^2) = \left[f \cdot \prod_{p|f} \left(1 - \frac{(D|p)}{p} \right) \right] h(D), \tag{1}$$

where $(\cdot|\cdot)$ denotes the Kronecker symbol. Thus, one would naturally expect that the percentage of quadratic orders having class number divisible by 3 should be strictly larger than the corresponding percentage for quadratic fields. Similarly, the average number of 3-torsion elements across all quadratic orders would also be expected to be strictly higher than the corresponding average for quadratic fields. (Note that the class number formula does not give complete information on the number of 3-torsion elements; indeed, extra factors of 3 in the class number may mean extra 3-torsion, but it could also mean extra 9-torsion or 27-torsion, etc.!)

In this article we begin by proving the latter statement, by determining the mean number of 3-torsion elements in the class groups of quadratic orders.

THEOREM 2. *When orders in quadratic fields are ordered by their absolute discriminants:*

(a) *The average number of* 3*-torsion elements in the class groups of imaginary quadratic orders is* $1 + \zeta(2)/\zeta(3)$.

(b) *The average number of* 3*-torsion elements in the class groups of real quadratic orders is* $1 + \frac{1}{3} \cdot \zeta(2)/\zeta(3)$.

Note that $\zeta(2)/\zeta(3) \approx 1.36843 > 1$.

More generally, we may consider the analogue of Theorem 2 when the average is taken not over all orders, but over some subset of orders defined by local conditions. More precisely, for each prime p, let Σ_p be any set of isomorphism classes of orders in étale quadratic algebras over $\mathbb{Q}_p$. We say that the collection (Σ_p) of local specifications is *acceptable* if, for all sufficiently large p, the set Σ_p contains all the maximal quadratic rings over $\mathbb{Z}_p$. Let Σ denote the set of quadratic orders $\mathcal{O}$, up to isomorphism, such that $\mathcal{O} \otimes \mathbb{Z}_p \in \Sigma_p$ for all p. Then we may ask what the mean number of 3-torsion elements in the class groups of imaginary (respectively, real) quadratic orders in Σ is.

To state such a result for general acceptable Σ, we need a bit of notation. For an étale cubic algebra K over $\mathbb{Q}_p$, we write $D(K)$ for the unique quadratic algebra over $\mathbb{Z}_p$ satisfying $\mathrm{Disc}(D(K)) = \mathrm{Disc}(K)$. Also, for an order R in an étale quadratic algebra over $\mathbb{Q}_p$, let $C(R)$ denote the weighted number of étale cubic algebras K over $\mathbb{Q}_p$ such that $R \subset D(K)$:

$$C(R) := \sum_{\substack{K \text{ étale cubic}/\mathbb{Q}_p \\ \text{s.t. } R \subset D(K)}} \frac{1}{\#\mathrm{Aut}(K)}. \tag{2}$$

We define the 'cubic mass' M_Σ of the family Σ as a product of local masses:

$$M_\Sigma := \prod_p \frac{\sum_{R \in \Sigma_p} C(R)/\mathrm{Disc}_p(R)}{\sum_{R \in \Sigma_p} (1/\#\mathrm{Aut}(R)) \cdot (1/\mathrm{Disc}_p(R))} = \prod_p \frac{\sum_{R \in \Sigma_p} C(R)/\mathrm{Disc}_p(R)}{\sum_{R \in \Sigma_p} 1/(2 \cdot \mathrm{Disc}_p(R))}, \tag{3}$$

where $\mathrm{Disc}_p(R)$ denotes the discriminant of R viewed as a power of p. We then prove the following generalization of Theorem 2.

THEOREM 3. *Let (Σ_p) be any acceptable collection of local specifications as above, and let Σ denote the set of all isomorphism classes of quadratic orders $\mathcal{O}$ such that $\mathcal{O} \otimes \mathbb{Z}_p \in \Sigma_p$ for all p. Then, when orders in Σ are ordered by their absolute discriminants:*

(a) *The average number of 3-torsion elements in the class groups of imaginary quadratic orders in Σ is $1 + M_\Sigma$.*

(b) *The average number of 3-torsion elements in the class groups of real quadratic orders in Σ is $1 + \frac{1}{3}M_\Sigma$.*

If Σ is the set of all orders in Theorem 3, then we show in Section 5 that $M_\Sigma = \zeta(2)/\zeta(3)$, and we recover Theorem 2; if Σ is the set of all maximal orders, then $M_\Sigma = 1$ and we recover Theorem 1. As would be expected, the mean number of 3-torsion elements in class groups of quadratic orders depends on which set of orders one is taking the average over. However, a remarkable consequence of Theorem 3 is the following generalization of Theorem 1.

COROLLARY 4. *Suppose one restricts to just those quadratic fields satisfying any specified set of local conditions at any finite set of primes. Then, when these quadratic fields are ordered by their absolute discriminants:*

(a) *The average number of 3-torsion elements in the class groups of such imaginary quadratic fields is 2.*

(b) *The average number of 3-torsion elements in the class groups of such real quadratic fields is $\frac{4}{3}$.*

Thus the mean number of 3-torsion elements in class groups of quadratic fields (that is, of maximal quadratic orders) remains the same even when one averages over families of quadratic fields defined by any desired finite set of local conditions.

We turn next to 3-torsion elements in the *ideal group* of a quadratic order $\mathcal{O}$, that is, the group $\mathcal{I}(\mathcal{O})$ of invertible fractional ideals of $\mathcal{O}$, of which the class group $\mathrm{Cl}(\mathcal{O})$ is a quotient. It may come as a surprise that if a quadratic order is not maximal, then it is possible for an *ideal* to have order 3, that is, I can be a fractional ideal of a quadratic order $\mathcal{O}$ satisfying $I^3 = \mathcal{O}$, but $I \neq \mathcal{O}$. We first illustrate this phenomenon with an example.

EXAMPLE 5. Let $\mathcal{O} = \mathbb{Z}[\sqrt{-11}]$ and let $I = (2, (1 - \sqrt{-11})/2)$. Then $I \subset \mathcal{O} \otimes \mathbb{Q}$ is a fractional ideal of $\mathcal{O}$ and has norm one. Since $I^3 \subset \mathcal{O}$, and I has norm one, we must have $I^3 = \mathcal{O}$, even though clearly $I \neq \mathcal{O}$. Hence I has order 3 in the ideal group of $\mathcal{O}$. It follows, in particular, that the *ideal class* represented by I also has order 3 in the class group of $\mathcal{O}$!

Example 5 shows that an element of the ideal class group can have order 3 simply because there exists an ideal representing it that has order 3 in the ideal group. This raises the question as to how many 3-torsion elements exist in the ideal group on average in quadratic orders. For maximal orders, it is easy to show that any 3-torsion element (indeed, any torsion element) in the ideal group must be simply the trivial ideal. For all orders, we have the following theorem.

THEOREM 6. *When orders in quadratic fields are ordered by their absolute discriminants, the average number of 3-torsion elements in the ideal groups of either imaginary or real quadratic orders is $\zeta(2)/\zeta(3)$.*

In the case of general sets of orders defined by any acceptable set of local conditions, we have the following generalization of Theorem 6.

THEOREM 7. *Let (Σ_p) be any acceptable collection of local specifications as above, and let Σ denote the set of all isomorphism classes of quadratic orders $\mathcal{O}$ such that $\mathcal{O} \otimes \mathbb{Z}_p \in \Sigma_p$ for all p. Then, when orders in Σ are ordered by their absolute discriminants:*

(a) *The average number of 3-torsion elements in the ideal groups of imaginary quadratic orders in Σ is M_Σ.*

(b) *The average number of 3-torsion elements in the ideal groups of real quadratic orders in Σ is M_Σ.*

In the preceding theorems, we have distinguished between the two groups $\mathrm{Cl}_3(\mathcal{O})$, the group of *ideal classes of order* 3, and $\mathcal{I}_3(\mathcal{O})$, the group of *ideals of order* 3. Theorems 3 and 7 give the mean values of $|\mathrm{Cl}_3(\mathcal{O})|$ and $|\mathcal{I}_3(\mathcal{O})|$, respectively, as $\mathcal{O}$ ranges over any family of orders defined by local conditions. In both Theorems 3 and 7, we have seen that unless the family consists entirely of maximal orders satisfying a finite number of local conditions, these averages depend on the particular families of orders over which the averages are taken. However, we see that these two theorems together imply the following theorem.

THEOREM 8. *Let (Σ_p) be any acceptable collection of local specifications as above, and let Σ denote the set of all isomorphism classes of quadratic orders $\mathcal{O}$ such that $\mathcal{O} \otimes \mathbb{Z}_p \in \Sigma_p$ for all p. Then, when orders in Σ are ordered by their absolute discriminants:*

(a) *The mean size of $|\mathrm{Cl}_3(\mathcal{O})| - |\mathcal{I}_3(\mathcal{O})|$ across imaginary quadratic orders $\mathcal{O}$ in Σ is* 1.

(b) *The mean size of $|\mathrm{Cl}_3(\mathcal{O})| - \frac{1}{3}|\mathcal{I}_3(\mathcal{O})|$ across real quadratic orders $\mathcal{O}$ in Σ is* 1.

It is a remarkable fact, which begs for explanation, that the mean values in Theorem 8 do not depend on the family of orders that one averages over! In particular, the case of maximal orders gives Corollary 4, because the only 3-torsion element of the ideal group in a maximal order is the trivial ideal.

We end this introduction by describing the methods used in this paper. Our approach combines the original methods of Davenport–Heilbronn with techniques that are class field theoretically ‘dual’ to those methods, which we explain now. First, recall that Davenport–Heilbronn proved Theorem 1 in [**9**] by:

(1) counting appropriate sets of binary cubic forms to compute the number of cubic fields of bounded discriminant, using a bijection (due to Delone and Faddeev [**10**]) between irreducible binary cubic forms and cubic orders;

(2) applying a duality from class field theory between cubic fields and 3-torsion elements of class groups of quadratic fields.

In Sections 2 and 3, we give a new proof of Theorem 1 without class field theory, by using a direct correspondence between binary cubic forms and 3-torsion elements of class groups of quadratic orders proved in [**1**], in place of the Delone–Faddeev correspondence. We describe a very precise version of this correspondence in Section 2 (cf. Theorem 9). In Section 3, we then show how the original counting results of Davenport [**7**, **8**], as applied in the asymptotic count of cubic fields in Davenport–Heilbronn [**9**], can also be used to extract Theorem 1, using the direct correspondence between integral binary cubic forms and 3-torsion elements of class groups of quadratic orders.

To fully illustrate the duality between the original strategy of [**9**] and our strategy described above, we give two ‘dual’ proofs of Theorem 2. In Section 4, we first generalize the proof of Theorem 1 given in Sections 2 and 3, and then in Section 5, we give a second proof of Theorem 2 via ring class field theory, generalizing the original proof of Davenport–Heilbronn

[9]. Both methods involve counting *irreducible* binary cubic forms in fundamental domains for the action of either $\mathrm{SL}_2(\mathbb{Z})$ or $\mathrm{GL}_2(\mathbb{Z})$, as developed in the work of Davenport [7, 8]. However, in our direct method described in Section 4, one must also count points in the 'cusps' of these fundamental regions! The points in the so-called cusp correspond essentially to reducible cubic forms. We find that reducible cubic forms correspond to 3-torsion elements of *ideal groups* of quadratic orders (cf. Theorem 17). In the case of maximal orders, the only torsion element of the ideal group is the identity, and thus the points in the cusps can be ignored when proving Theorem 1. However, in order to prove Theorems 2 and 3 (which do not restrict to maximal orders), we must include reducible forms in our counts, and this is the main goal of Section 4. Isolating the count of reducible forms in the fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ is also what allows us to deduce Theorem 6.

On the other hand, in Section 5, we describe the duality between non-trivial 3-torsion elements of class groups of a given quadratic order and cubic fields whose Galois closure is a ring class field of the fraction field of the quadratic order (cf. Proposition 35). To then count 3-torsion elements in the class groups of quadratic orders, we use the count of cubic fields of bounded discriminant proved by Davenport–Heilbronn [9], but we allow a given cubic field to be counted multiple times, as the Galois closure of a single cubic field can be viewed as the ring class field (of varying conductor) of multiple quadratic orders (cf. Subsection 5.2). This yields a second proof of Theorem 2; furthermore, it allows us to prove also Theorem 3 and Corollary 4, using a generalization of Davenport and Heilbronn's theorem on the density of discriminants of cubic fields established in [3, Theorem 8], which counts cubic orders of bounded discriminant satisfying any acceptable collection of local conditions.

Finally, in Section 6, we generalize the proof of Theorem 2 given in Section 3 to general acceptable families of quadratic orders, which in combination with Theorem 3 allows us to deduce Theorems 7 and 8. We note that, in order to conclude Theorem 7, we use both of the 'dual' perspectives provided in the two proofs of Theorem 2.

2. *Parametrization of order* 3 *ideal classes in quadratic orders*

In this section, we recall the parametrization of elements in the 3-torsion subgroups of ideal class groups of quadratic orders in terms of (orbits of) certain integer-matrix binary cubic forms as proved in [1]. We also deduce various relevant facts that will allow us to prove Theorems 1 and 2 in Sections 3 and 4, respectively, without using class field theory.

2.1. *Binary cubic forms and* 3*-torsion elements in class groups*

The key ingredient in the new proofs of Theorems 1 and 2 is a parametrization of ideal classes of order 3 in quadratic rings by means of equivalence classes of integer-matrix binary cubic forms, which was obtained in [1]. We begin by briefly recalling this parametrization.

Let $V_{\mathbb{R}}$ denote the four-dimensional real vector space of binary cubic forms $ax^3+bx^2y+cxy^2+dy^3$, where $a,b,c,d\in\mathbb{R}$, and let $V_{\mathbb{Z}}$ denote the lattice of those forms for which $a,b,c,d\in\mathbb{Z}$ (that is, the *integer-coefficient* binary cubic forms). The group $\mathrm{GL}_2(\mathbb{Z})$ acts on $V_{\mathbb{R}}$ by the so-called 'twisted action', that is, an element $\gamma\in\mathrm{GL}_2(\mathbb{Z})$ acts on a binary cubic form $f(x,y)$ by

$$(\gamma f)(x,y) := \frac{1}{\det(\gamma)} f((x,y)\gamma). \tag{4}$$

Furthermore, the action preserves $V_{\mathbb{Z}}$. We will be interested in the sublattice of binary cubic forms of the form $f(x,y)=ax^3+3bx^2y+3cxy^2+dy^3$, called *classically integral* or *integer-matrix* if a,b,c,d are integral. We denote the lattice of all integer-matrix forms in $V_{\mathbb{R}}$ by $V_{\mathbb{Z}}^*$. Note that $V_{\mathbb{Z}}^*$ has index 9 in $V_{\mathbb{Z}}$ and is also preserved by $\mathrm{GL}_2(\mathbb{Z})$. We also define the *reduced* *discriminant* $\mathrm{disc}(\cdot)$ on $V_{\mathbb{Z}}^*$ by

$$\mathrm{disc}(f) := -\tfrac{1}{27}\mathrm{Disc}(f) = -3b^2c^2 + 4ac^3 + 4b^3d + a^2d^2 - 6abcd, \tag{5}$$

where $\mathrm{Disc}(f)$ denotes the usual discriminant of f as an element of $V_{\mathbb{Z}}$. It is well known and easy to check that the action of $\mathrm{GL}_2(\mathbb{Z})$ on binary cubic forms preserves (both definitions of) the discriminant.

In [**11**], Eisenstein proved a beautiful correspondence between certain special $\mathrm{SL}_2(\mathbb{Z})$-classes in $V_{\mathbb{Z}}^*$ and ideal classes of order 3 in quadratic rings. We state here a refinement of Eisenstein's correspondence obtained in [**1**], which gives an exact interpretation for *all* $\mathrm{SL}_2(\mathbb{Z})$-classes in $V_{\mathbb{Z}}^*$ in terms of ideal classes in quadratic rings.

To state the theorem, we first require some terminology. We define a *quadratic ring* over $\mathbb{Z}$ (respectively, $\mathbb{Z}_p$) to be any commutative ring with unit that is free of rank 2 as a $\mathbb{Z}$-module (respectively, $\mathbb{Z}_p$-module). An *oriented* quadratic ring $\mathcal{O}$ over $\mathbb{Z}$ is then defined to be a quadratic ring along with a specific choice of isomorphism $\pi : \mathcal{O}/\mathbb{Z} \to \mathbb{Z}$. Note that an oriented quadratic ring has no non-trivial automorphisms. Finally, we say that a quadratic ring (or binary cubic form) is *non-degenerate* if it has non-zero discriminant.

THEOREM 9 ([**1**, Theorem 13]). *There is a natural bijection between the set of non-degenerate* $\mathrm{SL}_2(\mathbb{Z})$*-orbits on the space* $V_{\mathbb{Z}}^*$ *of integer-matrix binary cubic forms and the set of equivalence classes of triples* $(\mathcal{O}, I, \delta)$*, where* $\mathcal{O}$ *is a non-degenerate oriented quadratic ring over* $\mathbb{Z}$*,* I *is an ideal of* $\mathcal{O}$*, and* δ *is an invertible element of* $\mathcal{O} \otimes \mathbb{Q}$ *such that* $I^3 \subseteq \delta \cdot \mathcal{O}$ *and* $N(I)^3 = N(\delta)$*. (Here two triples* $(\mathcal{O}, I, \delta)$ *and* $(\mathcal{O}', I', \delta')$ *are equivalent if there is an isomorphism* $\phi : \mathcal{O} \to \mathcal{O}'$ *and an element* $\kappa \in \mathcal{O}' \otimes \mathbb{Q}$ *such that* $I' = \kappa\phi(I)$ *and* $\delta' = \kappa^3\phi(\delta)$*.) Under this bijection, the reduced discriminant of a binary cubic form is equal to the discriminant of the corresponding quadratic ring.*

The proof of this statement can be found in [**1**, Subsection 3.4]; here we simply sketch the map. Given a triple $(\mathcal{O}, I, \delta)$, the binary cubic form f corresponds to the symmetric trilinear form

$$I \times I \times I \longrightarrow \mathbb{Z} \quad (i_1, i_2, i_3) \longmapsto \pi(\delta^{-1} \cdot i_1 \cdot i_2 \cdot i_3) \tag{6}$$

given by applying multiplication in $\mathcal{O}$, dividing by δ, and then applying π. More explicitly, let us write $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\tau$ where $\langle 1, \tau\rangle$ is a *positively oriented* basis for an oriented quadratic ring, that is, $\pi(\tau) = 1$. Furthermore, let us write $I = \mathbb{Z}\alpha + \mathbb{Z}\beta$, where $\langle \alpha, \beta\rangle$ is a *positively oriented* basis for the $\mathbb{Z}$-submodule I of $\mathcal{O} \otimes \mathbb{Q}$, that is, the change-of-basis matrix from the positively oriented $\langle 1, \tau\rangle$ to $\langle \alpha, \beta\rangle$ has positive determinant. We can then find integers e_0, e_1, e_2, e_3, a, b, c, and d satisfying the following equations:

$$\begin{aligned} \alpha^3 &= \delta(e_0 + a\tau),\\ \alpha^2\beta &= \delta(e_1 + b\tau),\\ \alpha\beta^2 &= \delta(e_2 + c\tau),\\ \beta^3 &= \delta(e_3 + d\tau). \end{aligned} \tag{7}$$

The binary cubic form corresponding to the triple $(\mathcal{O}, I, \delta)$ is then $f(x, y) = ax^3 + 3bx^2y + 3cxy^2 + dy^3$.

Conversely, given a binary cubic form $f(x, y) = ax^3 + 3bx^2y + 3cxy^2 + dy^3$, we can explicitly construct the corresponding triple as follows. The ring $\mathcal{O}$ is completely determined by having discriminant equal to $\mathrm{disc}(f)$. Examining the system of equations in (7) shows that a positively oriented basis $\langle \alpha, \beta\rangle$ for I must satisfy

$$\alpha : \beta = (e_1 + b\tau) : (e_2 + c\tau),$$

where

$$e_1 = \tfrac{1}{2}(b^2c - 2ac^2 + abd - \epsilon b), \quad \text{and} \quad e_2 = -\tfrac{1}{2}(bc^2 - 2b^2d + acd + \epsilon c). \tag{8}$$

Here, $\epsilon = 0$ or 1 in accordance with whether $\mathrm{Disc}(\mathcal{O}) \equiv 0$ or 1 modulo 4, respectively. This uniquely determines α and β up to a scalar factor in $\mathcal{O} \otimes \mathbb{Q}$, and once α and β are fixed, the system in (7) determines δ uniquely. The $\mathcal{O}$-ideal structure of the rank 2 $\mathbb{Z}$-module I is given by the following action of τ on the basis elements of I:

$$\begin{gathered}\tau \cdot \alpha = \frac{B+\epsilon}{2} \cdot \alpha + A \cdot \beta \quad \text{and} \quad \tau \cdot \beta = -C \cdot \alpha + \frac{\epsilon - B}{2} \cdot \beta, \quad \text{where} \\ A = b^2 - ac, \quad B = ad - bc, \quad C = c^2 - bd.\end{gathered} \tag{9}$$

This completely (and explicitly) determines the triple $(\mathcal{O}, I, \delta)$ from the binary cubic form $f(x,y)$. Note that the equivalence defined on triples in the statement of the theorem exactly corresponds to $\mathrm{SL}_2(\mathbb{Z})$-equivalence on the side of binary cubic forms.

We may also deduce from this discussion a description of the stabilizer in $\mathrm{SL}_2(\mathbb{Z})$ of an element in $V_{\mathbb{Z}}^*$ in terms of the corresponding triple $(\mathcal{O}, I, \delta)$.

Corollary 10. *The stabilizer in* $\mathrm{SL}_2(\mathbb{Z})$ *of a non-degenerate element* $v \in V_{\mathbb{Z}}^*$ *is naturally isomorphic to* $U_3(\mathcal{O}_0)$, *where* $(\mathcal{O}, I, \delta)$ *is the triple corresponding to* v *as in Theorem* 9, $\mathcal{O}_0 = \mathrm{End}_{\mathcal{O}}(I)$ *is the endomorphism ring of* I, *and* $U_3(\mathcal{O}_0)$ *denotes the group of units of* $\mathcal{O}_0$ *having order dividing* 3.

Indeed, let $v \in V_{\mathbb{Z}}^*$ be associated to the triple $(\mathcal{O}, I, \delta)$ under Theorem 9. Then an $\mathrm{SL}_2(\mathbb{Z})$-transformation of the basis $\langle \alpha, \beta \rangle$ for I preserves the map in (6) precisely when γ acts by multiplication by a cube root of unity in the endomorphism ring $\mathcal{O}_0$ of I.

We may also similarly describe the orbits of $V_{\mathbb{Z}}^*$ under the action of $\mathrm{GL}_2(\mathbb{Z})$. This simply removes the orientation of the corresponding ring $\mathcal{O}$, thus identifying the triple $(\mathcal{O}, I, \delta)$ with its quadratic conjugate triple $(\mathcal{O}, \bar{I}, \bar{\delta})$.

Corollary 11. *There is a natural bijection between the set of non-degenerate* $\mathrm{GL}_2(\mathbb{Z})$-*orbits on the space* $V_{\mathbb{Z}}^*$ *of integer-matrix binary cubic forms and the set of equivalence classes of triples* $(\mathcal{O}, I, \delta)$, *where* $\mathcal{O}$ *is a non-degenerate (unoriented) quadratic ring,* I *is an ideal of* $\mathcal{O}$, *and* δ *is an invertible element of* $\mathcal{O} \otimes \mathbb{Q}$ *such that* $I^3 \subseteq \delta \cdot \mathcal{O}$ *and* $N(I)^3 = N(\delta)$. *Under this bijection, the reduced discriminant of a binary cubic form is equal to the discriminant of the corresponding quadratic ring. The stabilizer in* $\mathrm{GL}_2(\mathbb{Z})$ *of a non-degenerate element* $v \in V_{\mathbb{Z}}^*$ *is given by the semidirect product*

$$\mathrm{Aut}(\mathcal{O}; I, \delta) \ltimes U_3(\mathcal{O}_0),$$

where: $(\mathcal{O}, I, \delta)$ *is the triple corresponding to* v *as in Theorem* 9; $\mathrm{Aut}(\mathcal{O}; I, \delta)$ *is defined to be* C_2 *if there exists* $\kappa \in (\mathcal{O} \otimes \mathbb{Q})^\times$ *such that* $\bar{I} = \kappa I$ *and* $\bar{\delta} = \kappa^3 \delta$, *and is defined to be trivial otherwise;* $\mathcal{O}_0 = \mathrm{End}_{\mathcal{O}}(I)$ *is the endomorphism ring of* I; *and* $U_3(\mathcal{O}_0)$ *denotes the group of units of* $\mathcal{O}_0$ *having order dividing* 3.

Proof. Given Theorem 9, it remains to check where the now-combined $\mathrm{SL}_2(\mathbb{Z})$-orbits of an integer-matrix binary cubic form f and of γf, where $\gamma = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ map to. If the $\mathrm{SL}_2(\mathbb{Z})$-orbit of f corresponds to a triple $(\mathcal{O}, I, \delta)$ under the above bijection, then the $\mathrm{SL}_2(\mathbb{Z})$-orbit of γf corresponds to the triple $(\mathcal{O}, \bar{I}, \bar{\delta})$ where $\bar{\cdot}$ denotes the image under the non-trivial automorphism of the unoriented quadratic ring $\mathcal{O}$. Thus we obtain a correspondence between $\mathrm{GL}_2(\mathbb{Z})$-orbits of integer-matrix binary cubic forms and triples $(\mathcal{O}, I, \delta)$ as described above except that $\mathcal{O}$ is viewed as a quadratic ring without orientation.

For the stabilizer statement, note that an element g of $\mathrm{GL}_2(\mathbb{Z})$ preserving v must have determinant either $+1$ or -1. If g has determinant 1, then when it acts on the basis $\langle\alpha,\beta\rangle$ of I, it preserves the vector $v=(a,b,c,d)$ in (7) if and only if $\alpha^3,\alpha^2\beta,\alpha\beta^2,\beta^3$ remain unchanged; thus g must act by multiplication by a unit u in the unit group $U(\mathcal{O}_0)$ of $\mathcal{O}_0$ whose cube is 1. If g has determinant -1, then the basis element τ gets replaced by its conjugate $\bar{\tau}$ in addition to $\langle\alpha,\beta\rangle$ being transformed by g. If this is to preserve the vector $v=(a,b,c,d)$ in (7), then this means that conjugation on $\mathcal{O}$ maps I to κI and δ to $\kappa^3\delta$ for some $\kappa\in(\mathcal{O}\otimes\mathbb{Q})^\times$. The result follows. □

REMARK 12. The statements in Theorem 9, Corollary 10, and Corollary 11 also hold after base change to $\mathbb{Z}_p$, with the same proofs. In the case of Theorem 9, in the proof, by a *positively oriented* basis $\langle\alpha,\beta\rangle$ of an ideal I of R, we mean that the change-of-basis matrix from $\langle 1,\tau\rangle$ to $\langle\alpha,\beta\rangle$ has determinant equal to a power of p (so that all positively oriented bases $\langle\alpha,\beta\rangle$ of I form a single orbit for the action of $\mathrm{SL}_2(\mathbb{Z}_p)$); all other details remain identical. Corollary 11 and its analogue over $\mathbb{Z}_p$ will be relevant in Section 6, during the proofs of Theorems 7 and 8.

2.2. *Composition of cubic forms and 3-class groups*

Let us say that an integer-matrix binary cubic form f, or its corresponding triple $(\mathcal{O},I,\delta)$ via the correspondence of Theorem 9, is *projective* if I is projective as an $\mathcal{O}$-module (that is, if I is invertible as an ideal of $\mathcal{O}$); in such a case we have $I^3=(\delta)$. The bijection of Theorem 9 allows us to describe a composition law on the set of projective integer-matrix binary cubic forms, up to $\mathrm{SL}_2(\mathbb{Z})$-equivalence, having the same reduced discriminant. This turns the set of all $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of projective integer-matrix binary cubic forms having given reduced discriminant D into a group, which is closely related to the group $\mathrm{Cl}_3(\mathcal{O})$, if $\mathcal{O}$ also has discriminant D. In this section, we describe this group law and establish some of its relevant properties.

Fix an oriented quadratic ring $\mathcal{O}$. Given such an $\mathcal{O}$, we obtain a natural law of composition on equivalence classes of triples $(\mathcal{O},I,\delta)$, where I is an invertible ideal of $\mathcal{O}$ and $\delta\in(\mathcal{O}\otimes\mathbb{Q})^\times$ such that $I^3=\delta\cdot\mathcal{O}$ and $N(I)^3=N(\delta)$. It is defined by

$$(\mathcal{O},I,\delta)\circ(\mathcal{O},I',\delta')=(\mathcal{O},II',\delta\delta').$$

The equivalence classes of projective triples $(\mathcal{O},I,\delta)$ thus form a group under this composition law, which we denote by $H(\mathcal{O})$ (note that two oriented quadratic rings $\mathcal{O}$ and $\mathcal{O}'$ of the same discriminant are canonically isomorphic, and hence the groups $H(\mathcal{O})$ and $H(\mathcal{O}')$ are also canonically isomorphic). By Theorem 9, we also then obtain a corresponding composition law on $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of integer-matrix cubic forms f having a given reduced discriminant D (a higher-degree analogue of Gauss composition). We say that such a binary cubic form f is *projective* if the corresponding $(\mathcal{O},I,\delta)$ is projective. We will sometimes view $H(\mathcal{O})$ as the group consisting of the $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of integer-matrix binary cubic forms having reduced discriminant equal to $\mathrm{Disc}(\mathcal{O})$.

In order to understand the relationship between $H(\mathcal{O})$ and $\mathrm{Cl}_3(\mathcal{O})$, we first establish a lemma describing the number of preimages of an ideal class under the ‘forgetful’ map $H(\mathcal{O})\to\mathrm{Cl}_3(\mathcal{O})$ defined by $(\mathcal{O},I,\delta)\mapsto[I]$.

LEMMA 13. *Let $\mathcal{O}$ be an order in a quadratic field and I be an invertible ideal of $\mathcal{O}$ whose class has order 3 in the class group of $\mathcal{O}$. Then the number of elements $\delta\in\mathcal{O}$ (up to cube factors in $(\mathcal{O}\otimes\mathbb{Q})^\times$) yielding a valid triple $(\mathcal{O},I,\delta)$ in the sense of Theorem 9 is 1 if $\mathrm{Disc}(\mathcal{O})<-3$, and 3 otherwise.*

Proof. Fix an invertible ideal I of $\mathcal{O}$ that arises in some valid triple. The number of elements δ having norm equal to $N(I)^3$ and yielding distinct elements of $H(\mathcal{O})$ is then $|U^+(\mathcal{O})/U^+(\mathcal{O})^{\times 3}|$, where $U^+(\mathcal{O})$ denotes the group of units of $\mathcal{O}$ having norm 1. In fact, we have an exact sequence

$$1 \longrightarrow \frac{U^+(\mathcal{O})}{U^+(\mathcal{O})^{\times 3}} \longrightarrow H(\mathcal{O}) \longrightarrow \mathrm{Cl}_3(\mathcal{O}) \longrightarrow 1. \tag{10}$$

We see that, for all orders $\mathcal{O}$ in imaginary quadratic fields other than the maximal order $\mathbb{Z}[\sqrt{-3}]$, the unit group has cardinality 2 or 4, and therefore $|U^+(\mathcal{O})/U^+(\mathcal{O})^{\times 3}| = 1$. For real quadratic orders $\mathcal{O}$, the unit group has rank one and torsion equal to $\{\pm 1\}$, and so $|U^+(\mathcal{O})/U^+(\mathcal{O})^{\times 3}| = 3$. Finally, for $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$, we have $|U^+(\mathcal{O})/U^+(\mathcal{O})^{\times 3}| = 3$ as well. $\square$

Equation (10) thus makes precise the relationship between $H(\mathcal{O})$ and $\mathrm{Cl}_3(\mathcal{O})$. With regard to the sizes of these groups, we obtain the following corollary.

COROLLARY 14. *We have $|H(\mathcal{O})| = |\mathrm{Cl}_3(\mathcal{O})|$ when $\mathcal{O}$ has discriminant $\mathrm{Disc}(\mathcal{O}) < -3$, and $|H(\mathcal{O})| = 3 \cdot |\mathrm{Cl}_3(\mathcal{O})|$ otherwise.*

2.3. *Projective binary cubic forms and invertibility*

We now wish to explicitly describe the projective binary cubic forms. Recall that the *quadratic Hessian covariant* of $f(x,y) = ax^3 + 3bx^2y + 3cxy^2 + dy^3$ is given by $Q(x,y) = Ax^2 + Bxy + Cy^2$, where A, B, C are defined by (9); then Q also describes the norm form on I mapping into $\mathbb{Z}$. It is well known, going back to the work of Gauss, that I is invertible if and only if $Q(x,y)$ is *primitive*, that is, $(A,B,C) = (b^2 - ac, ad - bc, c^2 - bd) = 1$ (see, for example, [**6**, Proposition 7.4 and Theorem 7.7(i)–(ii)]). Thus,

$$\begin{aligned} f(x,y) = ax^3 + 3bx^2y + 3cxy^2 + dy^3 &\text{ is projective} \\ \iff (b^2 - ac, ad - bc, c^2 - bd) = 1. \end{aligned} \tag{11}$$

Let $\mathcal{S}$ denote the set of all projective forms $f(x,y) = ax^3 + 3bx^2y + 3cxy^2 + dy^3$ in $V_{\mathbb{Z}}^*$. Let $V_{\mathbb{Z}_p}^*$ denote the set of all forms $f(x,y) = ax^3 + 3bx^2y + 3cxy^2 + dy^3$ such that $a,b,c,d \in \mathbb{Z}_p$, and let $\mu_p^*(\mathcal{S})$ denote the p-adic density of the p-adic closure of $\mathcal{S}$ in $V_{\mathbb{Z}_p}^*$, where we normalize the additive measure μ_p^* on $V_{\mathbb{Z}_p}^* = \mathbb{Z}_p^4$ so that $\mu_p^*(V_{\mathbb{Z}_p}^*) = 1$. The following lemma gives the value of $\mu_p^*(\mathcal{S})$.

LEMMA 15. *We have $\mu_p^*(\mathcal{S}) = 1 - 1/p^2$.*

Proof. Suppose

$$b^2 - ac \equiv bc - ad \equiv c^2 - bd \equiv 0 \pmod{p}. \tag{12}$$

Then the pair (a,b) can take any value except $(0,r)$, where $r \not\equiv 0 \pmod{p}$. Given any such non-zero pair (a,b), the variables c and d are then clearly determined modulo p from (a,b). If $(a,b) \equiv (0,0) \pmod{p}$, then c must also vanish $\pmod{p}$, while d can be arbitrary $\pmod{p}$. We conclude that the total number of solutions $\pmod{p}$ to (12) for the quadruple (a,b,c,d) is $(p^2 - p) + p = p^2$. Thus $\mu_p^*(\mathcal{S}) = (p^4 - p^2)/p^4$, as claimed. $\square$

2.4. *Reducible forms*

As summarized in the introduction, the correspondence of Delone–Faddeev in [**10**] between irreducible binary cubic forms and orders in cubic fields was used by Davenport–Heilbronn [**9**] to determine the density of discriminants of cubic fields. Theorem 9, however, gives a different correspondence than the one due to Delone–Faddeev [**10**]; in particular, it does *not* restrict to irreducible forms. The question then arises: which elements of $H(\mathcal{O})$ correspond to the integer-matrix binary cubic forms that are reducible, that is, that factor over $\mathbb{Q}$ (equivalently, $\mathbb{Z}$)? We answer this question here, first by establishing which triples $(\mathcal{O}, I, \delta)$ correspond to reducible binary cubic forms.

LEMMA 16. *Let f be an element of $V_{\mathbb{Z}}^*$, and let $(\mathcal{O}, I, \delta)$ be a representative for the corresponding equivalence class of triples as given by Theorem 9. Then f has a rational zero as a binary cubic form if and only if δ is a cube in $(\mathcal{O} \otimes \mathbb{Q})^\times$.*

Proof. Suppose $\delta = \xi^3$ for some invertible $\xi \in \mathcal{O} \otimes \mathbb{Q}$. Then, by replacing I by $\xi^{-1}I$ and δ by $\xi^{-3}\delta$ if necessary, we may assume that $\delta = 1$. Let α be the smallest positive element in $I \cap \mathbb{Z}$, and extend to a basis $\langle \alpha, \beta \rangle$ of I. Then the binary cubic form f corresponding to the basis $\langle \alpha, \beta \rangle$ of I via Theorem 9 evidently has a zero, since $\alpha \in \mathbb{Z}$, $\delta = 1$, and so $a = 0$ in (7).

Conversely, suppose $(x_0, y_0) \in \mathbb{Q}^2$ with $f(x_0, y_0) = 0$. Without loss of generality, we may assume that $(x_0, y_0) \in \mathbb{Z}^2$. If $(\mathcal{O}, I, \delta)$ is the corresponding triple and I has positively oriented basis $\langle \alpha, \beta \rangle$, then, by (7) or (6), we obtain

$$(x_0\alpha + y_0\beta)^3 = n\delta \quad \text{for some } n \in \mathbb{Z}.$$

If $\xi = x_0\alpha + y_0\beta$, then we have $\xi^3 = n\delta$, and taking norms to $\mathbb{Z}$ on both sides reveals that $N(\xi)^3 = n^2N(\delta) = n^2N(I)^3$. Thus $n = m^3$ is a cube. This then implies that δ must be a cube in $(\mathcal{O} \otimes \mathbb{Q})^\times$ as well, namely $\delta = (\xi/m)^3$, as desired. □

The reducible forms thus form a subgroup of $H(\mathcal{O})$, which we denote by $H_{\text{red}}(\mathcal{O})$; by the previous lemma, it is the subgroup consisting of those triples $(\mathcal{O}, I, \delta)$, up to equivalence, for which δ is a cube. As in the introduction, let $\mathcal{I}_3(\mathcal{O})$ denote the 3-torsion subgroup of the ideal group of $\mathcal{O}$, that is, the set of invertible ideals I of $\mathcal{O}$ such that $I^3 = \mathcal{O}$. We may then define a map

$$\varphi : \mathcal{I}_3(\mathcal{O}) \longrightarrow H(\mathcal{O}) \quad \varphi : I \longmapsto (\mathcal{O}, I, 1). \tag{13}$$

It is evident that $\operatorname{im}(\mathcal{I}_3(\mathcal{O})) \subseteq H_{\text{red}}(\mathcal{O})$. In fact, we show that φ defines an isomorphism between $\mathcal{I}_3(\mathcal{O})$ and $H_{\text{red}}(\mathcal{O})$.

THEOREM 17. *The map φ yields an isomorphism of $\mathcal{I}_3(\mathcal{O})$ with $H_{\text{red}}(\mathcal{O})$.*

Proof. The preimage of the identity $(\mathcal{O}, \mathcal{O}, 1) \in H(\mathcal{O})$ can only contain 3-torsion ideals of the form $\kappa \cdot \mathcal{O}$ for $\kappa \in (\mathcal{O} \otimes \mathbb{Q})^\times$. To be a 3-torsion ideal, we must have $(\kappa\mathcal{O})^3 = \mathcal{O}$ which implies that $\kappa^3 \in \mathcal{O}^\times$ and so $\kappa \in \mathcal{O}^\times$. Therefore, the preimage of the identity is simply the ideal $\mathcal{O}$, and the map is injective. It remains to show surjectivity onto $H_{\text{red}}(\mathcal{O})$. Assume $(\mathcal{O}, I, \delta) \in H_{\text{red}}(\mathcal{O})$. Since δ is a cube by definition, let $\delta = \xi^3$ and recall that $(\mathcal{O}, I, \delta) \sim (\mathcal{O}, \xi^{-1}I, 1)$. Thus $\xi^{-1}I \in \mathcal{I}_3(\mathcal{O})$. □

COROLLARY 18. *Assume that $\mathcal{O}$ is maximal. Then $H_{\text{red}}(\mathcal{O})$ contains only the identity element of $H(\mathcal{O})$, which can be represented by $(\mathcal{O}, \mathcal{O}, 1)$.*

Proof. Since maximal orders are Dedekind domains, the only ideal that is 3-torsion in the ideal group is $\mathcal{O}$. □

3. *A proof of Davenport and Heilbronn's theorem on class numbers without class field theory*

Using the direct correspondence of Theorem 9, we can now deduce Theorem 1 by counting the relevant binary cubic forms. To do so, we need the following result of Davenport describing the asymptotic behavior of the number of binary cubic forms of bounded reduced discriminant in subsets of $V_{\mathbb{Z}}^*$ defined by finitely many congruence conditions.

THEOREM 19 ([**7**, **8**, **9**, Section 5, **3**, Theorem 26]). *Let S denote a set of integer-matrix binary cubic forms in $V_{\mathbb{Z}}^*$ defined by finitely many congruence conditions modulo prime powers. Let $V_{\mathbb{Z}}^{*(0)}$ denote the set of elements in $V_{\mathbb{Z}}^*$ having positive reduced discriminant, and $V_{\mathbb{Z}}^{*(1)}$ be the set of elements in $V_{\mathbb{Z}}^*$ having reduced negative discriminant. For $i = 0$ or 1, let $N^*(S \cap V_{\mathbb{Z}}^{*(i)}, X)$ denote the number of* irreducible $\mathrm{SL}_2(\mathbb{Z})$*-orbits on $S \cap V_{\mathbb{Z}}^{*(i)}$ having absolute reduced discriminant* $|\mathrm{disc}|$ *less than X. Then*

$$\lim_{X\to\infty} \frac{N^*(S \cap V_{\mathbb{Z}}^{*(i)}, X)}{X} = \frac{\pi^2}{4 \cdot n_i^*} \prod_p \mu_p^*(S), \tag{14}$$

where $\mu_p^*(S)$ denotes the p-adic density of S in $V_{\mathbb{Z}_p}^*$, and $n_i^* = 1$ or 3 for $i = 0$ or 1, respectively.

Note that, in both [**3**, **9**], this theorem is expressed in terms of $\mathrm{GL}_2(\mathbb{Z})$-orbits of binary cubic forms in $V_{\mathbb{Z}}$ with discriminant $\mathrm{Disc}(\cdot)$ defined by $-27 \cdot \mathrm{disc}(\cdot)$. Here, we have stated the theorem for $\mathrm{SL}_2(\mathbb{Z})$-orbits of integer-matrix binary cubic forms, and the p-adic measure is normalized so that $\mu_p^*(V_{\mathbb{Z}_p}^*) = 1$. This version is proved in exactly the same way as the original theorem, but since:

(a) $V_{\mathbb{Z}}^*$ has index 9 in $V_{\mathbb{Z}}$;
(b) we use the reduced discriminant $\mathrm{disc}(\cdot)$ instead of $\mathrm{Disc}(\cdot)$; and
(c) there are two $\mathrm{SL}_2(\mathbb{Z})$-orbits in every irreducible $\mathrm{GL}_2(\mathbb{Z})$-orbit,

the constant on the right-hand side of (14) changes from $\pi^2/12n_i$ as in [**3**] to $\pi^2/4n_i^*$, where $n_i = 6$ or 2 for $i = 0$ or 1, respectively.

Our goal then is to count the $\mathrm{SL}_2(\mathbb{Z})$-orbits of forms in $V_{\mathbb{Z}}^{*(i)}$ that correspond, under the bijection described in Theorem 9, to equivalence classes of triples $(\mathcal{O}, I, \delta)$, where $\mathcal{O}$ is a maximal quadratic ring and I is projective. However, if $\mathcal{O}$ is a maximal quadratic ring, then all ideals of $\mathcal{O}$ are projective, and so our only restriction on elements $f \in V_{\mathbb{Z}}^{*(i)}$ then is that $\mathrm{disc}(f)$ be the discriminant of a maximal quadratic ring. It is well known that a quadratic ring $\mathcal{O}$ is maximal if and only if the odd part of the discriminant of $\mathcal{O}$ is squarefree, and $\mathrm{disc}(\mathcal{O}) \equiv 1$, 5, 8, 9, 12, or 13 (mod 16). We therefore define, for every prime p,

$$\mathcal{V}_p := \begin{cases} \{f \in V_{\mathbb{Z}}^* : \mathrm{disc}(f) \equiv 1, 5, 8, 9, 12, 13 \pmod{16}\} & \text{if } p = 2; \\ \{f \in V_{\mathbb{Z}}^* : \mathrm{disc}_p(f) \text{ is squarefree}\} & \text{if } p \neq 2. \end{cases}$$

Here, $\mathrm{disc}_p(f)$ is the p-part of $\mathrm{disc}(f)$. If we set $\mathcal{V} := \cap_p \mathcal{V}_p$, then $\mathcal{V}$ is the set of forms in $V_{\mathbb{Z}}^*$ for which the ring $\mathcal{O}$ in the associated triple $(\mathcal{O}, I, \delta)$ is a maximal quadratic ring. The following lemma describes the p-adic densities of $\mathcal{V}$ (here, we are using the fact that the p-adic closure of $\mathcal{V}$ is $\mathcal{V}_p$).

LEMMA 20 ([**9**, Lemma 4]). *We have $\mu_p^*(\mathcal{V}_p) = (p^2 - 1)^2/p^4$.*

We define $N^*(\mathcal{V} \cap V_{\mathbb{Z}}^{*(i)}, X)$ analogously, as the number of irreducible orbits in $\mathcal{V} \cap V_{\mathbb{Z}}^{*(i)}$ having absolute reduced discriminant between 0 and X (for $i = 0, 1$). Since we are restricting to irreducible orbits, $N^*(\mathcal{V} \cap V_{\mathbb{Z}}^{*(i)}, X)$ counts those (equivalence classes of) triples $(\mathcal{O}, I, \delta)$, where $\mathcal{O}$ is maximal with $|\mathrm{Disc}(\mathcal{O})| < X$, but, by Corollary 18, the identity of $H(\mathcal{O})$ is *not* included in this count.

We cannot immediately apply Theorem 19 to compute $N^*(\mathcal{V} \cap V_{\mathbb{Z}}^{*(i)}, X)$, as the set $\mathcal{V}$ is defined by infinitely many congruence conditions. However, the following uniformity estimate for the complement of $\mathcal{V}_p$ for all p will allow us in Subsection 3.1 to strengthen (14) to also hold when $S = \mathcal{V}$.

PROPOSITION 21 ([**9**, Proposition 1]). *Define* $\mathcal{W}_p^* = V_{\mathbb{Z}}^* \backslash \mathcal{V}_p$ *for all primes* p. *Then* $N(\mathcal{W}_p^*; X) = O(X/p^2)$ *where the implied constant is independent of* p.

REMARK 22. None of the proofs of the quoted results in this section use class field theory except for [**9**, Proposition 1], which invokes one lemma (namely, [**9**, Lemma 7]) that is proved in [**9**] by class field theory; however, this lemma immediately follows from our Theorems 9 and 19, which do not appeal to class field theory.

3.1. *The mean number of 3-torsion elements in the class groups of quadratic fields without class field theory (Proof of Theorem 1)*

We now complete the proof of Theorem 1. Suppose that Y is any positive integer. It follows from Theorem 19 and Lemma 20 that

$$\lim_{X\to\infty} \frac{N^*(\cap_{p<Y}\mathcal{V}_p \cap V_{\mathbb{Z}}^{*(i)}, X)}{X} = \frac{\pi^2}{4n_i^*} \cdot \prod_{p<Y}\left(1-\frac{1}{p^2}\right)^2.$$

Letting Y tend to ∞, we obtain

$$\limsup_{X\to\infty} \frac{N^*(\mathcal{V} \cap V_{\mathbb{Z}}^{*(i)}, X)}{X} \leqslant \frac{\pi^2}{4n_i^*} \cdot \prod_{p}\left(1-\frac{1}{p^2}\right)^2 = \frac{3}{2n_i^*\zeta(2)}.$$

To obtain a lower bound for $N^*(\mathcal{V} \cap V_{\mathbb{Z}}^{*(i)}, X)$, we use the fact that

$$\bigcap_{p<Y} \mathcal{V}_p \subset \left(\mathcal{V} \cup \bigcup_{p\geqslant Y} \mathcal{W}_p^*\right). \tag{15}$$

By Proposition 21 and (15), we have

$$\liminf_{X\to\infty} \frac{N^*(\mathcal{V} \cap V_{\mathbb{Z}}^{*(i)}, X)}{X} \geqslant \frac{\pi^2}{4n_i^*} \cdot \prod_{p}\left(1-\frac{1}{p^2}\right)^2 - O\left(\sum_{p\geqslant Y} p^{-2}\right).$$

Letting Y tend to ∞ again, we obtain

$$\liminf_{X\to\infty} \frac{N^*(\mathcal{V} \cap V_{\mathbb{Z}}^{*(i)}, X)}{X} \geqslant \frac{\pi^2}{4n_i^*} \cdot \prod_{p}\left(1-\frac{1}{p^2}\right)^2 = \frac{3}{2n_i^*\zeta(2)}.$$

Thus,

$$\lim_{X\to\infty} \frac{N^*(\mathcal{V} \cap V_{\mathbb{Z}}^{*(i)}, X)}{X} = \frac{9}{n_i^*\pi^2}.$$

Finally, we use Corollaries 14 and 18 to relate $N^*(\mathcal{V} \cap V_{\mathbb{Z}}^{*(i)}, X)$ and 3-torsion ideal classes in maximal quadratic rings with discriminant less than X:

$$\sum_{\substack{0<\mathrm{Disc}(\mathcal{O})<X,\\ \mathcal{O}\text{ maximal}}} (3\cdot|\mathrm{Cl}_3(\mathcal{O})|-1) = N^*(\mathcal{V} \cap V_{\mathbb{Z}}^{*(0)}, X);$$
$$\sum_{\substack{0<-\mathrm{Disc}(\mathcal{O})<X,\\ \mathcal{O}\text{ maximal}}} (|\mathrm{Cl}_3(\mathcal{O})|-1) = N^*(\mathcal{V} \cap V_{\mathbb{Z}}^{*(1)}, X).$$

Since

$$\lim_{X\to\infty}\frac{\sum_{\substack{0<\mathrm{Disc}(\mathcal{O})<X,\\ \mathcal{O}\text{ maximal}}}1}{X}=\frac{3}{\pi^2}\quad\text{and}\quad\lim_{X\to\infty}\frac{\sum_{\substack{0<-\mathrm{Disc}(\mathcal{O})<X,\\ \mathcal{O}\text{ maximal}}}1}{X}=\frac{3}{\pi^2},\tag{16}$$

we conclude

$$\lim_{X\to\infty}\frac{\sum_{\substack{0<\mathrm{Disc}(\mathcal{O})<X,\\ \mathcal{O}\text{ maximal}}}|\mathrm{Cl}_3(\mathcal{O})|}{\sum_{\substack{0<\mathrm{Disc}(\mathcal{O})<X,\\ \mathcal{O}\text{ maximal}}}1}=\frac{1}{3}\left(1+\lim_{X\to\infty}\frac{N^*(\mathcal{V}\cap V_{\mathbb{Z}}^{*(0)};X)}{\sum_{\substack{0<\mathrm{Disc}(\mathcal{O})<X,\\ \mathcal{O}\text{ maximal}}}1}\right)=\frac{1}{3}\left(1+\frac{9/n_0^*}{3}\right)=\frac{4}{3},$$

$$\lim_{X\to\infty}\frac{\sum_{\substack{0<-\mathrm{Disc}(\mathcal{O})<X,\\ \mathcal{O}\text{ maximal}}}|\mathrm{Cl}_3(\mathcal{O})|}{\sum_{\substack{0<-\mathrm{Disc}(\mathcal{O})<X,\\ \mathcal{O}\text{ maximal}}}1}=1+\lim_{X\to\infty}\frac{N^*(\mathcal{V}\cap V_{\mathbb{Z}}^{*(1)};X)}{\sum_{\substack{0<-\mathrm{Disc}(\mathcal{O})<X,\\ \mathcal{O}\text{ maximal}}}1}=1+\frac{9/n_1^*}{3}=2.$$

3.2. *Generalization to orders*

The above proof of Theorem 1 can be generalized to orders to yield the special case of Theorem 8 where we average over all quadratic orders. This will also explain why the quantities being averaged in Theorem 8 arise naturally. All the ingredients remain the same as in the previous subsection, except that we now replace $\mathcal{V}\subset\mathcal{V}_{\mathbb{Z}}^*$ with the set $\mathcal{S}$ of all projective integer-matrix binary cubic forms as defined in Subsection 2.3. Recall that projective forms correspond under Theorem 9 to valid triples with an invertible ideal. However, since $N^*(S,X)$ only counts irreducible orbits, by Corollary 14 and Theorem 17, we obtain

$$N^*(\mathcal{S}\cap V_{\mathbb{Z}}^{*(i)},X)=\begin{cases}\displaystyle\sum_{0<\mathrm{Disc}(\mathcal{O})<X}3\cdot|\mathrm{Cl}_3(\mathcal{O})|-\sum_{0<\mathrm{Disc}(\mathcal{O})<X}|\mathcal{I}_3(\mathcal{O})| & \text{if } i=0,\\ \displaystyle\sum_{0<-\mathrm{Disc}(\mathcal{O})<X}|\mathrm{Cl}_3(\mathcal{O})|-\sum_{0<-\mathrm{Disc}(\mathcal{O})<X}|\mathcal{I}_3(\mathcal{O})| & \text{if } i=1.\end{cases}\tag{17}$$

As before, let Y be any positive integer and let $\mathcal{S}_p$ denote the p-adic closure of $\mathcal{S}$ in $V_{\mathbb{Z}_p}^*$, so that $\cap_p\mathcal{S}_p=\mathcal{S}$. It follows from Lemma 15 and Theorem 19 that

$$\lim_{X\to\infty}\frac{N^*(\cap_{p<Y}\mathcal{S}_p\cap V_{\mathbb{Z}}^{*(i)},X)}{X}=\frac{\pi^2}{4n_i^*}\cdot\prod_{p<Y}\left(1-\frac{1}{p^2}\right).$$

Letting Y tend to ∞ gives

$$\limsup_{X\to\infty}\frac{N^*(\mathcal{S}\cap V_{\mathbb{Z}}^{*(i)},X)}{X}\leqslant\frac{\pi^2}{4n_i^*}\cdot\prod_p\left(1-\frac{1}{p^2}\right)=\frac{3}{2n_i^*}.$$

Using again $\mathcal{W}_p^*$ to denote $V_{\mathbb{Z}}^*\backslash\mathcal{V}_p$, we still have that

$$\bigcap_{p<Y}\mathcal{S}_p\subset\left(\mathcal{S}\cup\bigcup_{p\geqslant Y}\mathcal{W}_p^*\right).$$

Thus, it follows from Theorem 21 that

$$\liminf_{X\to\infty}\frac{N^*(\mathcal{S}\cap V_{\mathbb{Z}}^{*(i)},X)}{X}\geqslant\frac{\pi^2}{4n_i^*}\cdot\prod_p\left(1-\frac{1}{p^2}\right)-O\left(\sum_{p\geqslant Y}p^{-2}\right),$$

and letting Y tend to ∞ gives

$$\liminf_{X\to\infty} \frac{N(\mathcal{S}\cap V_{\mathbb{Z}}^{*(i)},X)}{X} \geqslant \frac{\pi^2}{4n_i^*}\cdot\prod_p\left(1-\frac{1}{p^2}\right) = \frac{3}{2n_i^*}.$$

Thus

$$\lim_{X\to\infty} \frac{N^*(\mathcal{S}\cap V_{\mathbb{Z}}^{*(i)},X)}{X} = \frac{3}{2n_i^*}.$$

Since

$$\lim_{X\to\infty}\frac{\sum_{0<\mathrm{Disc}(\mathcal{O})<X}1}{X}=\frac{1}{2} \quad\text{and}\quad \lim_{X\to\infty}\frac{\sum_{0<-\mathrm{Disc}(\mathcal{O})<X}1}{X}=\frac{1}{2}, \tag{18}$$

by (17) we conclude that

$$\begin{aligned}
&\lim_{X\to\infty}\frac{\sum_{0<\mathrm{Disc}(\mathcal{O})<X}|\mathrm{Cl}_3(\mathcal{O})|-\frac{1}{3}|\mathcal{I}_3(\mathcal{O})|}{\sum_{0<\mathrm{Disc}(\mathcal{O})<X}1} = \frac{1}{3}\left(\frac{3/2n_0^*}{1/2}\right)=1, \quad\text{and}\\
&\lim_{X\to\infty}\frac{\sum_{0<-\mathrm{Disc}(\mathcal{O})<X}|\mathrm{Cl}_3(\mathcal{O})|-|\mathcal{I}_3(\mathcal{O})|}{\sum_{0<-\mathrm{Disc}(\mathcal{O})<X}1} = \frac{3/2n_1^*}{1/2}=1.
\end{aligned} \tag{19}$$

This proves Theorem 8 in the case that Σ is the set of all isomorphism classes of quadratic orders.

In the next section, we will count also the reducible $\mathrm{SL}_2(\mathbb{Z})$-orbits of $\mathcal{S}\cap V_{\mathbb{Z}}^{*(i)}$ having bounded reduced discriminant, which will establish the mean total number of 3-torsion elements in the class groups of imaginary quadratic orders and of real quadratic orders, as stated in Theorem 2.

4. *The mean number of* 3*-torsion elements in the ideal groups of quadratic orders* (*Proofs of Theorems* 2 *and* 6)

We have seen in Subsection 3.2 that counting irreducible orbits of integer-matrix binary cubic forms and using the correspondence described in Theorem 9 is not enough to conclude Theorem 2. In addition, Theorem 17 shows that in order to establish Theorem 6, we must compute the number of *reducible* integer-matrix binary cubic forms, up to the action of $\mathrm{SL}_2(\mathbb{Z})$, having bounded reduced discriminant. In [**7**, **8**], Davenport computed the number of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of irreducible integer-coefficient binary cubic forms of bounded non-reduced discriminant. In this section, we similarly count reducible integer-matrix forms with bounded reduced discriminant and establish the following result, from which both Theorems 2 and 6 follow.

PROPOSITION 23. *Let $h_{\mathrm{proj,red}}(D)$ denote the number of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of projective and reducible integer-matrix binary cubic forms of reduced discriminant D. Then*

$$\sum_{0<\mathrm{Disc}(\mathcal{O})<X}|H_{\mathrm{red}}(\mathcal{O})| = \sum_{0<D<X}h_{\mathrm{proj,red}}(D)=\frac{\zeta(2)}{2\zeta(3)}\cdot X+o(X)$$

and

$$\sum_{0<-\mathrm{Disc}(\mathcal{O})<X}|H_{\mathrm{red}}(\mathcal{O})| = \sum_{0<-D<X}h_{\mathrm{proj,red}}(D)=\frac{\zeta(2)}{2\zeta(3)}\cdot X+o(X).$$

Recall that, by definition, if $\mathcal{O}$ is the quadratic ring of discriminant D, then $|H_{\mathrm{red}}(\mathcal{O})| = h_{\mathrm{proj,red}}(D)$.

By Theorem 17, (18), and Proposition 23, we then obtain the following corollary.

Corollary 24 (Theorem 6). *Let $\mathcal{I}_3(\mathcal{O})$ denote the* 3*-torsion subgroup of the ideal group of the quadratic order $\mathcal{O}$. Then*

$$\lim_{X\to\infty}\frac{\sum_{0<\mathrm{Disc}(\mathcal{O})<X}|\mathcal{I}_3(\mathcal{O})|}{\sum_{0<\mathrm{Disc}(\mathcal{O})<X}1}=\frac{\zeta(2)}{\zeta(3)}\quad\textit{and}\quad\lim_{X\to\infty}\frac{\sum_{0<-\mathrm{Disc}(\mathcal{O})<X}|\mathcal{I}_3(\mathcal{O})|}{\sum_{0<-\mathrm{Disc}(\mathcal{O})<X}1}=\frac{\zeta(2)}{\zeta(3)}.$$

Finally, combining Theorem 6 with (19), we conclude the following corollary.

Corollary 25 (Theorem 2). *We have*

$$\lim_{X\to\infty}\frac{\sum_{0<\mathrm{Disc}(\mathcal{O})<X}|\mathrm{Cl}_3(\mathcal{O})|}{\sum_{0<\mathrm{Disc}(\mathcal{O})<X}1}=1+\frac{1}{3}\cdot\frac{\zeta(2)}{\zeta(3)},$$

and

$$\lim_{X\to\infty}\frac{\sum_{0<-\mathrm{Disc}(\mathcal{O})<X}|\mathrm{Cl}_3(\mathcal{O})|}{\sum_{0<-\mathrm{Disc}(\mathcal{O})<X}1}=1+\frac{\zeta(2)}{\zeta(3)}.$$

We now turn to the proof of Proposition 23.

4.1. *Counting reducible forms of negative reduced discriminant*

We first consider the case of negative reduced discriminant, when the quadratic Hessian covariant of a binary cubic form is positive definite. Gauss described a fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on positive-definite real binary quadratic forms in terms of inequalities on their coefficients. This allows us to describe an analogous fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on real binary cubic forms of negative reduced discriminant. Bounding the reduced discriminant cuts out a region of the fundamental domain which can be described via suitable bounds on the coefficients of the binary cubic forms (cf. Lemma 26). Within this region, we show that the number of $\mathrm{SL}_2(\mathbb{Z})$-classes of reducible integer-matrix cubic forms of bounded reduced discriminant can be computed, up to a negligible error term, by counting the number of integer-matrix binary cubic forms $f(x,y)$ in the region whose x^3-coefficient is zero and x^2y-coefficient is positive. We then carry out the latter count explicitly.

4.1.1. *Reduction theory.* Recall that if $f(x,y)=ax^3+3bx^2y+3cxy^2+dy^3$ is a binary cubic form where a, b, c, $d\in\mathbb{Z}$, then there is a canonically associated quadratic form Q, called the *quadratic* (*Hessian*) *covariant* of f, with coefficients defined by (9):

$$Q(x,y)=Ax^2+Bxy+Cy^2,\quad\text{where } A=b^2-ac,\ B=ad-bc,\ \text{and } C=c^2-bd. \tag{20}$$

Note that $\mathrm{Disc}(Q)=\mathrm{disc}(f)$, and so if $\mathrm{disc}(f)$ is negative, then its quadratic covariant is definite. The group $\mathrm{SL}_2(\mathbb{Z})$ acts on the set of positive-definite real binary quadratic forms, and it is well known that a fundamental domain for this action consists of those quadratic forms whose coefficients satisfy

$$-A<B\leqslant A<C\quad\text{or}\quad 0\leqslant B\leqslant A=C. \tag{21}$$

We call a binary quadratic form whose coefficients satisfy (21) *reduced*. Any binary cubic form of negative reduced discriminant is $\mathrm{SL}_2(\mathbb{Z})$-equivalent to one whose quadratic covariant is *reduced*. Furthermore, if two such binary cubic forms are equivalent under $\mathrm{SL}_2(\mathbb{Z})$ and both have quadratic covariants that are reduced, then their quadratic covariants are equal. The automorphism group of a reduced quadratic form always includes the identity matrix Id_2 and its negation $-1\cdot\mathrm{Id}_2$. In all but two cases, this is the full automorphism group (the binary quadratic form x^2+y^2 has two more distinct automorphisms while x^2+xy+y^2 has four more distinct automorphisms).

We now describe bounds on the coefficients of a binary cubic form f with reduced quadratic covariant Q satisfying $0<-\mathrm{Disc}(Q)<X$.

LEMMA 26 ([7, Lemma 1]). *Let a, b, c, d be real numbers, and let A, B, C be defined as in (20). Suppose that*

$$-A<B\leqslant A\leqslant C \quad \text{and} \quad 0<4AC-B^2<X. \tag{22}$$

Then

$$\begin{aligned}&|a|<\frac{\sqrt{2}}{\sqrt[4]{3}}\cdot X^{1/4}, \quad |b|<\frac{\sqrt{2}}{\sqrt[4]{3}}\cdot X^{1/4},\\ &|ad|<\frac{2}{\sqrt{3}}\cdot X^{1/2}, \quad |bc|<\frac{2}{\sqrt{3}}\cdot X^{1/2},\\ &|ac^3|<\frac{4}{3}\cdot X, \quad |b^3d|<\frac{4}{3}\cdot X,\\ &|c^2(bc-ad)|<X.\end{aligned}$$

Note that in the previous lemma, we have included some non-reduced quadratic forms, specifically when $A=C$. However, such cases are negligible by the following lemma.

LEMMA 27 ([7, Lemma 2]). *The number of integral binary cubic forms satisfying*

$$-A<B\leqslant A\leqslant C \quad \text{and} \quad 0<4AC-B^2<X$$

such that $A=C$ is $O(X^{3/4}\log X)$.

Finally, the following lemma implies that the number of reducible integer-matrix binary cubic forms with reduced quadratic covariant and bounded reduced discriminant is asymptotically the same as the number of binary cubic forms with $a=0$, reduced quadratic covariant, and bounded reduced discriminant.

LEMMA 28 ([7, Lemma 3]). *The number of reducible integral binary cubic forms f with $a\neq 0$ that satisfy $-A<B\leqslant A\leqslant C$ and for which $0<-\mathrm{Disc}(Q)<X$ is $O(X^{3/4+\epsilon})$, for any $\epsilon>0$.*

Let $h(D)$ denote the number of $\mathrm{SL}_2(\mathbb{Z})$-classes of integer-matrix binary cubic forms of reduced discriminant D, and define $h'(D)$ to be the number of $\mathrm{SL}_2(\mathbb{Z})$-classes of integer-matrix binary cubic forms of reduced discriminant D having a representative with $a=0$ and quadratic covariant that satisfies $-A<B\leqslant A\leqslant C$. Then, by the previous two lemmas, we see that

$$\sum_{0<-D<X} h(D)=\sum_{0<-D<X} h'(D)+O(X^{3/4+\epsilon}). \tag{23}$$

Thus, we focus our attention on computing $\sum_{0<-D<X} h'(D)$.

4.1.2. *The number of binary cubic forms of bounded reduced discriminant with $a=0$, $b>0$, and reduced quadratic covariant.* If $f(x,y)=3bx^2y+3cxy^2+dy^3$, then the coefficients of the quadratic covariant of f are given by

$$A=b^2, \quad B=-bc, \quad \text{and} \quad C=c^2-bd,$$

and, furthermore, $\mathrm{disc}(f) = \mathrm{Disc}(Q) = -3b^2c^2 + 4b^3d$. We are interested in the number of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of integer-matrix binary cubic forms with $a = 0$ such that

$$-A < B \leqslant A \leqslant C \quad \text{and} \quad 0 < -\mathrm{Disc}(Q) < X. \tag{24}$$

Note that in order for $\mathrm{Disc}(Q)$ to be non-zero, we must have $b \neq 0$. Furthermore, the $\mathrm{SL}_2(\mathbb{Z})$-element $-\mathrm{Id}_2$ acts on a form $f(x,y)$ by negating its coefficients, and thus we can assume that our choice of representative for a given $\mathrm{SL}_2(\mathbb{Z})$-equivalence class has both $a = 0$ and non-negative b. Apart from the cases when $A = B = C$ or $A = C$ and $B = 0$, the restrictions $a = 0$ and $b > 0$ describe a unique representative in each $\mathrm{SL}_2(\mathbb{Z})$-equivalence class of forms satisfying (24) and $a = 0$. If $A = B = C$, then the binary cubic form is of the form $3bx^2y - 3bxy^2$. Similarly, if $A = C$ and $B = 0$, then a binary cubic form with such a quadratic covariant is of the form $3bx^2y - by^3$. Thus, by Lemma 26, there are $O(X^{1/4})$ such forms in the region described by (22) with $a = 0$. If we define $h'_1(D)$ to be the number of integer-matrix binary cubic forms of reduced discriminant D with $a = 0$, $b > 0$, and whose quadratic covariant satisfies $-A < B \leqslant A \leqslant C$, then, by (23), we also have

$$\sum_{0<-D<X} h(D) = \sum_{0<-D<X} h'_1(D) + O(X^{3/4+\epsilon}). \tag{25}$$

To compute $\sum_{0<-D<X} h'_1(D)$, note that the inequalities in (24) imply that $-b^2 < bc < b^2 \leqslant c^2 - 3bd$ and $0 < 3b^2c^2 - 4b^3d < X$ when $a = 0$; hence if $b > 0$, then

$$-b < c \leqslant b \quad \text{and} \quad d < \tfrac{3}{4} \cdot b.$$

Also, since $B^2 \leqslant AC$, we have $bd \leqslant 0$, so $d \leqslant 0$. Using the upper bound on the reduced discriminant of f and the inequality $A \leqslant C$ from (24), we conclude that

$$\frac{3c^2}{4b} - \frac{X}{4b^3} < d \leqslant \frac{c^2}{b} - b.$$

The number of integer-matrix binary cubic forms with $a = 0$ and $b > 0$ satisfying (24) is therefore

$$\begin{aligned}
\sum_{0<-D<X} h'_1(D) &= \sum_{0<b<(\sqrt{2}/\sqrt[4]{3})X^{1/4}} \sum_{-b<c\leqslant b} \#\left\{d \in \mathbb{Z} : \frac{3c^2}{4b} - \frac{X}{4b^3} < d \leqslant \frac{c^2}{b} - b\right\}\\
&= \sum_{0<b<(\sqrt{2}/\sqrt[4]{3})X^{1/4}} \sum_{-b<c\leqslant b} \left(\left(\frac{c^2}{b} - b\right) - \left(\frac{3c^2}{4b} - \frac{X}{4b^3}\right) + O(1)\right)\\
&= \sum_{0<b<(\sqrt{2}/\sqrt[4]{3})X^{1/4}} \left(2b \cdot \frac{X}{4b^3} + O(b^2)\right)\\
&= \frac{\zeta(2)}{2} X + O(X^{3/4}).
\end{aligned}$$

Thus, by (25) the number of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of reducible integer-matrix binary cubic forms having bounded negative reduced discriminant is given by

$$\sum_{0<-D<X} h(D) = \frac{\zeta(2)}{2} \cdot X + O(X^{3/4+\epsilon}).$$

4.1.3. *Restriction to projective forms.* We now complete the proof of Proposition 23 in the case of negative reduced discriminant by further restricting to projective forms. Let $h'_{1,\mathrm{proj}}(D)$ be the number of projective integer-matrix binary cubic forms of reduced discriminant D with $a = 0$, $b > 0$, and reduced quadratic covariant. By (11), we know that such a form is projective if and only if $(b^2, bc, c^2 - bd) = 1$, or equivalently if and only if $(b,c) = 1$. Thus $h'_{1,\mathrm{proj}}(D)$ counts those integer-matrix binary cubic forms having reduced discriminant D,

$a = 0$, $b > 0$, $(b, c) = 1$, and reduced quadratic covariant. Define $h'_{1,n}(D)$ to be the number of integer-matrix binary cubic forms of reduced discriminant D with $a = 0$, $b > 0$, $n \mid (b, c)$, and reduced quadratic covariant. Note that $h'_{1,1}(D) = h'_1(D)$. We compute $\sum_{0<-D<X} h'_{1,\mathrm{proj}}(D)$ by using the inclusion–exclusion principle:

$$\sum_{0<-D<X} h'_{1,\mathrm{proj}}(D) = \sum_{0<-D<X} \sum_{n=1}^{\infty} \mu(n) h'_{1,n}(D) = \sum_{n=1}^{\infty} \mu(n) \cdot \left(\sum_{0<-D<X} h'_{1,n}(D) \right),$$

where $\mu(\cdot)$ denotes the Möbius function.

Fix $n \in \mathbb{Z}$, and let $3bx^2y + 3cxy^2 + dy^3$ have reduced discriminant $D = -3b^2c^2 + 4b^3d$, $b > 0$, and $n \mid (b, c)$. Let $b = n \cdot b_1$ and $c = n \cdot c_1$. Assume that $A = b^2$, $B = -bc$, $C = c^2 - bd$ satisfy (24). Then

$$-b_1 < c_1 \leqslant b_1 \quad \text{and} \quad d < \tfrac{3}{4} n b_1.$$

Furthermore, $d \leqslant 0$ and d satisfies

$$\frac{3nc_1^2}{4b_1} - \frac{X}{4n^3b_1^3} < d \leqslant \frac{nc_1^2}{b_1} - nb_1.$$

Therefore, the number of integer-matrix binary cubic forms with $a = 0$, $b > 0$, and $n \mid (b, c)$ satisfying (24) is

$$\begin{aligned}
\sum_{0<-D<X} h'_{1,n}(D) &= \sum_{0<b_1<(\sqrt{2}/\sqrt[4]{3}n)X^{1/4}} \; \sum_{-b_1<c_1\leqslant b_1} \# \left\{ d : \frac{3nc_1^2}{4b_1} - \frac{X}{4n^3b_1^3} < d \leqslant \frac{nc_1^2}{b_1} - nb_1 \right\} \\
&= \sum_{0<b_1<(\sqrt{2}/\sqrt[4]{3}n)X^{1/4}} \; \sum_{-b_1<c_1\leqslant b_1} \left(\left(\frac{nc_1^2}{b_1} - nb_1 \right) - \left(\frac{3nc_1^2}{4b_1} - \frac{X}{4n^3b_1^3} \right) + O(1) \right) \\
&= \sum_{0<b_1<(\sqrt{2}/\sqrt[4]{3}n)X^{1/4}} \left(2b_1 \cdot \frac{X}{4n^3b_1^3} + O(nb_1^2) \right) \\
&= \frac{\zeta(2)}{2n^3} X + O\left(\frac{X^{3/4}}{n^2} \right),
\end{aligned}$$

where the implied constants are independent of n. We conclude that

$$\begin{aligned}
\sum_{0<-D<X} h'_{1,\mathrm{proj}}(D) &= \sum_{n=1}^{\infty} \mu(n) \cdot \left(\frac{\zeta(2)}{2n^3} X + O\left(\frac{X^{3/4}}{n^2} \right) \right) \\
&= \frac{\zeta(2)}{2\zeta(3)} \cdot X + O(X^{3/4}).
\end{aligned}$$

If we now let $h_{\mathrm{proj,red}}(D)$ denote the number of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of projective reducible integer-matrix cubic forms of reduced discriminant D, then by the analogous reduction formula as in (25), we obtain

$$\sum_{0<-D<X} h_{\mathrm{proj,red}}(D) = \frac{\zeta(2)}{2\zeta(3)} \cdot X + o(X).$$

4.2. *Counting reducible forms of positive reduced discriminant*

Recall that implicit in our study of reducible binary cubic forms of negative reduced discriminant was the fact that their quadratic covariants were definite, and thus the fundamental domain for positive definite quadratic forms allowed us to make a well-defined choice for a representative for each $\mathrm{SL}_2(\mathbb{Z})$-class of binary cubic forms we were counting. If $f(x, y) = ax^3 + 3bx^2y + 3cxy^2 + dy^3$ has positive reduced discriminant, then its quadratic covariant as defined in (20) is indefinite. However, if we can associate a different $\mathrm{SL}_2(\mathbb{Z})$-covariant quadratic form that is positive definite to each binary cubic form of positive reduced discriminant, then we can carry out the analogous count. Again, we follow Davenport [8] and note that a binary cubic form of the form $f(x,y) = ax^3 + 3bx^2y + 3cxy^2 + dy^3$ with positive reduced discriminant has one real root and two complex roots. Thus, if α denotes the real root, then we can write

$$f(x,y) = (y - \alpha \cdot x)(Px^2 + Qxy + Ry^2), \quad \text{where } P = 3b + 3c\alpha + d\alpha^2,\ Q = 3c + d\alpha,\ R = d.$$

We call the binary quadratic form with coefficients P, Q, and R the (*definite*) *quadratic factor* of the binary cubic form f.

4.2.1. *Reduction theory.* As in the case of reduced negative discriminant, a fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ consists of those real quadratic forms $Px^2 + Qxy + Ry^2$ whose coefficients satisfy

$$-P < Q \leqslant P < R \quad \text{or} \quad 0 \leqslant Q \leqslant P = R. \tag{26}$$

It is clear that any real binary cubic form having positive reduced discriminant is properly equivalent to one with quadratic factor satisfying the inequalities in (26). If there are two such binary cubic forms that are equivalent under $\mathrm{SL}_2(\mathbb{Z})$ and both quadratic factors satisfy (26), then the element of $\mathrm{SL}_2(\mathbb{Z})$ taking one cubic form to another must preserve the quadratic factor up to scaling. Thus, it must be an element of the automorphism group of the quadratic factor, hence either Id_2 or $-\mathrm{Id}_2$ when the quadratic factor is not a scalar multiple of $x^2 + y^2$ or $x^2 + xy + y^2$. Apart from these two exceptional cases, in each such $\mathrm{SL}_2(\mathbb{Z})$-equivalence class there is one binary cubic form with reduced quadratic factor and $b > 0$. Furthermore, using the fact that the non-reduced discriminant of a binary form is the product of the pairwise differences of the roots, one can show that

$$\mathrm{disc}(f) = \tfrac{1}{27}(4PR - Q^2)(P + Q\alpha + R\alpha^2)^2$$

if α, P, Q, R are defined as above. We now state the analogues of Lemmas 26–28.

LEMMA 29 ([8, Lemma 1]). *Let α, P, Q, R be real numbers satisfying*

$$-P < Q \leqslant P \leqslant R \quad \text{and} \quad 0 < \tfrac{1}{27}(4PR - Q^2)(P + Q\alpha + R\alpha^2)^2 < X. \tag{27}$$

If a, b, c, and d are given by the formulas

$$a = -P\alpha, \quad b = \frac{P - Q\alpha}{3}, \quad c = \frac{Q - R\alpha}{3}, \quad d = R,$$

then

$$\begin{aligned}
&a < \sqrt{6}X^{1/4}, \quad |b| < 2\sqrt[4]{\frac{2}{9}}X^{1/4},\\
&|ad| < 3\sqrt{2}X^{1/2}, \quad |bc| < \frac{4\sqrt{2}}{3}X^{1/2},\\
&|ac^3| < \frac{20}{3}X, \quad |b^3d| < \frac{20}{3}X,\\
&c^2|9bc - ad| < 432X.
\end{aligned}$$

LEMMA 30 ([8, Lemma 2]). *The number of integral binary cubic forms f satisfying*

$$-P < Q \leqslant P \leqslant R \quad \text{and} \quad 0 < \mathrm{disc}(f) < X$$

such that $P = R$ is $O(X^{3/4}\log X)$.

LEMMA 31 ([8, Lemma 3]). *The number of reducible integral binary cubic forms f with $a \neq 0$ that satisfy $-P < Q \leqslant P \leqslant R$ and for which $0 < \mathrm{disc}(f) < X$ is $O(X^{3/4+\epsilon})$, for any $\epsilon > 0$.*

Define $h'(D)$ to be the number of $\mathrm{SL}_2(\mathbb{Z})$-classes of integer-matrix binary cubic forms having reduced discriminant D with $a = 0$ and whose quadratic factor satisfies

$$-P < Q \leqslant P \leqslant R.$$

Then, by the previous two lemmas, we see that

$$\sum_{0<D<X} h(D) = \sum_{0<D<X} h'(D) + O(X^{3/4+\epsilon}). \tag{28}$$

Thus, we focus our attention on computing $\sum_{0<D<X} h'(D)$.

4.2.2. *The number of binary cubic forms of bounded reduced discriminant with $a = 0$, $b > 0$ and reduced quadratic factor.* If $f(x, y) = 3bx^2y + 3cxy^2 + dy^3$, then the coefficients of its quadratic factor are given by

$$P = 3b, \quad Q = 3c, \quad R = d.$$

Furthermore, $\mathrm{disc}(f) = -\frac{1}{27}\mathrm{Disc}(Px^2 + Qxy + Ry^2)P^2 = -3b^2c^2 + 4b^3d$. We are interested in the number of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of integer-matrix binary cubic forms f with $a = 0$ such that

$$-P < Q \leqslant P \leqslant R \quad \text{and} \quad 0 < \mathrm{disc}(f) < X.$$

Note that in order for the discriminant of f to be non-zero, we must have $b \neq 0$. Thus, we can assume that our choice of representative for a given $\mathrm{SL}_2(\mathbb{Z})$-equivalence class has both $a = 0$ and positive b. Apart from the cases when $P = Q = R$ or $P = R$ and $Q = 0$, the restrictions $a = 0$ and $b > 0$ describe a unique representative in each $\mathrm{SL}_2(\mathbb{Z})$-equivalence class of forms satisfying (26) and $a = 0$. If $P = Q = R$, then the binary cubic form is of the form $3bx^2y + 3bxy^2 + 3by^3$. Similarly, if $P = R$ and $Q = 0$, then the binary cubic form is of the form $3bx^2y + 3by^3$. Thus, by Lemma 29, there are $O(X^{1/4})$ such forms in the region described by (27) with $a = 0$. If we define $h'_1(D)$ to be the number of integer-matrix binary cubic forms having reduced discriminant D with $a = 0$ and $b > 0$ and whose quadratic factor satisfies $-P < Q \leqslant P \leqslant R$, then, by (28), we have

$$\sum_{0<D<X} h(D) = \sum_{0<D<X} h'_1(D) + O(X^{3/4+\epsilon}). \tag{29}$$

To compute $\sum_{0<D<X} h'_1(D)$, note that the inequalities in (27) imply that $-3b < 3c \leqslant 3b \leqslant d$ and $0 < -3b^2c^2 + 4b^3d < X$ when $a = 0$; hence if $b > 0$, then

$$-b < c \leqslant b \quad \text{and} \quad 3b < d.$$

Thus $d > 0$. Using the upper bound on the reduced discriminant of f, we conclude that

$$3b < d < \frac{X}{4b^3} + \frac{3c^2}{4b}.$$

Therefore, the number of integer-matrix binary cubic forms with $a = 0$ and $b > 0$ satisfying (27) is

$$\begin{aligned}
\sum_{0<D<X} h'_1(D) &= \sum_{0<b<\sqrt[4]{32/9}X^{1/4}} \sum_{-b<c\leqslant b} \#\left\{d : 3b < d < \frac{X}{4b^3} + \frac{3c^2}{4b}\right\} \\
&= \sum_{0<b<\sqrt[4]{32/9}X^{1/4}} \sum_{-b<c\leqslant b} \left(\frac{X}{4b^3} + \frac{3c^2}{4b} - 3b + O(1)\right) \\
&= \sum_{0<b<\sqrt[4]{32/9}X^{1/4}} \left(2b \cdot \frac{X}{4b^3} + O(b^2)\right) = \frac{\zeta(2)}{2}X + O(X^{3/4}).
\end{aligned}$$

Hence, by (29), the number of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of reducible integer-matrix binary cubic forms of bounded positive reduced discriminant is given by

$$\sum_{0<D<X} h(D) = \frac{\zeta(2)}{2} \cdot X + O(X^{3/4+\epsilon}).$$

4.2.3. *Restriction to projective forms.* We have seen that the number of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of reducible integer-matrix binary cubic forms with positive reduced discriminant less than X is $(\zeta(2)/2)X + o(X)$. We complete the proof of Proposition 23 by further restricting to projective forms. Let $h'_{1,\mathrm{proj}}(D)$ be the number of projective integer-matrix binary cubic forms having reduced discriminant D, $a = 0$, $b > 0$, and reduced definite quadratic factor. By (11), we know that such a form is projective if and only if $(b^2, bc, c^2 - bd) = 1$, or equivalently if and only if $(b, c) = 1$. Thus, $h'_{1,\mathrm{proj}}(D)$ counts those integer-matrix forms having reduced discriminant D, $a = 0$, $b > 0$, $(b, c) = 1$, and reduced quadratic factor. Define $h'_{1,n}(D)$ to be the number of $\mathrm{SL}_2(\mathbb{Z})$-classes of integer-matrix binary cubic forms having reduced discriminant D, $a = 0$, $b > 0$, $n \mid (b, c)$, and reduced quadratic factor. Then we have $h'_{1,1}(D) = h'_{1,\mathrm{proj}}(D)$. As before, we compute $\sum_{0<D<X} h'_{1,\mathrm{proj}}(D)$ by using the inclusion–exclusion principle:

$$\sum_{0<D<X} h'_{1,\mathrm{proj}}(D) = \sum_{0<D<X} \sum_{n=1}^{\infty} \mu(n) h'_{1,n}(D) = \sum_{n=1}^{\infty} \mu(n) \cdot \left(\sum_{0<D<X} h'_{1,n}(D) \right).$$

Fix $n \in \mathbb{Z}$, and let $3bx^2y + 3cxy^2 + dy^3$ have reduced discriminant $D = -3b^2c^2 + 4b^3d$, $b > 0$, and $n \mid (b, c)$. Let $b = n \cdot b_1$ and $c = n \cdot c_1$. Assume that P, Q, R satisfy (26); then

$$-b_1 < c_1 \leqslant b_1 \quad \text{and} \quad 3nb_1 < d.$$

Furthermore, $d > 0$ and d satisfies

$$3nb_1 < d < \frac{X}{4n^3b_1^3} - \frac{3nc_1^2}{4b_1}.$$

Therefore, the number of integer-matrix binary cubic forms with $a = 0$, $b > 0$, and $n \mid (b, c)$ satisfying (26) is

$$\begin{aligned}
\sum_{0<D<X} h'_{1,n}(D) &= \sum_{0<b_1<\sqrt[4]{32/9n}X^{1/4}} \; \sum_{-b_1<c_1\leqslant b_1} \# \left\{ d : 3nb_1 < d < \frac{X}{4n^3b_1^3} + \frac{3nc_1^2}{4b_1} \right\} \\
&= \sum_{0<b_1<\sqrt[4]{32/9n}X^{1/4}} \; \sum_{-b_1<c_1\leqslant b_1} \left(\frac{X}{4n^3b_1^3} + \frac{3nc_1^2}{4b_1} - 3nb_1 + O(1) \right) \\
&= \sum_{0<b_1<\sqrt[4]{32/9n}X^{1/4}} \left(2b_1 \cdot \frac{X}{4n^3b_1^3} + O(nb_1^2) \right) \\
&= \frac{\zeta(2)}{2n^3} X + O\left(\frac{X^{3/4}}{n^2} \right),
\end{aligned}$$

where the implied constants are again independent of n. We conclude that

$$\begin{aligned}
\sum_{0<D<X} h'_{1,\mathrm{proj}}(D) &= \sum_{n=1}^{\infty} \mu(n) \cdot \left(\frac{\zeta(2)}{2n^3} X + O\left(\frac{X^{3/4}}{n^2} \right) \right) \\
&= \frac{\zeta(2)}{2\zeta(3)} X + O(X^{3/4}).
\end{aligned}$$

If we let $h_{\mathrm{proj,red}}(D)$ denote the number of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of projective reducible integer-matrix binary cubic forms of reduced discriminant D, then by the analogous reduction formula as in (25), we obtain

$$\sum_{0<D<X} h_{\mathrm{proj,red}}(D) = \frac{\zeta(2)}{2\zeta(3)} \cdot X + o(X).$$

5. *The mean number of* 3*-torsion elements in class groups of quadratic orders via ring class field theory* (*Proofs of Theorems* 2 *and* 3)

In the previous sections, we have proven Theorems 1, 2, and 6 without appealing to class field theory. To prove Theorem 3 and Corollary 4, we use a generalization of the class field theory argument originally due to Davenport and Heilbronn. In particular, we show that the elements of $\mathrm{Cl}_3(\mathcal{O})$ for a quadratic order $\mathcal{O}$ can be enumerated via certain non-Galois cubic fields. This involves the theory of ring class fields (see [**6**, Section 9]), together with the theorem of Davenport and Heilbronn on the density of discriminants of cubic fields.

THEOREM 32 ([**9**]). *Let $N_3(\xi,\eta)$ denote the number of cubic fields K up to isomorphism that satisfy $\xi < \mathrm{Disc}(K) < \eta$. Then*

$$N_3(0,X) = \frac{1}{12\zeta(3)}X + o(X) \quad \textit{and} \quad N_3(-X,0) = \frac{1}{4\zeta(3)}X + o(X).$$

Using class field theory, Davenport and Heilbronn were able to deduce Theorem 1 using this count. The new contribution of this section is to extend their argument to all orders and to acceptable sets of orders, using the theory of ring class fields, thus re-proving Theorem 2 from this perspective and also proving Theorem 3.

5.1. *Ring class fields associated to quadratic orders*

For a fixed quadratic order $\mathcal{O}$, let k denote the field $\mathcal{O}\otimes\mathbb{Q}$, and let $\mathcal{O}_k$ denote the maximal order in k. If $[\mathcal{O}_k : \mathcal{O}] = f$, then we say that the *conductor* of $\mathcal{O}$ is equal to f (or sometimes, the ideal in $\mathcal{O}_k$ generated by f).

We begin with a well-known description of $\mathrm{Cl}(\mathcal{O})$ in terms of ideal classes of $\mathcal{O}_k$:

LEMMA 33 ([**6**, Proposition 7.22]). *Let $I_k(f)$ denote the subgroup of the group of invertible ideals of $\mathcal{O}_k$ consisting of ideals that are prime to f, and let $P_{k,\mathbb{Z}}(f)$ denote the subgroup of the group of principal ideals of $\mathcal{O}_k$ consisting of those (α) such that $\alpha \equiv a \pmod{f\mathcal{O}_k}$ for some integer a that is coprime to f. Then*

$$\mathrm{Cl}(\mathcal{O}) \cong I_k(f)/P_{k,\mathbb{Z}}(f).$$

Recall that the *ray class group* of k of conductor f is defined as the quotient $\mathrm{Cl}_k(f) := I_k(f)/P_{k,1}(f)$, where $P_{k,1}(f)$ is the subgroup of principal ideals of $\mathcal{O}_k$ consisting of those (α) such that $\alpha \equiv 1 \pmod{f\mathcal{O}_k}$. By Lemma 33, we have the following exact sequence:

$$1 \longrightarrow P_{k,\mathbb{Z}}(f)/P_{k,1}(f) \longrightarrow \mathrm{Cl}_k(f) \longrightarrow \mathrm{Cl}(\mathcal{O}) \longrightarrow 1. \tag{30}$$

Let σ denote the non-trivial automorphism of $\mathrm{Gal}(k/\mathbb{Q})$. For a finite abelian group G, let $G[3]$ denote its 3-Sylow subgroup, and if G is a finite $\mathrm{Gal}(k/\mathbb{Q})$-module, then we can decompose $G[3] = G[3]^+ \oplus G[3]^-$, where $G[3]^\pm := \{g \in G : \sigma(g) = g^{\pm 1}\}$.

LEMMA 34 ([**13**, Lemma 1.10]). *If $\mathcal{O}$ is a quadratic order of conductor f, k the quadratic field $\mathcal{O}\otimes\mathbb{Q}$, and $\mathrm{Cl}_k(f)$ the ray class group of k of conductor f, then $\mathrm{Cl}_k(f)[3]^- \cong \mathrm{Cl}(\mathcal{O})[3]$.*

Proof. It is clear that the exact sequence in (30) is a sequence of finite $\mathrm{Gal}(k/\mathbb{Q})$-modules, implying the exactness of the following sequences:

$$1 \longrightarrow (P_{k,\mathbb{Z}}(f)/P_{k,1}(f))[3]^{+} \longrightarrow \mathrm{Cl}_k(f)[3]^{+} \longrightarrow \mathrm{Cl}(\mathcal{O})[3]^{+} \longrightarrow 1,$$
$$1 \longrightarrow (P_{k,\mathbb{Z}}(f)/P_{k,1}(f))[3]^{-} \longrightarrow \mathrm{Cl}_k(f)[3]^{-} \longrightarrow \mathrm{Cl}(\mathcal{O})[3]^{-} \longrightarrow 1.$$

We see that $(P_{k,\mathbb{Z}}(f)/P_{k,1}(f))[3]^{-}$ is trivial, since any element $[(\alpha)]$ such that $\alpha \equiv a \pmod{f\mathcal{O}_k}$, for some integer a that is coprime to f, can also be represented by $a\mathcal{O}_k$. Moreover, for any such class $[a\mathcal{O}_k] \in (P_{k,\mathbb{Z}}(f)/P_{k,1}(f))[3]^{-}$, we must have

$$[a\mathcal{O}_k] = [\sigma(a\mathcal{O}_k)] = [a\mathcal{O}_k]^{-1}.$$

Hence $[a\mathcal{O}_k]$ has order dividing 2 and equal to a power of 3, and so must be trivial. Similarly, $\mathrm{Cl}(\mathcal{O})[3]^{+}$ is trivial since if $[I] \in \mathrm{Cl}(\mathcal{O})[3]^{+}$, then $[I] = [\sigma(I)]$. Because $N(I) = \sigma(I)I \in \mathbb{Z}$, $[I]$ has order dividing 2 and equal to a power of 3 in $\mathrm{Cl}(\mathcal{O})$, and is therefore trivial. □

PROPOSITION 35. *Let $\mathcal{O}$ be a quadratic order. The number of isomorphism classes of cubic fields K such that* $\mathrm{Disc}(\mathcal{O}) = c^2\mathrm{Disc}(K)$ *for some integer c is* $(|\mathrm{Cl}_3(\mathcal{O})| - 1)/2$.

Proof. We prove the proposition by showing that such isomorphism classes of cubic fields K are in bijection with subgroups of $\mathrm{Cl}(\mathcal{O})$ of index 3.

We first show how to associate a quadratic order $\mathcal{O}$ and an index 3 subgroup H of $\mathrm{Cl}(\mathcal{O})[3]$ to any non-cyclic cubic extension K of $\mathbb{Q}$. If K is a non-Galois cubic field, then the normal closure $\widetilde{K}$ of K over $\mathbb{Q}$ contains a unique quadratic field k. One checks that the discriminants of K and k satisfy $\mathrm{Disc}(K) = \mathrm{Disc}(k)f^2$, where f is the conductor of the cubic extension $\widetilde{K}/k$ (see [**12**] or [4, Theorem 9.2.6]). By class field theory, $\widetilde{K}/k$ corresponds to a subgroup H of $\mathrm{Cl}_k(f)[3]$ of index 3. Since $\widetilde{K}/\mathbb{Q}$ is a Galois extension, H is a $\mathrm{Gal}(k/\mathbb{Q})$-module. If σ denotes the non-trivial automorphism in $\mathrm{Gal}(k/\mathbb{Q})$, then we see that $\widetilde{K}$ is Galois over $\mathbb{Q}$ if and only if $\sigma(\widetilde{K}) = \widetilde{K}$. Artin reciprocity implies that the subgroup of $\mathrm{Cl}_k(f)[3]$ corresponding to $\sigma(\widetilde{K})$ is the image of H under the action of σ on $\mathrm{Cl}_k(f)[3]$. As $\widetilde{K}$ is Galois, we conclude that H is stable under σ, and we can write $H = H^+ \oplus H^-$ where $H^{\pm} := H \cap \mathrm{Cl}_k(f)[3]^{\pm}$.

We now show that $H^+ = \mathrm{Cl}_k(f)[3]^+$. Consider the exact sequence

$$1 \longrightarrow \mathrm{Gal}(\widetilde{K}/k) \longrightarrow \mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \longrightarrow \mathrm{Gal}(k/\mathbb{Q}) \longrightarrow 1. \tag{31}$$

Note that, by definition, $\mathrm{Gal}(\widetilde{K}/k) \cong \mathrm{Cl}_k(f)[3]/H$. For any lift of σ to $\tilde{\sigma} \in \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$, Artin reciprocity implies that the action of conjugation on $\mathrm{Gal}(\widetilde{K}/k)$ by $\tilde{\sigma}$ corresponds to the action of σ on $\mathrm{Cl}_k(f)[3]/H$. Since $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ is isomorphic to the symmetric group (and is not a direct product), conjugation $\mathrm{Gal}(\widetilde{K}/k)$ acts as inversion. Since the index of H in $\mathrm{Cl}_k(f)[3]$ is of odd prime order, either $H^+ = \mathrm{Cl}_k(f)[3]^+$ or $H^- = \mathrm{Cl}_k(f)[3]^-$. For $\tilde{\sigma}$ to act as inversion on $\mathrm{Cl}_k(f)[3]/H$, we must have $\mathrm{Cl}_k(f)[3]/H \cong \mathrm{Cl}_k(f)[3]^-/H^-$. By Lemma 34, H corresponds to a subgroup of $\mathrm{Cl}(\mathcal{O})[3]$ of index 3, where $\mathcal{O}$ is the unique quadratic order of index f in the ring of integers $\mathcal{O}_k$.

It remains to show that, for any given order $\mathcal{O}$ in a quadratic field k, each index three subgroup of $\mathrm{Cl}(\mathcal{O})$ corresponds in this way to a unique cubic field K up to isomorphism. Let H be a subgroup of $\mathrm{Cl}(\mathcal{O})[3] \cong \mathrm{Cl}_k(f)[3]^-$ of index 3 where $\mathcal{O}$ has index f in $\mathcal{O}_k$. Then H corresponds to a cubic extension $\widetilde{K}/k$ of conductor $d \mid f$, and the action of σ is by inversion. Hence the exact sequence (31) does not split, and $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) = \mathrm{Gal}(\widetilde{K}/k) \rtimes \mathrm{Gal}(k/\mathbb{Q}) \cong S_3$, and thus $\widetilde{K}$ is the Galois closure of a unique cubic field K up to isomorphism.

We conclude that

$$\begin{aligned}\sum_{d|f} \#\{\text{cubic fields } K \text{ such that } \mathrm{Disc}(K) = d^2\mathrm{Disc}(k)\} \\ = \#\{\text{subgroups of } \mathrm{Cl}(\mathcal{O}) \text{ of index } 3\} = \frac{1}{2}(|\mathrm{Cl}_3(\mathcal{O})| - 1),\end{aligned} \tag{32}$$

where $\mathcal{O}$ is the quadratic order of index f in the maximal order of k, that is, $\mathcal{O}$ is the unique quadratic order with discriminant equal to $f^2\mathrm{Disc}(k)$; note that conjugate cubic fields are counted only once, and so we have obtained the desired statement (with $c = f/d$). □

The integer c corresponding to a cubic field K via Proposition 35 is called the *conductor* of K relative to $\mathcal{O}$. In particular, we see that the conductor c of K relative to $\mathcal{O}$ must divide the conductor f of $\mathcal{O}$.

5.2. *A second proof of the mean number of* 3*-torsion elements in the class groups of quadratic orders* (*Proof of Theorem* 2 *via class field theory*)

Proposition 35 shows that Theorem 2 may be proved by summing, over all quadratic orders $\mathcal{O}$ of absolute discriminant less than X, the number of cubic fields K such that $\mathrm{Disc}(\mathcal{O})/\mathrm{Disc}(K)$ is a square. However, in this sum, a single cubic field K may be counted a number of times since there are many $\mathcal{O}$ for which $\mathrm{Disc}(\mathcal{O})/\mathrm{Disc}(K)$ is a square, and one must control the asymptotic behavior of this sum as $X \to \infty$.

To accomplish this, we rearrange the sum as a sum over the conductor f of $\mathcal{O}$, and then sum over $\mathcal{O}$ in the interior of this main sum. This allows us to use a uniformity estimate for large f, yielding the desired asymptotic formulae. More precisely, for X large and $i = 0, 1$, we are interested in evaluating

$$N^{(i)}(X) := \sum_{0<(-1)^i\mathrm{Disc}(\mathcal{O})<X} \#\left\{\text{cubic fields } K \text{ such that } \frac{\mathrm{Disc}(\mathcal{O})}{\mathrm{Disc}(K)} = c^2,\, c \in \mathbb{Z}\right\}. \tag{33}$$

We rearrange this as a sum over c and subsequently over cubic fields:

$$\begin{aligned}N^{(i)}(X) &= \sum_{c=1}^{\infty} \sum_{0<(-1)^i\mathrm{Disc}(\mathcal{O})<X} \#\left\{\text{cubic fields } K \text{ such that } \mathrm{Disc}(K) = \frac{\mathrm{Disc}(\mathcal{O})}{c^2}\right\} \\ &= \sum_{c=1}^{\infty} \sum_{\substack{\text{non-Galois } K \text{ s.t.} \\ 0<(-1)^i\mathrm{Disc}(K)<X/c^2}} 1.\end{aligned} \tag{34}$$

Let Y be an arbitrary positive integer. From (34) and Theorem 32, we obtain

$$\begin{aligned}N^{(i)}(X) &= \sum_{c=1}^{Y-1} \frac{1}{2n_i\zeta(3)} \cdot \frac{X}{c^2} + o(X) + O\left(\sum_{c=Y}^{\infty} X/c^2\right) \\ &= \sum_{c=1}^{Y-1} \frac{1}{2n_i\zeta(3)} \cdot \frac{X}{c^2} + o(X) + O(X/Y),\end{aligned}$$

where $n_0 = 6$ and $n_1 = 2$ (that is, n_i is the size of the automorphism group of $\mathbb{R}^3$ if $i = 0$ and $\mathbb{R} \otimes \mathbb{C}$ if $i = 1$). Thus,

$$\lim_{X\to\infty} \frac{N^{(i)}(X)}{X} = \sum_{c=1}^{Y-1} \frac{1}{2n_i\zeta(3)} \cdot \frac{1}{c^2} + O(1/Y).$$

Letting Y tend to ∞, we conclude that

$$\lim_{X\to\infty}\frac{N^{(i)}(X)}{X}=\sum_{c=1}^{\infty}\frac{1}{2n_i\zeta(3)}\cdot\frac{1}{c^2}=\frac{\zeta(2)}{2n_i\zeta(3)}.$$

Finally, using Proposition 35 and (18), we obtain

$$\lim_{X\to\infty}\frac{\sum_{0<(-1)^i\mathrm{Disc}(\mathcal{O})<X}|\mathrm{Cl}_3(\mathcal{O})|}{\sum_{0<(-1)^i\mathrm{Disc}(\mathcal{O})<X}1}=1+\lim_{X\to\infty}\frac{4\cdot N^{(i)}(X)}{X}=\begin{cases}1+\dfrac{\zeta(2)}{3\zeta(3)} & \text{if } i=0,\\ 1+\dfrac{\zeta(2)}{\zeta(3)} & \text{if } i=1.\end{cases}$$

5.3. *The mean number of 3-torsion elements in the class groups of quadratic orders in acceptable families* (*Proof of Theorem* 3)

We now determine the mean number of 3-torsion elements in the class groups of quadratic orders satisfying any acceptable set of local conditions. As described in the introduction, for each prime p, let Σ_p be a set of isomorphism classes of non-degenerate quadratic rings over $\mathbb{Z}_p$. Recall that a collection $\Sigma=(\Sigma_p)$ is *acceptable* if, for all sufficiently large p, the set Σ_p contains the maximal quadratic rings over $\mathbb{Z}_p$. We denote by Σ the set of quadratic orders $\mathcal{O}$ over $\mathbb{Z}$, up to isomorphism, such that $\mathcal{O}\otimes\mathbb{Z}_p\in\Sigma_p$ for all p. For a quadratic order $\mathcal{O}$, we write '$\mathcal{O}\in\Sigma$' (or say that '$\mathcal{O}$ is a Σ-order') if $\mathcal{O}\otimes\mathbb{Z}_p\in\Sigma_p$ for all primes p.

Let us fix an acceptable collection $\Sigma=(\Sigma_p)$ of local specifications. We first recall a necessary generalization of Theorem 32.

THEOREM 36 ([**3**, Theorem 8]). *Let* $(\Sigma_p^{(3)})\cup\Sigma_\infty^{(3)}$ *be an acceptable collection of local specifications* for cubic orders, *that is, for all sufficiently large primes* p, $\Sigma_p^{(3)}$ *contains all maximal cubic rings over* $\mathbb{Z}_p$ *that are not totally ramified. Let* $\Sigma^{(3)}$ *denote the set of all isomorphism classes of orders* $\mathcal{O}_3$ *in cubic fields for which* $\mathcal{O}_3\otimes\mathbb{Q}_p\in\Sigma_p^{(3)}$ *for all* p *and* $\mathcal{O}_3\otimes\mathbb{R}\in\Sigma_\infty^{(3)}$, *and denote by* $N_3(\Sigma^{(3)},X)$ *the number of cubic orders* $\mathcal{O}_3\in\Sigma^{(3)}$ *that satisfy* $|\mathrm{Disc}(\mathcal{O}_3)|<X$. *Then*

$$N_3(\Sigma^{(3)},X)=\left(\frac{1}{2}\sum_{R_3\in\Sigma_\infty^{(3)}}\frac{1}{|\mathrm{Aut}(R_3)|}\right)\cdot\prod_p\left(\frac{p-1}{p}\cdot\sum_{R_3\in\Sigma_p^{(3)}}\frac{1}{\mathrm{Disc}_p(R_3)}\cdot\frac{1}{|\mathrm{Aut}(R_3)|}\right)\cdot X+o(X),$$

where $\mathrm{Disc}_p(\cdot)$ *denotes the* p*-power of* $\mathrm{Disc}(\cdot)$.

We can use the above theorem to prove Theorem 3 by comparing the number of 3-torsion elements in the class groups of quadratic Σ-orders $\mathcal{O}$ of absolute discriminant less than X and the number of cubic fields corresponding to such class group elements of $\mathcal{O}\in\Sigma$ with absolute discriminant less than X via Proposition 35. Analogous to (33), we define

$$\begin{aligned}N^{(i)}(X,\Sigma)&:=\sum_{\substack{\mathcal{O}\in\Sigma\text{ s.t.}\\0<(-1)^i\mathrm{Disc}(\mathcal{O})<X}}\#\left\{\text{cubic fields } K \text{ such that } \frac{\mathrm{Disc}(\mathcal{O})}{\mathrm{Disc}(K)}=c^2, c\in\mathbb{Z}\right\}\\&=\sum_{c=1}^{\infty}\sum_{\substack{\mathcal{O}\in\Sigma\text{ s.t.}\\0<(-1)^i\mathrm{Disc}(\mathcal{O})<X}}\#\left\{\text{cubic fields } K \text{ such that } \mathrm{Disc}(K)=\frac{\mathrm{Disc}(\mathcal{O})}{c^2}\right\}.\end{aligned}\tag{35}$$

For any $c\in\mathbb{Z}$, let $c^{-2}\Sigma$ denote the set of quadratic orders $\mathcal{O}$ that contain an index c Σ-order. We can decompose $c^{-2}\Sigma$ into the following local specifications: for all p, if $p^{c_p}\mid\mid c$ where $c_p\in\mathbb{Z}_{\geqslant 0}$, let $p^{-2c_p}\Sigma_p$ denote the set of non-degenerate quadratic rings over $\mathbb{Z}_p$ which contain an index p^{c_p} subring that lies in Σ_p. It is then clear that $(p^{-2c_p}\Sigma_p)=c^{-2}\Sigma$ is acceptable since Σ is.

Finally, let $\Sigma^{(3),c}$ be the set of cubic fields K such that there exists a quadratic order $\mathcal{O} \in c^{-2}\Sigma$ with $\mathrm{Disc}(K) = \mathrm{Disc}(\mathcal{O})$. These are the set of cubic fields K such that their *quadratic resolvent ring* contains a Σ-order with index c, or equivalently, is a $c^{-2}\Sigma$-order. Let $D(K)$ denote the quadratic resolvent ring of the cubic field K, that is, $D(K)$ is the unique quadratic order with discriminant equal to that of K. The local specifications for $\Sigma^{(3),c}$ are as follows: for all p and with c_p defined as above, $\Sigma_p^{(3),c_p}$ is the set of étale cubic algebras K_p over $\mathbb{Q}_p$ such that the quadratic resolvent ring $D(K_p)$ over $\mathbb{Z}_p$ is a $p^{-2c_p}\Sigma_p$-order. Meanwhile, $\Sigma_\infty^{(3),c}$ has one cubic ring over $\mathbb{R}$ specified by the choice $i = 0$ or 1: it contains $\mathbb{R}^3$ if $i = 0$ and $\mathbb{R} \otimes \mathbb{C}$ if $i = 1$. Then $\Sigma^{(3),c} = (\Sigma_p^{(3),c_p}) \cup \Sigma_\infty^{(3),c}$, and in order to use Theorem 36, it remains to show that $\Sigma^{(3),c}$ is acceptable.

To show the acceptability of $\Sigma^{(3),c}$, consider any $p > 2$ large enough so that Σ_p contains all maximal quadratic rings and $c_p = 0$, that is, $p \nmid c$. Let K_p be an étale cubic algebra over $\mathbb{Q}_p$ that is not totally ramified. This implies that $p^2 \nmid \mathrm{Disc}(K_p)$, and so $p^2 \nmid D(K_p)$; therefore, $D(K_p)$ must be maximal. By our choice of p, we have $D(K_p) \in \Sigma_p$, and so $K_p \in \Sigma^{(3),c}$. Hence $\Sigma^{(3),c}$ is acceptable.

Using these definitions, we can rewrite $N^{(i)}(X, \Sigma)$ as

$$\begin{aligned} N^{(i)}(X,\Sigma) &= \sum_{c=1}^{\infty} \sum_{\substack{\mathcal{O}\in\Sigma \text{ s.t.} \\ 0<(-1)^i\mathrm{Disc}(\mathcal{O})<X}} \#\left\{\text{cubic fields } K \text{ such that } \mathrm{Disc}(K) = \frac{\mathrm{Disc}(\mathcal{O})}{c^2}\right\} \\ &= \sum_{c=1}^{\infty} \sum_{\substack{\mathcal{O}\in c^{-2}\Sigma \text{ s.t.} \\ 0<(-1)^i\mathrm{Disc}(\mathcal{O})<X/c^2}} \#\{\text{cubic fields } K \text{ such that } \mathrm{Disc}(K) = \mathrm{Disc}(\mathcal{O})\} \\ &= \sum_{c=1}^{\infty} \sum_{\substack{K\in\Sigma^{(3),c} \text{ s.t.} \\ 0<(-1)^i\mathrm{Disc}(K)<X/c^2}} 1 = \sum_{c=1}^{\infty} N_3\left(\Sigma^{(3),c}, \frac{X}{c^2}\right). \end{aligned} \tag{36}$$

Again, let Y be an arbitrary positive integer. From (36), Theorem 36, and Theorem 32, we obtain

$$\begin{aligned} N^{(i)}(X,\Sigma) = \sum_{c=1}^{Y-1} \frac{1}{2n_i} \cdot \prod_p \left(\frac{p-1}{p} \cdot \sum_{K_p\in\Sigma_p^{(3),c_p}} \frac{1}{\mathrm{Disc}_p(K_p)} \cdot \frac{1}{|\mathrm{Aut}(K_p)|} \right) \cdot \frac{X}{c^2} \\ + O\left(\sum_{c=Y}^{\infty} X/c^2\right) + o(X), \end{aligned}$$

where $n_0 = 6$ and $n_1 = 2$ as before. Thus, since $O(\sum_{c=Y}^{\infty} X/c^2) = O(X/Y)$, we have

$$\lim_{X\to\infty} \frac{N^{(i)}(X,\Sigma)}{X} = \sum_{c=1}^{Y-1} \frac{1}{2n_i} \cdot \prod_p \left(\frac{p-1}{p} \cdot \sum_{K_p\in\Sigma_p^{(3),c_p}} \frac{1}{\mathrm{Disc}_p(K_p)} \cdot \frac{1}{|\mathrm{Aut}(K_p)|} \right) \cdot \frac{1}{c^2} + O(1/Y).$$

Letting Y tend to ∞, we conclude that

$$\lim_{X\to\infty} \frac{N^{(i)}(X,\Sigma)}{X} = \sum_{c=1}^{\infty} \frac{1}{2n_i} \cdot \prod_p \left(\frac{p-1}{p} \cdot \sum_{K_p\in\Sigma_p^{(3),c_p}} \frac{1}{\mathrm{Disc}_p(K_p)} \cdot \frac{1}{|\mathrm{Aut}(K_p)|} \right) \cdot \frac{1}{c^2}.$$

Let M_Σ be defined as in (3) and let M_Σ^{eq} be the following product of local masses:

$$M_\Sigma^{\mathrm{eq}} := \prod_p \frac{\sum_{R\in\Sigma_p} C^{\mathrm{eq}}(R)/\mathrm{Disc}_p(R)}{\sum_{R\in\Sigma_p} 1/\mathrm{Disc}_p(R)\cdot 1/\#\mathrm{Aut}(R)}$$
$$= \prod_p \frac{\sum_{R\in\Sigma_p} C^{\mathrm{eq}}(R)/\mathrm{Disc}_p(R)}{\sum_{R\in\Sigma_p} 1/(2\cdot \mathrm{Disc}_p(R))}, \tag{37}$$

where $C^{\mathrm{eq}}(R)$ is defined for an étale quadratic algebra R over $\mathbb{Z}_p$ as the (weighted) number of étale cubic algebras K_p over $\mathbb{Q}_p$ such that $R = D(K_p)$:

$$C^{\mathrm{eq}}(R) := \sum_{\substack{K_p \text{ étale cubic } /\mathbb{Q}_p\\ \text{s.t. } R=D(K_p)}} \frac{1}{\#\mathrm{Aut}(K_p)}.$$

Then

$$\lim_{X\to\infty} \frac{N^{(i)}(X,\Sigma)}{X} = \frac{1}{2n_i}\cdot\sum_{c=1}^{\infty}\frac{1}{c^2}\cdot\prod_p\left(\frac{p-1}{p}\cdot\sum_{K_p\in\Sigma_p^{(3),c_p}}\frac{1}{\mathrm{Disc}_p(K_p)}\cdot\frac{1}{|\mathrm{Aut}(K_p)|}\right)$$
$$= \frac{1}{2n_i}\cdot\sum_{c=1}^{\infty}\frac{1}{c^2}\cdot\prod_p\left(\frac{p-1}{p}\cdot\sum_{R\in p^{-2c_p}\Sigma_p}\frac{1}{\mathrm{Disc}_p(R)}\cdot C^{\mathrm{eq}}(R)\right)$$
$$= \frac{1}{2n_i}\cdot\prod_p\left(\frac{p-1}{p}\cdot\sum_{i=0}^{\infty}\sum_{\substack{R\in\Sigma_p \text{ s.t.}\\ \exists R' \text{ s.t. } [R':R]=p^i}}\frac{1}{\mathrm{Disc}_p(R)}\cdot C^{\mathrm{eq}}(R')\right)$$
$$= \frac{1}{2n_i}\cdot\prod_p\left(\frac{p-1}{p}\cdot\sum_{R\in\Sigma_p}\frac{1}{\mathrm{Disc}_p(R)}\cdot C(R)\right). \tag{38}$$

Recall that $C(R)$ is defined as the (weighted) number of etale cubic algebras K_p over $\mathbb{Q}_p$ such that $R\subset D(K_p)$ (cf. equation (2)). The final equality follows from the fact that if we fix $R\in\Sigma_p$, the cubic algebras K_p with discriminant $p^{2i}\cdot\mathrm{Disc}_p(R)$ are disjoint for distinct choices of i. (The penultimate equality follows from unique factorization of integers.)

Using (32) and (35), we see that

$$2\cdot N^{(i)}(X,\Sigma) = \sum_{\substack{\mathcal{O}\in\Sigma \text{ s.t.}\\ 0<(-1)^i\mathrm{Disc}(\mathcal{O})<X}} (\#\mathrm{Cl}_3(\mathcal{O})-1). \tag{39}$$

We now have the following elementary lemma counting quadratic orders.

Lemma 37 ([2, §4]). (a) *The number of real* Σ*-orders* $\mathcal{O}$ *with* $|\mathrm{Disc}(\mathcal{O})|<X$ *is asymptotically*

$$\frac{1}{2}\cdot\prod_p\left(\frac{p-1}{p}\cdot\sum_{R\in\Sigma}\frac{1}{\mathrm{Disc}_p(R)}\cdot\frac{1}{\#\mathrm{Aut}(R)}\right)\cdot X.$$

(b) *The number of complex* Σ*-orders* $\mathcal{O}$ *with* $|\mathrm{Disc}(\mathcal{O})|<X$ *is asymptotically*

$$\frac{1}{2}\cdot\prod_p\left(\frac{p-1}{p}\cdot\sum_{R\in\Sigma}\frac{1}{\mathrm{Disc}_p(R)}\cdot\frac{1}{\#\mathrm{Aut}(R)}\right)\cdot X.$$

By (38), (39), and Lemma 37, we then obtain

$$\begin{aligned}
&\lim_{X\to\infty}\frac{\sum_{\substack{\mathcal{O}\in\Sigma,\\ 0<(-1)^i\mathrm{Disc}(\mathcal{O})<X}}\#\mathrm{Cl}_3(\mathcal{O})}{\sum_{\substack{\mathcal{O}\in\Sigma,\\ 0<(-1)^i\mathrm{Disc}(\mathcal{O})<X}}1}\\
&=1+\lim_{X\to\infty}\frac{2\cdot N^{(i)}(X,\Sigma)}{\sum_{\substack{\mathcal{O}\in\Sigma,\\ 0<(-1)^i\mathrm{Disc}(\mathcal{O})<X}}1}\\
&=1+\frac{(1/n_i)\cdot\prod_p((p-1)/p\cdot\sum_{R\in\Sigma_p}1/\mathrm{Disc}_p(R)\cdot C(R))}{(1/2)\cdot\prod_p((p-1)/p\cdot\sum_{R\in\Sigma_p}1/\mathrm{Disc}_p(R)\cdot 1/\#\mathrm{Aut}(R))}\\
&=1+\frac{2}{n_i}\cdot\prod_p\frac{\sum_{R\in\Sigma_p}C(R)/\mathrm{Disc}_p(R)}{\sum_{R\in\Sigma_p}1/(2\cdot\mathrm{Disc}_p(R))}=1+\frac{2}{n_i}\cdot M_\Sigma. \qquad (40)
\end{aligned}$$

As $n_0=6$ and $n_1=2$, this proves Theorem 3.

5.4. *Families of quadratic fields defined by finitely many local conditions always have the same average number of* 3*-torsion elements in their class groups* (*Proof of Corollary* 4)

We now consider the special case of Theorem 3 where (Σ_p) is any acceptable collection of local specifications of *maximal* quadratic rings over $\mathbb{Z}_p$. Then, if Σ denotes the set of all isomorphism classes of quadratic orders $\mathcal{O}$ such that $\mathcal{O}\otimes\mathbb{Z}_p\in\Sigma_p$ for all p, then Σ will be a set of maximal orders satisfying a specified set of local conditions at some finite set of primes. We prove in this section that regardless of what the acceptable set of maximal orders Σ is, the average size of the 3-torsion subgroup in the class groups of imaginary (respectively, real) quadratic orders in Σ is always given by 2 (respectively, $\frac{4}{3}$). To do so, we use Theorem 3 and show that $M_\Sigma=1$ in these cases.

LEMMA 38. *For any maximal quadratic ring R over $\mathbb{Z}_p$, we have $C(R)=\frac{1}{2}$, where $C(R)$ denotes the weighted number of étale cubic algebras K_p over $\mathbb{Q}_p$ such that R is contained in the unique quadratic algebra over $\mathbb{Z}_p$ with the same discriminant as K_p* (*cf. equation* (2)).

Proof. For all primes $p\neq 2$, there are four maximal quadratic rings over $\mathbb{Z}_p$ (up to isomorphism), namely $\mathbb{Z}_p\oplus\mathbb{Z}_p$, $\mathbb{Z}_p[\sqrt{p}]$, $\mathbb{Z}_p[\sqrt{\epsilon}]$, and $\mathbb{Z}_p[\sqrt{\epsilon\cdot p}]$, where ϵ is an integer that is not a square mod p. For each choice of R, we compute $C(R)$:

$$\begin{aligned}
C(\mathbb{Z}_p\oplus\mathbb{Z}_p)&=\frac{1}{\#\mathrm{Aut}(\mathbb{Q}_p\oplus\mathbb{Q}_p\oplus\mathbb{Q}_p)}+\frac{1}{\#\mathrm{Aut}(\mathbb{Q}_{p^3})}=\frac{1}{6}+\frac{1}{3}=\frac{1}{2},\\
C(\mathbb{Z}_p[\sqrt{\alpha}])&=\frac{1}{\#\mathrm{Aut}(\mathbb{Q}_p\oplus\mathbb{Q}_p[\sqrt{\alpha}])}=\frac{1}{2}\quad\text{for }\alpha=p,\ \epsilon\text{ and }p\cdot\epsilon.
\end{aligned}$$

Here, $\mathbb{Q}_{p^3}$ denotes the unique unramified cubic extension of $\mathbb{Q}_p$. Note that any ramified cubic field extension K_p of $\mathbb{Q}_p$ has discriminant divisible by p^2 (since p will have ramification index 3 in K_p). This implies that $D(K_p)$ is not maximal for ramified K_p, and so no maximal quadratic ring is contained in $D(K_p)$.

When $p=2$, there are eight maximal quadratic rings over $\mathbb{Z}_2$ (up to isomorphism), namely $\mathbb{Z}_2\oplus\mathbb{Z}_2$ and $\mathbb{Z}_2[\sqrt{\alpha}]$, where $\alpha=2$, 3, 5, 6, 7, 10, or 14. As above, we have that $C(\mathbb{Z}_2\oplus\mathbb{Z}_2)=\frac{1}{2}$. Finally, it is easy to see that, for each possible value of α,

$$C(\mathbb{Z}_2[\sqrt{\alpha}])=\frac{1}{\#\mathrm{Aut}(\mathbb{Q}_2\oplus\mathbb{Q}_2[\sqrt{\alpha}])}=\frac{1}{2}.$$

Again, any ramified cubic extension K_2 of $\mathbb{Q}_2$ has discriminant divisible by 4, which implies that $D(K_2)$ does not contain any maximal orders. $\square$

By the above lemma, we see that if (Σ_p) is any acceptable collection of local specifications of maximal quadratic rings over $\mathbb{Z}_p$, then

$$\sum_{R\in\Sigma_p} \frac{C(R)}{\mathrm{Disc}_p(R)} = \sum_{R\in\Sigma_p} \frac{1}{2\cdot \mathrm{Disc}_p(R)}.$$

Thus $M_\Sigma = 1$, and so by Theorem 3 we obtain Corollary 4.

6. *The mean number of* 3*-torsion elements in the ideal groups of quadratic orders in acceptable families* (*Proof of Theorems* 7 *and* 8)

Finally, we prove Theorems 7 and 8, which generalize Theorem 6 and the work of Subsection 3.2 by determining the mean number of 3-torsion elements in the ideal groups of quadratic orders satisfying quite general sets of local conditions.

To this end, fix an acceptable collection (Σ_p) of local specifications for quadratic orders, and fix any $i \in \{0,1\}$. Let $S = S(\Sigma, i)$ denote the set of all irreducible elements $v \in V_{\mathbb{Z}}^{*(i)}$ such that, in the corresponding triple $(\mathcal{O}, I, \delta)$, we have that $\mathcal{O} \in \Sigma$ and I is invertible as an ideal class of $\mathcal{O}$ (implying that $I \otimes \mathbb{Z}_p$ is the trivial ideal class of $\mathcal{O}\otimes\mathbb{Z}_p$ for all p).

Proposition 39 ([**3**, Theorem 31]). *Let $S_p(\Sigma, i)$ denote the closure of $S(\Sigma,i)$ in $V_{\mathbb{Z}_p}^*$. Then*

$$\lim_{X\to\infty} \frac{N^*(S(\Sigma,i);X)}{X} = \frac{1}{2n_i^*}\cdot \prod_p \left(\frac{p-1}{p}\cdot \sum_{x\in S_p(\Sigma,i)/\mathrm{GL}_2(\mathbb{Z}_p)} \frac{1}{\mathrm{disc}_p(x)}\cdot \frac{1}{|\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z}_p)}(x)|}\right), \tag{41}$$

where $\mathrm{disc}_p(x)$ *denotes the reduced discriminant of $x \in V_{\mathbb{Z}_p}^*$ as a power of p and* $\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z}_p)}(x)$ *denotes the stabilizer of x in* $\mathrm{GL}_2(\mathbb{Z}_p)$.

Proof. First, note that although $S(\Sigma,i)$ might be defined by infinitely many congruence conditions, the estimate provided in Proposition 21 (and the fact that Σ is acceptable) shows that equation (14) continues to hold for the set $S(\Sigma,i)$, that is,

$$\lim_{X\to\infty} \frac{N^*(S(\Sigma,i),X)}{X} = \frac{\pi^2}{4\cdot n_i^*}\prod_p \mu_p^*(S(\Sigma,i)).$$

The argument is identical to that in Subsections 3.1 or 3.2.

If $\mu_p(S)$ denotes the p-adic density of S in $V_{\mathbb{Z}}$, where μ_p is normalized so that $\mu_p(V_{\mathbb{Z}}) = 1$, then $\mu_p^*(S) = \mu_p(S)$ for $p \neq 3$ and $\mu_3^*(S) = 9\mu_3(S)$. (This is just a reformulation of the fact that $[V_{\mathbb{Z}} : V_{\mathbb{Z}}^*] = 9$.) Thus,

$$\lim_{X\to\infty} \frac{N^*(S(\Sigma,i),X)}{X} = \frac{9\cdot\pi^2}{4\cdot n_i^*}\prod_p \mu_p(S(\Sigma,i)).$$

By [**3**, Lemma 32], we have that

$$\mu_p(S(\Sigma,i)) = \frac{\#\mathrm{GL}_2(\mathbb{F}_p)}{p^4}\cdot \sum_{x\in S_p/\mathrm{GL}_2(\mathbb{Z}_p)} \frac{1}{\mathrm{Disc}_p(x)}\cdot\frac{1}{|\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z}_p)}(x)|},$$

where $\mathrm{Disc}_p(x)$ denotes the discriminant of $x \in V^*_{\mathbb{Z}_p}$ as a power of p. Note that since $\mathrm{Disc}_p(x) = \mathrm{disc}_p(x)$ for all $p \neq 3$ and $\mathrm{Disc}_3(x) = 27 \cdot \mathrm{disc}_3(x)$, we have that

$$\begin{aligned}
&\lim_{X\to\infty} \frac{N^*(S(\Sigma,i),X)}{X}\\
&\quad = \frac{9\cdot\pi^2}{4\cdot n_i^*}\cdot\frac{1}{27}\cdot\prod_p \frac{\#\mathrm{GL}_2(\mathbb{F}_p)}{p^4}\cdot \sum_{x\in S_p(\Sigma,i)/\mathrm{GL}_2(\mathbb{Z}_p)} \frac{1}{\mathrm{disc}_p(x)}\cdot\frac{1}{|\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z}_p)}(x)|}\\
&\quad = \frac{1}{2n_i^*}\cdot\prod_p\left(\frac{p-1}{p}\right)\sum_{x\in S_p(\Sigma,i)/\mathrm{GL}_2(\mathbb{Z}_p)} \frac{1}{\mathrm{disc}_p(x)}\cdot\frac{1}{|\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z}_p)}(x)|}. \qquad \square
\end{aligned}$$

Now, if we set

$$M_p(S(\Sigma,i)) := \sum_{x\in S_p(\Sigma,i)/\mathrm{GL}_2(\mathbb{Z}_p)} \frac{1}{\mathrm{disc}_p(x)}\cdot\frac{1}{|\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z}_p)}(x)|}, \tag{42}$$

then the description of the stabilizer in Corollary 11 (in its form over $\mathbb{Z}_p$; see Remark 12) allows us to express $M_p(S(\Sigma,i))$ in another way. Namely, if $R \in \Sigma_p$ is a non-degenerate quadratic ring over $\mathbb{Z}_p$, then in a corresponding triple (R,I,δ) we can always choose $I = R$, since I is a principal ideal (recall that invertible means locally principal). Let $\tau(R)$ denote the number of elements δ, modulo cubes, yielding a valid triple (R,R,δ) over $\mathbb{Z}_p$. Then $\tau(R) = |U^+(R)/U^+(R)^{\times 3}|$, where $U^+(R)$ denotes the group of units of R having norm 1. Since (R,R,δ) is $\mathrm{GL}_2(\mathbb{Z}_p)$-equivalent to the triple $(R,R,\bar\delta)$, and $\bar\delta = \kappa^3\delta$ for some $\kappa \in R\otimes\mathbb{Q}$ if and only if δ is itself a cube (since $\bar\delta = N(I)^3/\delta$), then we see that

$$M_p(S(\Sigma,i)) = \sum \frac{|U^+(R)/U^+(R)^{\times 3}|}{\mathrm{Disc}_p(R)\cdot|\mathrm{Aut}(R)|\cdot|U_3^+(R)|}, \tag{43}$$

where the sum is over all isomorphism classes of quadratic rings R over $\mathbb{Z}_p$ lying in Σ_p, and where $U_3^+(R)$ denotes the subgroup of 3-torsion elements of $U^+(R)$. We have the following lemma.

LEMMA 40. *Let R be a non-degenerate quadratic ring over $\mathbb{Z}_p$. Then*

$$\frac{|U^+(R)/U^+(R)^{\times 3}|}{|U_3^+(R)|}$$

is 1 if $p \neq 3$, and is 3 if $p = 3$.

Proof. The unit group of R, as a multiplicative group, is a finitely generated, rank 2 $\mathbb{Z}_p$-module. Hence the submodule $U^+(R)$, consisting of those units having norm 1, is a finitely generated rank 1 $\mathbb{Z}_p$-module. It follows that there is an isomorphism $U^+(R) \cong F \times \mathbb{Z}_p$ as $\mathbb{Z}_p$-modules, where F is a finite abelian p-group.

Let F_3 denote the 3-torsion subgroup of F. Since F_3 is the kernel of the multiplication-by-3 map on F, it is clear that $|F/(3\cdot F)|/|F_3| = 1$. Therefore, it suffices to check the lemma on the 'free' part of $U^+(R)$, namely the $\mathbb{Z}_p$-module $\mathbb{Z}_p$, where the result is clear. (The case $p = 3$ differs because $3\cdot\mathbb{Z}_p$ equals $\mathbb{Z}_p$ for $p \neq 3$, while $3\cdot\mathbb{Z}_3$ has index 3 in $\mathbb{Z}_3$.) $\square$

Combining (41)–(43), and Lemma 40, we obtain

$$\lim_{X\to\infty} \frac{N^*(S(\Sigma,i),X)}{X} = \frac{3}{2n_i^*}\cdot\prod_p\left(\frac{p-1}{p}\cdot\sum_{R\in\Sigma_p}\frac{1}{2\cdot\mathrm{Disc}_p(R)}\right). \tag{44}$$

By Corollary 14 and Theorem 17, we have

$$N^*(S(\Sigma,i),X)=\begin{cases}\displaystyle\sum_{\substack{\mathcal{O}\in\Sigma,\\ 0<\mathrm{Disc}(\mathcal{O})<X}}(3\cdot|\mathrm{Cl}_3(\mathcal{O})|-|\mathcal{I}_3(\mathcal{O})|) & \text{if } i=0,\\ \displaystyle\sum_{\substack{\mathcal{O}\in\Sigma,\\ 0<-\mathrm{Disc}(\mathcal{O})<X}}(|\mathrm{Cl}_3(\mathcal{O})|-|\mathcal{I}_3(\mathcal{O})|) & \text{if } i=1.\end{cases} \tag{45}$$

Hence we conclude using Lemma 37 that

$$\frac{\sum_{\substack{\mathcal{O}\in\Sigma,\\ 0<\mathrm{Disc}(\mathcal{O})<X}}(|\mathrm{Cl}_3(\mathcal{O})|-\frac{1}{3}\cdot|\mathcal{I}_3(\mathcal{O})|)}{\sum_{\substack{\mathcal{O}\in\Sigma\\ 0<\mathrm{Disc}(\mathcal{O})<X}}1}$$
$$=\frac{1}{3}\cdot\frac{(3/2n_0^*)\cdot\prod_p((p-1)/p\cdot\sum_{R\in\Sigma_p}1/(2\cdot\mathrm{Disc}_p(R)))}{(1/2)\cdot\prod_p((p-1)/p\cdot\sum_{R\in\Sigma_p}1/(2\cdot\mathrm{Disc}_p(R)))}=1,$$

and

$$\frac{\sum_{\substack{\mathcal{O}\in\Sigma,\\ 0<-\mathrm{Disc}(\mathcal{O})<X}}(|\mathrm{Cl}_3(\mathcal{O})|-|\mathcal{I}_3(\mathcal{O})|)}{\sum_{\substack{\mathcal{O}\in\Sigma,\\ 0<-\mathrm{Disc}(\mathcal{O})<X}}1}$$
$$=\frac{(3/2n_1^*)\cdot\prod_p((p-1)/p\cdot\sum_{R\in\Sigma_p}1/(2\cdot\mathrm{Disc}_p(R)))}{(1/2)\cdot\prod_p((p-1)/p\cdot\sum_{R\in\Sigma_p}1/(2\cdot\mathrm{Disc}_p(R)))}=1,$$

yielding Theorem 8. In conjunction with Theorem 3, we also then obtain Theorem 7.

Acknowledgements. We are very grateful to Henri Cohen, Benedict Gross, Hendrik Lenstra, Jay Pottharst, Arul Shankar, Peter Stevenhagen, and Jacob Tsimerman for all their help and for many valuable discussions.

References

1. M. Bhargava, 'Higher composition laws I: A new view on Gauss composition, and quadratic generalizations', *Ann. of Math.* 159 (2004) 217–250.
2. M. Bhargava, 'Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants', *Int. Math. Res. Not.* 2007 (2007) 1–20.
3. M. Bhargava, A. Shankar and J. Tsimerman, 'On the Davenport–Heilbronn theorems and second order terms', *Invent. Math.* 193 (2013) 439–499.
4. H. Cohen, *Advanced topics in computational number theory* (Springer, New York, 2000).
5. H. Cohen and H. W. Lenstra, 'Heuristics on class groups of number fields', *Number theory (Noordwijkerhout*, 1983), Lecture Notes in Mathematics 1068 (Springer, Berlin, 1984) 33–62.
6. D. Cox, *Primes of the form* x^2+ny^2 (John Wiley & Sons Inc., New York, 1989).
7. H. Davenport, 'On the class-number of binary cubic forms I', *J. London Math. Soc.* 26 (1951) 183–192.
8. H. Davenport, 'On the class-number of binary cubic forms II', *J. London Math. Soc.* 26 (1951) 192–198.
9. H. Davenport and H. Heilbronn, 'On the density of discriminants of cubic fields II', *Proc. Roy. Soc. London Ser. A* 322 (1971) 405–420.
10. B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, Translations of Mathematical Monographs, American Mathematical Society 10 (1964).
11. G. Eisenstein, 'Aufgaben und Lehrsätze', *J. reine angew. Math.* 27 (1844) 89–106.
12. H. Hasse, 'Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage', *Math. Z.* 31 (1930) 565–582.
13. J. Nakagawa, 'On the relations among the class numbers of binary cubic forms', *Invent. Math.* 134 (1998) 101–138.

Manjul Bhargava
Department of Mathematics
Princeton University
Fine Hall, Washington Road
Princeton, NJ 08544
USA

bhargava@math.princeton.edu

Ila Varma
Department of Mathematics
Princeton University
Fine Hall, Washington Road
Princeton, NJ 08544
USA

ivarma@math.princeton.edu