QUADRATIC TWISTS OF ELLIPTIC CURVES AND CLASS NUMBERS

MICHAEL GRIFFIN, KEN ONO AND WEI-LUN TSAI

ABSTRACT. For positive rank r elliptic curves $E(\mathbb{Q})$, we employ ideal class pairings

$$E(\mathbb{Q}) \times E_{-D}(\mathbb{Q}) \to \mathrm{CL}(-D),$$

for quadratic twists $E_{-D}(\mathbb{Q})$ with a suitable "small y-height" rational point, to obtain effective class number lower bounds. For the curves $E^{(a)} : y^2 = x^3 - a$, with rank $r(a)$, this gives

$$h(-D) \geq \frac{1}{10} \cdot \frac{|E_{\mathrm{tor}}(\mathbb{Q})|}{\sqrt{R_{\mathbb{Q}}(E)}} \cdot \frac{\Gamma\left(\frac{r(a)}{2}+1\right)}{(4\pi)^{\frac{r(a)}{2}}} \cdot \frac{\log(D)^{\frac{r(a)}{2}}}{\log \log D},$$

representing an improvement to the classical lower bound of Goldfeld, Gross and Zagier when $r(a) \geq 3$. We prove that the number of twists $E_{-D}^{(a)}(\mathbb{Q})$ with such a point (resp. with such a point and rank ≥ 2 under the Parity Conjecture) is $\gg_{a,\varepsilon} X^{\frac{1}{2}-\varepsilon}$. We give infinitely many cases where $r(a) \geq 6$. These results can be viewed as an analogue of the classical estimate of Gouvêa and Mazur for the number of rank ≥ 2 quadratic twists, where in addition we obtain "log-power" improvements to the Goldfeld-Gross-Zagier class number lower bound.

1. INTRODUCTION AND STATEMENT OF RESULTS

Originally posed by Gauss, the problem of obtaining effective lower bounds for class numbers $h(-D)$ of imaginary quadratic fields $\mathbb{Q}(\sqrt{-D})$, which also count equivalence classes of integral positive definite binary quadratic forms of fundamental discriminant $-D$, has been one of fundamental challenges in number theory. In the 1930s, Siegel [20] proved, for every $\varepsilon > 0$, that there are constants $c_1(\varepsilon), c_2(\varepsilon) > 0$ for which

$$c_1(\varepsilon) D^{\frac{1}{2}-\varepsilon} \leq h(-D) \leq c_2(\varepsilon) D^{\frac{1}{2}+\varepsilon}.$$

Unfortunately, Siegel's lower bound is inexplicit; there is no known formula for $c_1(\varepsilon)$. As a consequence, the problem of obtaining an effective nontrivial lower bound remained open for many decades. Finally in the 1980s, Goldfeld, Gross and Zagier [6, 8, 11] solved this problem by making use of ideas and results related to the Birch and Swinnerton-Dyer Conjecture. Thanks to the existence of an elliptic curve with analytic rank 3, Oesterlé [15] used their work to establish the effective lower bound

$$(1.1) \qquad h(-D) > \frac{1}{7000} (\log D) \prod_{\substack{p \mid D \text{ prime} \\ p \neq D}} \left(1 - \frac{[2\sqrt{p}]}{p+1}\right).$$

In recent work [9], the first two authors obtained effective lower bounds that improve on (1.1) for certain polynomial families of discriminants. The method makes direct use of the arithmetic of elliptic curves. The idea is to employ *ideal class pairings*, maps of the form

$$E(\mathbb{Q}) \times E_{-D}(\mathbb{Q}) \to \mathrm{CL}(-D),$$

where E_{-D} is the $-D$-quadratic twist of E. Such maps were first defined and studied by Buell, Call, and Soleng [2, 3, 23].

Suppose that $E/\mathbb{Q}$ is given by

$$E: \quad y^2 = x^3 + a_4 x + a_6,$$

where $a_4, a_6 \in \mathbb{Z}$, with j-invariant $j(E)$ and discriminant $\Delta(E)$, and suppose that $E(\mathbb{Q})$ has Mordell rank $r = r_{\mathbb{Q}}(E) \geq 1$. Throughout, we suppose that $-D < 0$ denotes a negative fundamental discriminant. We let $E_{-D}/\mathbb{Q}$ be its $-D$-quadratic twist[1] given by the model

$$(1.2) \qquad\qquad E_{-D}: \quad -D \cdot \left(\frac{y}{2}\right)^2 = x^3 + a_4 x + a_6.$$

Suppose that $Q_{-D} = \left(\frac{u}{w^2}, \frac{v}{w^3}\right) \in E_{-D}(\mathbb{Q})$, where[2] $uv \neq 0$. In Section 2.1, we recall Theorem 2.1, which gives the explicit construction of the pairing. Moreover, the theorem determines situations where the classes obtained by pairing points in $E(\mathbb{Q})$ with Q_{-D} are inequivalent, thereby providing a lower bound for $h(-D)$.

We use this idea to derive lower bounds for $h(-D)$ in terms of $\Omega_r := \pi^{\frac{r}{2}}/\Gamma\left(\frac{r}{2}+1\right)$, the volume of the $\mathbb{R}^r$-unit ball, the regulator $R_{\mathbb{Q}}(E)$, the diameter $d(E)$ (see (2.4)), the torsion subgroup $E_{\text{tor}}(\mathbb{Q})$ and the point Q_{-D}. We define the natural constants

$$(1.3) \qquad\qquad c(E) := \frac{|E_{\text{tor}}(\mathbb{Q})|}{2^{r+1}\sqrt{R_{\mathbb{Q}}(E)} \cdot \Omega_r},$$

and

$$(1.4) \qquad\qquad c(E, Q_{-D}) := c(E) \cdot \prod_{\substack{p \text{ prime} \\ p|w}} \left(1 - \frac{1}{|E(\mathbb{F}_p)|}\right).$$

Here $|E(\mathbb{F}_p)|$ denotes the number of $\mathbb{F}_p$-points on the reduction of E modulo p (even for primes of bad reduction), including the point at infinity.

Our first result is a generalization of Theorem 1.1 of [9], which uses the usual logarithmic heights (see Section 2.2) of $j(E)$ and $\Delta(E)$, to define

$$(1.5) \qquad\qquad \delta(E) := \frac{1}{2}h_W(j(E)) + \frac{1}{3}h_W(\Delta(E)) + \frac{20}{3}.$$

To facilitate the comparison with $\log(D)$, we define

$$(1.6) \qquad\qquad T_E(-D, Q_{-D}) := \log\left(\frac{D}{|u| + w^2}\right) - \delta(E).$$

Finally, we say that $Q_{-D} = \left(\frac{u}{w^2}, \frac{v}{w^3}\right) \in E_{-D}(\mathbb{Q})$ is *suitable for* E if $uv \neq 0$ and

$$(1.7) \qquad (|u| + w^2)\exp(\delta(E) + d(E)) < D < \frac{(|u| + w^2)^2 \max(|u|, w^2)^2}{v^4}.$$

It turns out that suitable rational points Q_{-D} will have "small" v. For notational convenience, we let $\widehat{c}(E, Q_{-D}) := 2 \cdot 3^r r \sqrt{d(E)} c(E) \cdot \mathcal{S}(w)$, where $\mathcal{S}(w)$ denotes the number of positive square-free divisors of w. We obtain the following theorem.

---

[1] For reasons which will become apparent later, we use this nonstandard normalization.

[2] We note that these hypotheses guarantee that v is even when $-D$ is odd.

Theorem 1.1. *Assuming the notation and hypotheses above, if Q_{-D} is suitable for E, then*

$$h(-D) \geq c(E, Q_{-D}) \cdot T_E(-D, Q_{-D})^{\frac{r}{2}} - \widehat{c}(E, Q_{-D}) \cdot T_E(-D, Q_{-D})^{\frac{r-1}{2}}.$$

To give an indication of the frequency that Theorem 1.1 offers an improvement to (1.1), we consider the elliptic curves

$$(1.8) \qquad\qquad E^{(a)}: \quad y^2 = x^3 - a,$$

where a is a positive integer. By constructing explicit infinite order points $Q_{-D} \in E_{-D}^{(a)}(\mathbb{Q})$, which are often suitable, we obtain effective lower bounds for $h(-D)$, formulated in terms of the rank of $E^{(a)}$ and the natural constant $c(E^{(a)})$ defined in (1.3). For notational convenience, we let

$$(1.9) \qquad \mathfrak{S}(E) := \{-D : E_{-D}(\mathbb{Q}) \text{ has an infinite order suitable point } Q_{-D}\}.$$

Theorem 1.2. *If $E^{(a)}(\mathbb{Q})$ has rank r and $\varepsilon > 0$, then we have*

$$\# \left\{ -X < -D < 0 \ : \ -D \in \mathfrak{S}(E^{(a)}) \text{ and } h(-D) > \frac{c(E^{(a)})}{5} \cdot \frac{\log(D)^{\frac{r}{2}}}{\log\log D} \right\} \gg_{a,\varepsilon} X^{\frac{1}{2}-\varepsilon}.$$

Assuming the Parity Conjecture for elliptic curves, we may also require $r_{\mathbb{Q}}(E_{-D}^{(a)}) \geq 2$.

Four Remarks.

(1) The multiplicative constant $1/5$ was chosen for aesthetics, and is the lower bound offered in the abstract. By Lemma 4.2, one can replace $1/5$ with any constant < 0.2158.

(2) The lower bound $\gg_{a,\varepsilon} X^{\frac{1}{2}-\varepsilon}$ for the number of discriminants $-X < -D < 0$ in Theorem 1.2 is an improvement of the results in [9] (see the second Remark after Theorem 1.2 in [9]), where $\gg X^{\frac{1}{3}}$ many discriminants are obtained.

(3) Each rank 1 curve $E^{(a)}(\mathbb{Q})$ gives $\gg_{a,\varepsilon} X^{\frac{1}{2}-\varepsilon}$ many discriminants $-X < -D < 0$ with

$$h(-D) > \frac{c(E^{(a)})}{5} \cdot \frac{\sqrt{\log D}}{\log\log D}.$$

Although such estimates do not improve on (1.1), it is plausible that a new proof of Gauss's class number 1 problem, famously proved by Baker, Heegner and Stark [1, 12, 25], can be obtained by making use of the large supply of rank 1 curves $E^{(a)}(\mathbb{Q})$.

(4) Goldfeld's famous conjecture [7] on quadratic twists of elliptic curves implies that asymptotically "half of the quadratic twists" of $E^{(a)}$ have rank 0 (resp. 1). Theorem 1.2 is related to the well-studied problem of estimating the number of those rare twists with rank ≥ 2. In an important paper, Stewart and Top (see Theorem 3 of [26]) unconditionally proved

$$\#\{-X < -D < 0 \ : \ r_{\mathbb{Q}}(E_{-D}^{(a)}) \geq 2\} \gg_a \frac{X^{\frac{1}{7}}}{\log X}.$$

However, it is widely believed that this lower bound is not optimal. Indeed, a classical result of Gouvêa and Mazur (see Theorem 2 of [10])), which assumes the Parity Conjecture, gives

$$\#\{-X < -D < 0 \ : \ r_{\mathbb{Q}}(E_{-D}^{(a)}) \geq 2\} \gg_{a,\varepsilon} X^{\frac{1}{2}-\varepsilon}.$$

If $r(a) \geq 3$, then Theorem 1.2 can be viewed as an analogue of this result, where we also obtain a "log-power" improvement to the Goldfeld-Gross-Zagier class number lower bound (1.1).

Example 1. *The elliptic curve*[3] $E^{(174)}(\mathbb{Q})$ *has no nontrivial torsion, and has rank* 3, *with generators* $(7, 13), (25/4, 67/8),$ *and* $(151/25, -851/125)$. *Moreover, we have* $\Omega_3 = 4\pi/3 \approx 4.1887$ *and* $R_{\mathbb{Q}}(E^{(174)}) \approx 46.1056$, *which gives* $c(E^{(174)}) \approx 0.0385 > 1/26$. *Therefore, Theorem 1.2 implies that*

$$\#\left\{-X < -D < 0 \ : \ -D \in \mathfrak{S}(E^{(174)}) \text{ and } h(-D) > \frac{1}{130} \cdot \frac{\log(D)^{\frac{3}{2}}}{\log\log D}\right\} \gg_\varepsilon X^{\frac{1}{2}-\varepsilon}.$$

Assuming the Parity Conjecture, we may also require that $r_{\mathbb{Q}}(E_{-D}^{(174)}) \geq 2$.

Example 2. *Theorem 1.2 holds for infinite (if any) subgroups of* $E^{(a)}(\mathbb{Q})$ *(see Lemma 2.5), where one employs the natural analogues of* $R_{\mathbb{Q}}(E^{(a)})$. *Elkies* [4, 5] *found that* $E^{(k)}$, *where*

$$k := 2195745961 \cdot 41389156704451409263 7683,$$

has $r_{\mathbb{Q}}(E^{(k)}) \geq 17$. *Theorem 1.2 for this curve then gives*

$$\#\left\{-X < -D < 0 \ : \ -D \in \mathfrak{S}(E^{(k)}) \text{ and } h(-D) > \frac{c(E^{(k)})}{5} \cdot \frac{\log(D)^{\frac{17}{2}}}{\log\log D}\right\} \gg_{k,\varepsilon} X^{\frac{1}{2}-\varepsilon},$$

offering a large "log-power" improvement to (1.1). Using the 17 independent points listed in [4, 5], *one can find that* $c(E^{(k)}) \approx 4.81326 \cdot 10^{-19}$. *Again, assuming the Parity Conjecture, we may also require that* $r_{\mathbb{Q}}(E_{-D}^{(k)}) \geq 2$.

Example 3. *For* $r \in \{3, 4, 5, 6\}$, *we consider curves* $E^{(a_r(T))}/\mathbb{Q}(T)$, *where*
$$a_3(T) := 2^4 3^3(4T^6 - 8T^4 + 40T^2 - 31),$$

$$a_4(T) := 6075T^{12} + 38070T^{11} + 81513T^{10} + 83106T^9 + 67797T^8 + 39528T^7 + 27270T^6$$
$$+ 58968T^5 + 89181T^4 + 84834T^3 + 52353T^2 + 23814T - 9261,$$

$$a_5(T) := \frac{64}{27}\left(T^{18} + 2973T^{12} - 369249T^6 + 11764900\right),$$

$$a_6(T) := (2^6 \cdot 7^{54} \cdot 13^2 \cdot 1297 \cdot 74449^3 \cdot 793041539 \cdot 1995792099060563/27) \cdot T^{54}$$
$$+ (2^9 \cdot 7^{53} \cdot 13 \cdot 1999 \cdot 74449^2 \cdot 1923403 \cdot 881277323405000103687971) \cdot T^{53} + \cdots$$
$$+ \cdots + \cdots + (2^9 \cdot 7^{53} \cdot 13 \cdot 1999 \cdot 74449^2 \cdot 1923403 \cdot 881277323405000103687971) \cdot T$$
$$+ (2^6 \cdot 5^3 \cdot 11 \cdot 8123 \cdot 1882419814724639$$
$$\cdot 177610817485358112101332029225675499667600288403153465585113540179/27).$$

Using work of Mestre [14], *Stewart and Top* [26] *proved that each* $E^{(a_r(T))}/\mathbb{Q}(T)$ *has rank* r. *By Silverman's specialization theorem* [22], *for all but finitely many integers* t, *Theorem 1.2 gives*

$$\#\left\{-X < -D < 0 \ : \ -D \in \mathfrak{S}(E^{(a_r(t))}) \text{ and } h(-D) > \frac{c_r(t)}{5} \cdot \frac{\log(D)^{\frac{r}{2}}}{\log\log D}\right\} \gg_{r,\varepsilon} X^{\frac{1}{2}-\varepsilon},$$

---

[3]All computations in this paper were performed using SageMath [19].

where $c_r(t)$ is defined using the r points given in [26]. *Again, assuming the Parity Conjecture, we may also require that* $r_{\mathbb{Q}}(E_{-D}^{(a_r(t))}) \geq 2$.

This paper is organized as follows. In Section 2 we prove Theorem 1.1, an extension of Theorem 1.1 of [9]. To prove Theorem 1.2, we use the fact that the existence of a suitable point $Q_{-D} \in E_{-D}^{(a)}(\mathbb{Q})$ for $E^{(a)}$ is equivalent to the solvability of the Diophantine equation

$$-Dt^2 = m^3 - an^6,$$

where the integer triples (m, n, t) satisfy certain inequalities. To make use of this fact, in Section 3 we prove an auxiliary theorem of independent interest (see Theorem 3.1), which gives asymptotic formulas for the number of solutions to this equation where the parameters are chosen from natural intervals. In particular, as a function of $T = T(X)$, this theorem can be used to estimate (see (3.6)) the number of discriminants $-X < -D < 0$ for which there is an infinite order rational point $Q_{-D} = \left(\frac{u}{w^2}, \frac{v}{w^3}\right) \in E_{-D}(\mathbb{Q})$ with $T \leq v \leq 2T$. This result is obtained using the Pólya-Vinogradov inequality, combined with a sieve-type count involving solutions to polynomial congruences. In Section 4, we then prove Theorem 1.2.

Acknowledgements

2. Ideal class pairings and the proof of Theorem 1.1

Works by Buell, Call, and Soleng [2, 3, 23] offered elliptic curve ideal class pairings, which produce discriminant $-D$ integral positive definite binary quadratic forms from points on $E(\mathbb{Q})$ and $E_{-D}(\mathbb{Q})$. Theorem 2.1 of [9] is a generalization and minor correction of Theorem 4.1 of [23].[4] We begin by recalling this result.

2.1. **Ideal class pairing.** Assume the notation from Section 1. Let $P = (\frac{A}{C^2}, \frac{B}{C^3}) \in E(\mathbb{Q})$, with $A, B, C \in \mathbb{Z}$, and $Q = (\frac{u}{w^2}, \frac{v}{w^3}) \in E_{-D}(\mathbb{Q})$, with $u, v, w \in \mathbb{Z}$, not necessarily in lowest terms, but so that no sixth power divides $\gcd(u^3, v^2, w^6)$. Every Q clearly has such a representation, and thanks to (1.2), we find that $\gcd(u, w^2)$ and $\gcd(v, w^3)$ both divide D. Moreover, suppose that $uv \neq 0$, which guarantees that v is even when $-D$ is odd. If we let $\alpha := |Aw^2 - uC^2|$ and $G := \gcd(\alpha, C^6 v^2)$, then there are integers ℓ for which $F_{P,Q}(X, Y)$ defined below is a discriminant $-D$ positive definite integral binary quadratic form.

$$(2.1) \qquad F_{P,Q}(X, Y) := \frac{\alpha}{G} \cdot X^2 + \frac{2w^3B + \ell \cdot \frac{\alpha}{G}}{C^3 v} \cdot XY + \frac{\left(2w^3B + \ell \cdot \frac{\alpha}{G}\right)^2 + C^6 v^2 D}{4C^6 v^2 \cdot \frac{\alpha}{G}} \cdot Y^2.$$

Theorem 2.1. [Theorem 2.1 of [9]] *Assuming the notation and hypotheses above, $F_{P,Q}(X, Y)$ is well defined (e.g. there is such an ℓ) in* CL$(-D)$. *Moreover, if (P_1, Q_1) and (P_2, Q_2) are two such pairs for which $F_{P_1,Q_1}(X, Y)$ and $F_{P_2,Q_2}(X, Y)$ are* SL$_2(\mathbb{Z})$-*equivalent, then $\frac{\alpha_1}{G_1} = \frac{\alpha_2}{G_2}$ or $\frac{\alpha_1 \alpha_2}{G_1 G_2} > D/4$.*

---

[4]This corrects sign errors in the discriminants in Theorem 4.1 of [23], and also ensures the resulting quadratic forms are integral when $C \neq 1$. Moreover, this theorem allows for both even and odd discriminants.

Example 4. *For $E : y^2 = x^3 - 4x + 9$, we have points $P_1 := (0, 3)$ and $P_2 := (-2, 3)$. We consider the example of $h(-24) = 2$. Using $Q := (-3, 1) \in E_{-24}(\mathbb{Q})$ and $\ell = 2$, we obtain representatives for the two inequivalent discriminant -24 forms*

$$F_{P_1,Q}(X, Y) = 3X^2 + 12XY + 14Y^2 \quad \text{and} \quad F_{P_2,Q}(X, Y) = X^2 + 8XY + 22Y^2.$$

2.2. **Proof of Theorem 1.1.** To deduce Theorem 1.1 from Theorem 2.1, we use estimates for the number of bounded height rational points on elliptic curves. We recall the facts we require. Each rational point $P \in E(\mathbb{Q})$ has the form $P = (\frac{A}{C^2}, \frac{B}{C^3})$, with A, B, C integers such that $\gcd(A, C) = \gcd(B, C) = 1$. The *naive height* of P is $H(P) = H(x) := \max(|A|, |C^2|)$, and the *logarithmic height* (or Weil height) is $h_W(P) = h_W(x) := \log H(P)$. Finally, we recall the *canonical height*

$$(2.2) \qquad \qquad \widehat{h}(P) := \tfrac{1}{2} \lim_{n \to \infty} \frac{h_W(nP)}{n^2}.$$

The following theorem of Silverman [22] bounds the difference between the logarithmic and canonical heights of rational points in terms of the logarithmic heights of $j(E)$ and $\Delta(E)$.

Theorem 2.2 (Theorem 1.1 of [22]). *If $P \in E(\mathbb{Q})$, then*

$$-\tfrac{1}{8}h_W(j(E)) - \tfrac{1}{12}h_W(\Delta(E)) - 0.973 \leq \widehat{h}(P) - \frac{1}{2}h_W(P) \leq \tfrac{1}{12}h_W(j(E)) + \tfrac{1}{12}h_W(\Delta(E)) + 1.07.$$

Asymptotics for the number of rational points on an elliptic curve with bounded height are well known (for example, see [13, Prop 4.18]). If $E(\mathbb{Q})$ has rank $r \geq 1$ and $\Omega_r := \pi^{\frac{r}{2}}/\Gamma\left(\frac{r}{2} + 1\right)$, then in terms of the regulator $R_{\mathbb{Q}}(E)$ and $|E_{\text{tor}}(\mathbb{Q})|$, we have

$$(2.3) \qquad \qquad \#\{P \in E(\mathbb{Q}) \mid \widehat{h}(P) \leq T/4\} \sim \frac{|E_{\text{tor}}(\mathbb{Q})|}{2^r \sqrt{R_{\mathbb{Q}}(E)}} \cdot \Omega_r T^{\frac{r}{2}}.$$

To prove Theorem 1.1, we require effective lower bounds for the number of points with bounded height, which is essentially the problem of counting lattice points in r-dimensional spheres. To this end, we let $B(R)$ denote the closed ball in $\mathbb{R}^r$ of radius R centered at the origin. Furthermore, if $\mathcal{P}$ is any parallelepiped, then let $d(\mathcal{P})$ denote its (squared) diameter, the largest square-distance between any two vertices. In our setting, if $\{P_1, \ldots, P_r\}$ is a basis of $E(\mathbb{Q})/E_{\text{tor}}(\mathbb{Q})$, then the (squared) diameter is

$$(2.4) \qquad \qquad d(E) := \max_{\delta_i \in \{\pm 1, 0\}} \widehat{h}\left(\sum_{i=1}^{r} \delta_i P_i\right).$$

This is the diameter of the parallelepiped in $\mathbb{R}^r$ constructed from vectors $\mathbf{v}_1, \ldots \mathbf{v}_r$, where $\mathbf{v}_i \cdot \mathbf{v}_j = \langle P_i, P_j \rangle := \tfrac{1}{2}\left(\widehat{h}(P_i + P_j) - \widehat{h}(P_i) - \widehat{h}(P_j)\right)$.

Lemma 2.3. *Let Λ be a lattice in $\mathbb{R}^r$ of full rank, and let $\mathcal{P}$ be any fundamental parallelepiped of Λ. If $T > 4d(\mathcal{P})$, then we have*

$$\left| \frac{2^r \operatorname{Vol} \mathcal{P}}{\Omega_r} \cdot \#\{\Lambda \cap B(\tfrac{1}{2}T^{\frac{1}{2}})\} - T^{\frac{r}{2}} \right| \leq 3^r T^{\frac{r-1}{2}} d(\mathcal{P})^{\frac{1}{2}}.$$

Proof. Let $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\}$ be a basis for Λ, and let $\mathbf{w} := \sum_{i=1}^{r} \frac{1}{2}\mathbf{v}_i$. For each point $\lambda \in \Lambda$, let P_λ be the half-open parallelepiped given by

$$\mathcal{P}_\lambda = \left\{ \lambda + \sum_{i=1}^{r} x_i \mathbf{v}_i \ \middle| \ x_i \in [0,1) \right\}.$$

If $\mathcal{P}_\lambda$ intersects the shifted ball $B(\frac{1}{2}T^{\frac{1}{2}} - \frac{1}{2}d^{\frac{1}{2}}) + \mathbf{w}$, then $\lambda \in B(\frac{1}{2}T^{\frac{1}{2}})$. Therefore, we have

$$\# \left(\Lambda \cap B(\tfrac{1}{2}T^{\frac{1}{2}}) \right) \ \geq \ \frac{\mathrm{Vol}\left(B(\frac{1}{2}T^{\frac{1}{2}} - \frac{1}{2}d^{\frac{1}{2}}) \right)}{\mathrm{Vol}(\mathcal{P}_\lambda)} = \frac{\Omega_r}{2^r \, \mathrm{Vol}(\mathcal{P}_\lambda)} \cdot \left(T^{\frac{1}{2}} - d^{\frac{1}{2}} \right)^r.$$

On the other hand, If $\lambda \in B(\frac{1}{2}T^{\frac{1}{2}})$, then $\mathcal{P}_\lambda$ is contained in the shifted ball $B(\frac{1}{2}T^{\frac{1}{2}} + \frac{1}{2}d^{\frac{1}{2}}) + \mathbf{w}$. Therefore, we have

$$\# \left(\Lambda \cap B(\tfrac{1}{2}T^{\frac{1}{2}}) \right) \ \leq \ \frac{\mathrm{Vol}\left(B(\frac{1}{2}T^{\frac{1}{2}} + \frac{1}{2}d^{\frac{1}{2}}) \right)}{\mathrm{Vol}(\mathcal{P}_\lambda)} = \frac{\Omega_r}{2^r \, \mathrm{Vol}(\mathcal{P}_\lambda)} \cdot \left(T^{\frac{1}{2}} + d^{\frac{1}{2}} \right)^r.$$

We now apply the approximation

$$(x+y)^r \leq x^r + b^{-1}x^{r-1}y\left((1+b)^r - 1\right) < x^r + b^{-1}x^{r-1}y\left(1+b\right)^r,$$

whenever x and y are positive and $0 < y/x < b < 1$. By hypothesis, we have $\sqrt{T} > 2\sqrt{d(\mathcal{P})}$, and so the conclusion follows by letting $b = 1/2$. $\qquad\square$

We use this lemma to count bounded height rational points on an elliptic curve, whose coordinates have denominators that satisfy certain coprimality conditions. Namely, suppose that $Q_{-D} = \left(\frac{u}{w^2}, \frac{v}{w^3} \right) \in E_{-D}(\mathbb{Q})$ is as in Theorem 1.1. Recalling the constant $c(E, Q_{-D})$ defined in (1.4), we have the following lemma which counts the points with bounded height on $E(\mathbb{Q})$ with denominators that are coprime to w.

Lemma 2.4. *Assume the notation and hypotheses in Theorem 1.1. If $T > 4d(E)$, then*

$$\#\{P = \left(\tfrac{A}{C^2}, \tfrac{B}{C^2} \right) \in E(\mathbb{Q}) \mid \widehat{h}(P) \leq T/4 \ \text{and} \ \gcd(C, w) = 1\}$$
$$\geq c(E, Q_{-D}) \cdot T^{\frac{r}{2}} - \widehat{c}(E, Q_{-D}) \cdot T^{\frac{r-1}{2}}.$$

Proof. Let $\mathcal{B} := \{P_1, \ldots, P_r\}$ be any basis for $E(\mathbb{Q})$, and consider linearly independent vectors $v_1, v_2, \ldots, v_r \in \mathbb{R}^r$ for which $v_i \cdot v_j = \langle P_i, P_j \rangle$. Let $\psi : E(\mathbb{Q}) \to \mathbb{R}^r$ be the additive homomorphism defined so that $\psi(P_i) = v_i$, and $\psi(E_{\mathrm{tor}}(\mathbb{Q}))$ is the origin.

For any integer n, let

$$(2.5) \qquad E_{\langle n \rangle} := \{P = \left(\tfrac{A}{C^2}, \tfrac{B}{C^2} \right) \in E(\mathbb{Q}) \mid \widehat{h}(P) \leq T \ \text{and} \ n \mid C\}.$$

If p is prime, then $E_{\langle p \rangle}$ is the kernel of the reduction modulo p map $E(\mathbb{Q}) \to E(\mathbb{F}_p)$, which includes the point at infinity. This set is closed under addition, and the image $\Lambda_p := \psi(E_{\langle p \rangle})$ is a lattice. If p is a prime of good reduction for E, then this follows since the reduction map is a group homomorphism. Otherwise, the claim is straightforward to confirm directly with the definition of the group law. More generally, $\Lambda_n := \psi(E_{\langle n \rangle})$ is a lattice for any square-free integer n, since $\Lambda_n = \bigcap_{p \mid n} \Lambda_p$.

By the Nagell-Lutz Theorem, $E_{\langle n \rangle} \cap E_{\text{tor}}(\mathbb{Q})$ is trivial if $n > 1$, and so ψ is injective on $E_{\langle n \rangle}$. Thus, by an inclusion/exclusion argument we have that

$$(2.6) \quad \#\left\{ P = \left(\tfrac{A}{C^2}, \tfrac{B}{C^2} \right) \in E(\mathbb{Q}) \mid \widehat{h}(P) \leq T/4 \text{ and } \gcd(C, w) = 1 \right\}$$
$$= |E_{\text{tor}}(\mathbb{Q})| \cdot \#(\Lambda_1 \cap B(\tfrac{1}{2}T^{\frac{1}{2}})) - \sum_{p \mid w} \#(\Lambda_p \cap B(\tfrac{1}{2}T^{\frac{1}{2}})) + \sum_{\substack{p,q \mid w \\ p \neq q}} \#(\Lambda_{pq} \cap B(\tfrac{1}{2}T^{\frac{1}{2}})) - \dots,$$

where the sums are over prime divisors of w.

By Lemma 2.3, we have that

$$\left| \frac{2^r \operatorname{Vol}(\mathcal{P}_n)}{\Omega_r} \cdot \#\{\Lambda \cap B(\tfrac{1}{2}T^{\frac{1}{2}})\} - T^{\frac{r}{2}} \right| \leq 3^r T^{\frac{r-1}{2}} d_n^{\frac{1}{2}},$$

where d_n is the minimum diameter of any choice of $\mathcal{P}_n$. Note that if $\mathcal{P}_n$ is any parallelepiped for Λ_n, then

$$\operatorname{Vol}(\mathcal{P}_n) = [\Lambda_1 : \Lambda_n] \operatorname{Vol}(\mathcal{P}_1).$$

Moreover, since $E_{\langle n \rangle} \cap E_{\text{tor}}(\mathbb{Q})$ is trivial for $n > 1$, we have that

$$[\Lambda_1 : \Lambda_n] \cdot |E_{\text{tor}}(\mathbb{Q})| = |E(\mathbb{Q})/E_{\langle n \rangle}| = \prod_{p \mid n} |E(\mathbb{F}_p)|.$$

Together, these two equations give that

$$\frac{\Omega_r}{\operatorname{Vol}(\mathcal{P}_n)} = \frac{\Omega_r \cdot E_{\text{tor}}(\mathbb{Q})}{\operatorname{Vol}(\mathcal{P}_1) \cdot \prod_{p \mid n} |E(\mathbb{F}_p)|}.$$

We may choose $\mathcal{P}_n$ so that

$$\sqrt{d_n} \leq [\Lambda_1 : \Lambda_n] \sqrt{d_1}.$$

Together with (2.6), these imply that

$$(2.7) \quad \#\left\{ P = \left(\tfrac{A}{C^2}, \tfrac{B}{C^2} \right) \in E(\mathbb{Q}) \mid \widehat{h}(P) \leq T \text{ and } \gcd(C, w) = 1 \right\}$$
$$\geq \frac{|E_{\text{tor}}(\mathbb{Q})|}{2^r \sqrt{R_{\mathbb{Q}}(E)}} \cdot \Omega_r \cdot \left(T^{\frac{r}{2}} \cdot \prod_{\substack{p \text{ prime} \\ p \mid w}} \left(1 - \frac{1}{|E(\mathbb{F}_p)|} \right) - 3^r 2^{\omega(w)} T^{\frac{r-1}{2}} \sqrt{d_1} \right),$$

where $\omega(w)$ is the number of distinct prime factors of w. Since $2^{\omega(w)} = \mathcal{S}(w)$, the lemma follows. $\qquad \square$

These same arguments can be used to give lower bounds for the number of points of bounded height generated from any linearly independent points in $E(\mathbb{Q})$.

Lemma 2.5. *Assume the notation and hypotheses above. Suppose G is a subgroup of $E_{\text{tor}}(\mathbb{Q})$, and that $\mathcal{B} := \{P_1, \dots, P_m\}$ is a set of linearly independent points in $E(\mathbb{Q})$ listed in ascending order by height. If $T > 4d(\mathcal{B})$, then*

$$\#\{P = \left(\tfrac{A}{C^2}, \tfrac{B}{C^2}\right) \in E(\mathbb{Q}) \mid \widehat{h}(P) \leq T/4 \text{ and } \gcd(C, w) = 1\}$$

$$\geq \frac{|G|}{2^r \sqrt{\widehat{h}(P_m)^m}} \cdot \Omega_m \left(T^{\frac{m}{2}} \cdot \prod_{\substack{p \text{ prime} \\ p|w}} \left(1 - \frac{1}{|E(\mathbb{F}_p)|}\right) - 3^m m^2 \mathcal{S}(w) \sqrt{2\widehat{h}(P_m)} T^{\frac{m-1}{2}} \right).$$

Proof. The proof of Lemma 2.4 applies with two modifications. Note that $d(\mathcal{B}) \leq 2m^2 \widehat{h}(P_m)$, and that the volume of the parallelepiped for $\mathcal{B}$ satisfies $\mathrm{Vol}(\mathcal{B}) \leq \prod_{i=1}^m \widehat{h}(P_i)^{1/2} \leq \widehat{h}(P_r)^{\frac{m}{2}}$. $\square$

Proof of Theorem 1.1. By hypothesis, we have that

$$(|u| + w^2)^2 \exp(4\delta(E) + d(E)) < D < \frac{(|u| + w^2)^2 \max(|u|, w^2)^2}{v^4}.$$

Lemma 2.4 implies that

$$(2.8) \quad \#\{P = \left(\tfrac{A}{C^2}, \tfrac{B}{C^3}\right) \in E(\mathbb{Q}) \mid \widehat{h}(P) \leq \tfrac{1}{4} T_E(-D, Q_{-D}) \text{ and } \gcd(w, C) = 1\}$$

$$\geq c(E, Q_{-D}) \cdot T_E(t)^{\frac{r}{2}} - \widehat{c}(E, Q_{-D}) T_E(t)^{\frac{r-1}{2}}.$$

We show that points $P_1 \neq \pm P_2$ in this set map to inequivalent forms when paired with $Q_{-D} = \left(\tfrac{u}{w^2}, \tfrac{v}{w^3}\right) \in E_{-D}(\mathbb{Q})$.

Suppose that $P_1 = (\tfrac{A_1}{C_1^2}, \tfrac{B_1}{C_1^3})$, $P_2 = (\tfrac{A_2}{C_2^2}, \tfrac{B_2}{C_2^3}) \in E(\mathbb{Q})$ satisfy $\widehat{h}(P_i) \leq \tfrac{1}{4} T_E(-D, Q)$, and let $F_1 := F_{P_1, Q_{-D}}(X, Y)$ and $F_2 := F_{P_2, Q_{-D}}(X, Y)$. Thanks to Theorem 2.2, we have that

$$(2.9) \quad h_W(P_i) \leq 2 \left(\widehat{h}(P_i) + \tfrac{1}{8} h_W(j(E)) + \tfrac{1}{12} h_W(\Delta(E)) + 0.973 \right)$$

$$\leq \tfrac{1}{2} \log \left| \frac{D}{(|u| + w^2)^2} \right| - \log(2) = \tfrac{1}{2} \log \left| \frac{D}{4(|u| + w^2)^2} \right|.$$

We observe that $\alpha_i = |A_i s w^2 - u C_i^2| \leq (|u| + w^2) H(P_i)$. By Theorem 2.2, we have

$$(2.10) \qquad\qquad H(P_i) = \exp(h_W(P_i)) \leq \frac{\sqrt{D}}{2(|u| + w^2)},$$

which gives that $\frac{\alpha_i}{G_i} \leq \tfrac{1}{2}\sqrt{D}$. Hence, we find that $\frac{\alpha_1}{G_1} \frac{\alpha_2}{G_2} \leq \tfrac{1}{4} D$, and so by Theorem 2.1, $F_1(X, Y)$ and $F_2(X, Y)$ are inequivalent, unless

$$(2.11) \qquad\qquad \frac{\alpha_1}{G_1} = \frac{|A_1 w^2 - u C_1^2|}{G_1} = \frac{|A_2 w^2 - u C_2^2|}{G_2} = \frac{\alpha_2}{G_2}.$$

Since $\gcd(A_i, C_i) = \gcd(C_i, w) = 1$, we have that $G_i = \gcd(\alpha_i, v^2)$, and so $G_i \leq v^2$. Rearranging (2.11), we obtain

$$(2.12) \qquad\qquad u(C_1^2 G_2 \pm C_2^2 G_1) = w^2 (A_1 G_2 \pm A_2 G_1),$$

where both signs are the same. Since u and w^2 are co-prime, we have that

$$(2.13) \qquad\qquad w^2 \mid (C_1^2 G_2 \pm C_2^2 G_1) \text{ and } u \mid (A_1 G_2 \pm A_2 G_1).$$

However, by hypothesis $D \leq \frac{(|u|+w^2)^2 \max(|u|,w^2)^2}{v^4}$, and so, combined with (2.10), we find that

$$|A_i|, C_i^2 \leq H(P_i) < \frac{\max(|u|, w^2)}{2v^2}.$$

This gives that

$$|C_1^2 G_2 \pm C_2^2 G_1| \text{ and } |A_1 G_2 \pm A_2 G_1| < \max(|u|, w^2).$$

However, the divisibility conditions in (2.13) imply that at least one of $(C_1^2 G_2 \pm C_2^2 G_1)$ and $(A_1 G_2 \pm A_2 G_1)$ is zero, and therefore, by (2.12), both are zero. Then we have that $A_1 G_2 = \pm A_2 G_1$, and $C_1^2 G_2 = \pm C_2^2 G_1$, where once again both signs are the same. Dividing these terms gives that $\frac{A_1}{C_1^2} = \frac{A_2}{C_2^2}$, which implies that $P_1 = \pm P_2$. This explains the extra factor of $1/2$ which appears in (1.3). This completes the proof. $\square$

3. An auxilary Diophantine result

Theorems 1.2 involves the quadratic twists of the elliptic curves

$$E^{(a)} : \quad y^2 = x^3 - a.$$

Here we prove an auxiliary Diophantine result (see Theorem 3.1), motivated by these curves, which will play a central role in the proof of Theorem 1.2. To make this precise, in this section we fix a curve $E^{(a)}$, where a is a positive integer, and we let $N^{(a)}$ denote its conductor, which is well known to be a multiple of 3.

Fix an arithmetic progression $h \pmod{4N^{(a)}}$, where $\gcd(h, 4N^{(a)}) = 1$. As $X \to +\infty$, we aim to count the number of square-free $0 < d < X$ for which there are integer triples (m, n, t) with

$$(3.1) \qquad\qquad -dt^2 = m^3 - an^6,$$

where

$$(3.2) \qquad \gcd(t, 6am) = 1, \ \gcd(n, am) = 1, \ m \equiv h \pmod{4N^{(a)}} \text{ and } n \equiv 0 \pmod{4N^{(a)}},$$

$$(3.3) \qquad\qquad T \leq t \leq 2T, \quad M \leq m \leq 2M, \quad N \leq n \leq 2N,$$

where[5] $M = M_a(X) := \frac{1}{4} T(X)^A \cdot X^{\frac{1}{3}}$ and $N = N_a(X) := \frac{1}{2} a^{-\frac{1}{6}} T(X)^B \cdot X^{\frac{1}{6}}$. Here we assume that $T := T(X)$ is a non-decreasing function from $\mathbb{R}^+ \mapsto [1, \infty)$, and we require that

$$(3.4) \qquad\qquad 0 < A < 2B < \frac{2}{3}.$$

For large X, this last condition guarantees that the square-free d in (3.1) satisfies $0 < d < X$.

For positive square-free integers d, we let

$$(3.5) \qquad\qquad N_h^{(a)}(d; X, T) := \#\{(m, n, t) \text{ satisfying } (3.1 - 3.4)\}.$$

Theorems 1.2 will be obtained from the following summatory asymptotic for $N_h^{(a)}(d; X, T)$.

Theorem 3.1. *Assume the notation and hypotheses above. As $X \to +\infty$, we have*

$$\sum_{1 \leq d \leq X} N_h^{(a)}(d; X, T) \asymp_a X^{\frac{1}{2}} T^{A+B-1} + o_{a,\varepsilon}(X^{\frac{1}{3}+\varepsilon} T^{A+1}).$$

---

[5]The function $M_a(X)$ does not depend on the choice of a.

Three Remarks.
(1) Theorem 3.1 illustrates that the vast majority of triples (m, n, t), for any given d, have small t. If $T(X) = o(X^\varepsilon)$, then the summation in the theorem is $\gg_a X^{\frac{1}{2}-\varepsilon}$. Indeed, one can even choose $T(X) := 1$ and obtain this asymptotic. On the other hand, since $-1 < A + B - 1 < 0$, the asymptotic is $o(X^{\frac{1}{2}-\varepsilon})$ if $T(X) := X^C$ for any positive C.

(2) Assuming the hypotheses of Theorem 3.1, an elementary argument (see (3.16)) shows that $N_h^{(a)}(d; X, T) = O(X^\varepsilon)$. Therefore, if $T = T(X) = o(X^{\frac{1}{6(B-2)}})$ (e.g. a log power), then we have
(3.6)
$$\#\left\{-X < -D < 0 \ : \ \exists \left(\frac{u}{w^2}, \frac{v}{w^3}\right) \in E_{-D}^{(a)}(\mathbb{Q}) \setminus E_{\text{tor}}^{(a)}(\mathbb{Q}) \text{ with } T \le v \le 2T\right\} \gg_{a,\varepsilon} X^{\frac{1}{2}-\varepsilon} T^{A+B-1}.$$

(3) Soundararajan considered [24] similar Diophantine equations in his work on torsion in class groups of imaginary quadratic fields, and has results which are analogous to Theorem 3.1.

3.1. **The counting function $\rho_m^{(a)}(M)$.** The proof of Theorem 3.1 requires the counting function

(3.7)
$$\rho_m^{(a)}(M) := \#\{n \pmod{M} \ : \ an^6 \equiv m^3 \pmod{M}\},$$

where a, m and M are non-zero integers. The following lemma gives a closed formula for this function in terms of $\text{ord}_p(n) := \max\{t \ge 0 \ : \ p^t \mid n\}$, Legendre symbols $\left(\frac{\cdot}{p}\right)$ and the cubic residue symbol

(3.8)
$$\left[\frac{b}{p}\right]_3 := \begin{cases} 0 & \text{if } p \mid b, \\ -1 & \text{if } b \text{ is not a cubic residue modulo } p, \\ 1 & \text{if } b \text{ is a cubic residue modulo } p. \end{cases}$$

Lemma 3.2. *Assuming the notation above, the following are true.*
(1) The function $\rho_m^{(a)}(M)$ is multiplicative in M.
(2) If $p = 2$, $p \nmid am$ and $\alpha \ge 1$, then $\rho_m^{(a)}(2^\alpha) = \widetilde{\rho}_m^{(a)}(2^\alpha)$, where

$$\widetilde{\rho}_m^{(a)}(2^\alpha) := \begin{cases} 1 & \text{if } \alpha = 1, \\ 1 + \displaystyle\prod_{q \mid am \text{ prime}} \left(\frac{-1}{q}\right) & \text{if } \alpha \ge 2. \end{cases}$$

(3) If $p = 3$, $p \nmid am$ and $\alpha \ge 1$, then $\rho_m^{(a)}(3^\alpha) = \widetilde{\rho}_m^{(a)}(3^\alpha)$, where

$$\widetilde{\rho}_m^{(a)}(3^\alpha) := \begin{cases} \left(1 + \left(\frac{a^{-1}m}{3}\right)\right) & \text{if } \alpha = 1, \\ \frac{3}{2} \cdot \left(1 + \left(\frac{a^{-1}m}{3}\right)\right) \left(1 + \left[\frac{a^{-1}}{9}\right]_3\right) & \text{if } \alpha \ge 2. \end{cases}$$

(4) If $p \ge 5$ is prime, $p \nmid am$ and $\alpha \ge 1$, then $\rho_m^{(a)}(p^\alpha) = \widetilde{\rho}_m^{(a)}(p^\alpha)$, where

$$\widetilde{\rho}_m^{(a)}(p^\alpha) := \frac{1}{2} \cdot \left(1 + \left[\frac{a^{-1}}{p}\right]_3\right) \left(1 + \left(\frac{a^{-1}m}{p}\right)\right) \left(2 + \left(\frac{-3}{p}\right)\right).$$

(5) *If $p \geq 5$ is prime, $p \nmid a$, $p|m$ and $\alpha \geq 1$, then $\rho_m^{(a)}(p^\alpha) = \widehat{\rho}_m^{(a)}(p^\alpha)$, where*

$$\widehat{\rho}_m^{(a)}(p^\alpha) := \begin{cases} 2\alpha - 1 & \text{if } \alpha \leq 3 \cdot \operatorname{ord}_p(m), \\ 0 & \text{if } \alpha > 3 \cdot \operatorname{ord}_p(m) \text{ and } 2 \nmid \operatorname{ord}_p(m), \\ \widetilde{\rho}_{m/p^{\operatorname{ord}_p(m)}}^{(a)}(p^{\alpha - 3 \cdot \operatorname{ord}_p(m)}) & \text{if } \alpha > 3 \cdot \operatorname{ord}_p(m) \text{ and } 2|\operatorname{ord}_p(m). \end{cases}$$

(6) *If $p \geq 5$ is prime, $p|a$ and $\alpha \geq 1$, then*

$$\rho_m^{(a)}(p^\alpha) = \begin{cases} p^\alpha & \text{if } \alpha \leq 3 \cdot \operatorname{ord}_p(m) \text{ and } \alpha \leq \operatorname{ord}_p(a), \\ 2 \cdot (\alpha - \operatorname{ord}_p(a)) - 1 & \text{if } \alpha \leq 3 \cdot \operatorname{ord}_p(m) \text{ and } \alpha > \operatorname{ord}_p(a), \\ \widehat{\rho}_{m/p^{\operatorname{ord}_p(a)}}^{(a)}(p^{\alpha - \operatorname{ord}_p(a)}) & \text{if } \alpha > 3 \cdot \operatorname{ord}_p(m) > \operatorname{ord}_p(a), \\ \widetilde{\rho}_{m/p^{\operatorname{ord}_p(a)}}^{(a)}(p^{\alpha - \operatorname{ord}_p(a)}) & \text{if } \alpha > 3 \cdot \operatorname{ord}_p(m) = \operatorname{ord}_p(a). \end{cases}$$

Proof. Claim (1) follows immediately by the Chinese Remainder Theorem.

For claim (2), since $2 \nmid am$, we may rewrite the congruence equation as the equation

$$n^6 \equiv a^{-1}m^3 \pmod{2^\alpha}.$$

By observation, we have $\rho_m^{(a)}(2) = 1$. Moreover, for any $\alpha \geq 2$, using Hensel's Lemma, we get $\rho_m^{(a)}(2^\alpha) = \rho_m^{(a)}(4)$. Since $(\mathbb{Z}/4\mathbb{Z})^\times$ is cyclic group of order 2, the congruence is $1 \equiv am \pmod 4$. Hence, this condition is determined by $1 + \displaystyle\prod_{q|am \text{ prime}} \left(\frac{-1}{q}\right)$.

Similarly, for claim (3), we consider the equation $n^6 \equiv a^{-1}m^3 \pmod{3^\alpha}$. If $\alpha = 1$, then it turns out that $1 \equiv a^{-1}m \pmod 3$, which corresponds to the factor $1 + \left(\frac{a^{-1}m}{3}\right)$. Furthermore, for any $\alpha \geq 2$, using Hensel's Lemma, we only need to consider the equation $n^6 \equiv a^{-1}m^3 \pmod 9$. Since $(\mathbb{Z}/9\mathbb{Z})^\times$ is a cyclic group of order 6, the equations becomes $1 \equiv a^{-1}m^3 \pmod 9$. Hence, we have $\rho_m^{(a)}(3^\alpha) = 6$ if $a^{-1}m$ is a quadratic residue modulo 3 and a^{-1} is a cubic residue modulo 9. Otherwise, we have $\rho_m^{(a)}(3^\alpha) = 0$.

For claim (4), we again apply Hensel's Lemma to get $\rho_m^{(a)}(p^\alpha) = \rho_m^{(a)}(p)$. Therefore, it suffices to establish the formula for $\rho_m^{(a)}(p)$. It is clear that $\rho_m^{(a)}(p) = 0$ when a^{-1} is not a cubic residue modulo p, or $a^{-1}m$ is not quadratic residue modulo p. Moreover, since p is an odd prime, if $\rho_m^{(a)}(p) \neq 0$, then the condition $p \equiv 1 \pmod 3$ and $p > 3$ gives $\rho_m^{(a)}(p) = 6$. Otherwise, we have $\rho_m^{(a)}(p) = 2$. These two cases determine the last factor $2 + \left(\frac{-3}{p}\right)$.

Next, we deal with claims (5) by factoring out prime factor p of a and m to get the results from previous claims (2)–(4). For claim (5), if $\alpha \leq 3 \cdot \operatorname{ord}_p(m)$, then we solve the equation $n^6 \equiv 0 \pmod{p^\alpha}$. Hence, we have $\rho_m^{(a)}(p^\alpha) = 2\alpha - 1$. Moreover, if $\alpha > 3 \cdot \operatorname{ord}_p(m)$, then $2 \nmid \operatorname{ord}_p(m)$ gives $\rho_m^{(a)}(p^\alpha) = 0$ by comparing p-valuations on the both sides of the equation. Now, we consider the last case $\alpha > 3 \cdot \operatorname{ord}_p(m)$ and $2|\operatorname{ord}_p(m)$. After removing the prime factor from the original equation, we have

$$n^6 \equiv a^{-1}\left(\frac{m}{p^{\operatorname{ord}_p(m)}}\right)^3 \pmod{p^{\alpha - 3 \cdot \operatorname{ord}_p(m)}}.$$

Hence, we can use claims (2)–(4) to solve the above equation. Finally, we apply the same argument to obtain (6). Hence, the result follows from the previous claims (2)–(5). □

To prove Theorem 3.1, we will need to obtain "average value" results for $\rho_m^{(a)}(M)$. To this end, we must contend with the fact that the cubic residue symbol $\left[\frac{\cdot}{p}\right]_3$ is not multiplicative. However, using the algebraic number theory of the Eisenstein field, we can circumvent this issue by making use of the genuine cubic character $\left(\frac{\cdot}{\pi}\right)_3$.

To make this precise, we let $\omega := (-1 + \sqrt{-3})/2$, and we employ the ring of Eisenstein integers $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$. Let π be a prime in $\mathbb{Z}[\omega]$ such that the norm $N(\pi) \neq 3$. Given any $\beta \in \mathbb{Z}[\omega]$ and $k \in \{0, 1, 2\}$, the *cubic residue character* of $\beta \pmod{\pi}$ is defined by

$$(3.9) \qquad \left(\frac{\beta}{\pi}\right)_3 := \begin{cases} \omega^k & \text{if } \beta^{\frac{N(\pi)-1}{3}} \equiv \omega^k \pmod{\pi}, \\ 0 & \text{if } \pi \mid \beta. \end{cases}$$

Lemma 3.3. *Assuming the notation above, the following are true.*
(1) The cubic function $\left(\frac{\cdot}{\pi}\right)_3$ defines a multiplicative character from $\mathbb{Z}[\omega]$ to $\mathbb{C}$.
(2) If $N(\pi) = p$ is a prime $p \equiv 1 \pmod{3}$, then $p = \pi \cdot \overline{\pi}$, where $\overline{\pi}$ is the conjugate of π in $\mathbb{Z}[\omega]$, and we have

$$\left[\frac{n}{p}\right]_3 = \frac{2}{3} \cdot \left(\frac{n}{\pi}\right)_3 + \frac{2}{3} \cdot \left(\frac{n}{\overline{\pi}}\right)_3 - \frac{1}{3}.$$

(3) If $\pi = p$ is a prime with $p \equiv 2 \pmod{3}$, then for any $n \in \mathbb{Z}$ with $p \nmid n$ we have

$$\left[\frac{n}{p}\right]_3 = \left(\frac{n}{p}\right)_3.$$

Proof. Given any β_1 and β_2 in $\mathbb{Z}[\omega]$. By the definition of $\left(\frac{\cdot}{\pi}\right)_3$, we obtain

$$\left(\frac{\beta_1\beta_2}{\pi}\right)_3 = \left(\frac{\beta_1}{\pi}\right)_3 \left(\frac{\beta_2}{\pi}\right)_3.$$

Hence, the claim (1) holds.

Next, we recall the well-known fact that

$$(3.10) \qquad n \text{ is a cubic residue modulo } \pi \iff \left(\frac{n}{\pi}\right)_3 = 1.$$

Suppose that n is a cubic residue modulo p. Then n is a cubic residue modulo π (resp. $\overline{\pi}$). Hence, by the definition of cubic residue symbol and (3.10), we have

$$\left[\frac{n}{p}\right]_3 = 1 = \frac{2}{3} \cdot \left(\frac{n}{\pi}\right)_3 + \frac{2}{3} \cdot \left(\frac{n}{\overline{\pi}}\right)_3 - \frac{1}{3}.$$

Similarly, if n is a cubic non-residue modulo p, then we have n is a cubic non-residue modulo π (resp. $\overline{\pi}$). It follows that

$$\left[\frac{n}{p}\right]_3 = -1, \quad \text{and} \quad \overline{\left(\frac{n}{\pi}\right)_3} = \left(\frac{n}{\overline{\pi}}\right)_3 \neq 1.$$

Hence, by the fact that $\left(\frac{n}{\pi}\right)_3 + \overline{\left(\frac{n}{\pi}\right)_3} = -1$, we get the desired formula.

Last, we deal with the claim (3). Since $p \equiv 2 \pmod{3}$, we know that p is still a prime in $\mathbb{Z}[\omega]$. Hence, the proof of (3) is directly from the fact that every integer is a cubic residue modulo p for $p \equiv 2 \pmod{3}$. $\qquad \square$

3.2. **Some average value theorems for $\rho_m^{(a)}(M)$.** To prove Theorem 3.1, we require asymptotic formulas controlling the average behavior of the counting functions $\rho_m^{(a)}(M)$. To this end, we need to establish that there is ample cancellation for certain sums arising from Legendre symbols and the cubic residue symbols.

Such cancellation can be deduced using the Pólya-Vinogradov [16, 27] inequality for any non-principal Dirichlet character $\chi(\cdot)$ modulo q

$$(3.11) \qquad \sum_{M \leq n \leq M+X} \chi(n) \ll \sqrt{q} \log q,$$

where the implied constant in $\ll$ is absolute. The following lemma, which involves $\tau(n)$, the number of divisors of n, and Euler's totient function $\varphi(n)$, will play a central role in the proof of the two parts of Theorem 3.1.

Lemma 3.4. *If t is an integer for which $\gcd(t,6) = 1$, and let d_1, d_2, and d_3 denote square-free divisors of t for which $d_2 \neq 1$, then we have*

$$\sum_{\substack{M \leq m \leq 2M \\ m \equiv h \ (\mathrm{mod}\ 4N^{(a)}) \\ \gcd(6am,t)=1}} \left(\frac{a^{-1}}{d_1}\right)_3 \left(\frac{a^{-1}m}{d_2}\right) \left(\frac{-3}{d_3}\right) \ll_a \tau(t)\sqrt{d_2}\log d_2.$$

Proof. Using the orthogonality property of the two Dirichlet characters modulo $4N^{(a)}$ to isolate the congruence class $m \equiv h \,(\mathrm{mod}\ 4N^{(a)})$, we immediately obtain

$$K := \sum_{\substack{M \leq m \leq 2M \\ m \equiv h \ (\mathrm{mod}\ 4N^{(a)}) \\ \gcd(6am,t)=1}} \left(\frac{a^{-1}}{d_1}\right)_3 \left(\frac{a^{-1}m}{d_2}\right) \left(\frac{-3}{d_3}\right)$$

$$= \frac{1}{\varphi(4N^{(a)})}\left(\frac{a^{-1}}{d_1}\right)_3 \left(\frac{-3}{d_3}\right) \sum_{\chi \ (\mathrm{mod}\ 4N^{(a)})} \sum_{\substack{M \leq m \leq 2M \\ \gcd(6am,t)=1}} \chi(h^{-1}m)\left(\frac{a^{-1}m}{d_2}\right).$$

We now use the elementary fact that $\sum_{d|n}\mu(d) = 1$ (resp. 0) if $n = 1$ (resp. $n > 1$). Namely, by considering factorizatons of m, say $m = fg$, we obtain

$$K = \frac{1}{\varphi(4N^{(a)})}\left(\frac{a^{-1}}{d_1}\right)_3 \left(\frac{-3}{d_3}\right) \sum_{\chi \ (\mathrm{mod}\ 4N^{(a)})} \sum_{M \leq m \leq 2M} \sum_{f|\gcd(6am,t)} \mu(f)\chi(h^{-1}m)\left(\frac{a^{-1}m}{d_2}\right)$$

$$\leq \frac{1}{\varphi(4N^{(a)})} \sum_{\chi \ (\mathrm{mod}\ 4N^{(a)})} \sum_{f|t} \left| \sum_{M/f \leq m \leq 2M/f} \chi(g)\left(\frac{g}{d_2}\right) \right|.$$

Note that $\chi(\cdot)\left(\frac{\cdot}{d_2}\right)$ is a non-principal character with conductor that is a divisor of $4N^{(a)}d_2$. Therefore, the Pólya-Vinogradov inequality (3.11) gives

$$K \ll_a \sum_{f|t} \sqrt{d_2}\log d_2 = \tau(t)\sqrt{d_2}\log d_2.$$

This completes the proof. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

The lemma above establishes cancellation when summing over m, which appears in an upper parameter of a quadratic residue symbol. The proof of Theorem 3.1 also requires the following lemma which guarantees ample cancellation of a similar sum involving the lower parameters of these symbols. To state this lemma, we let $\omega(n)$ denote the number of distinct prime factors of n, and we let $\widehat{\omega}(\alpha)$, where $\alpha \in \mathbb{Z}[\omega]$, denote the number of distinct prime factors $\pi \equiv 1 \pmod{3}$. Moreover, we extend the Möbius function to $\mathbb{Z}[\omega]$ in the natural way.

Lemma 3.5. *Suppose that a and m are non-zero integers for which am is not an integral square, and a is not an integral cube. If $R_1, R_2, R_3 \geq 2$ are integers and $T > 0$, then we have*

$$\Psi_m^{(a)}(R_1, R_2, R_3; T) := \sum_{\substack{r_1 r_1' \leq 2T/R_1 \\ \gcd(r_1 r_1', 6am)=1}} \sum_{\substack{r_2 r_2' \leq 2T/R_2 \\ \gcd(r_2 r_2', 6am)=1}} \sum_{\substack{r_3 r_3' \leq 2T/R_3 \\ \gcd(r_3 r_3', 6am)=1}} S_{1,r_1} \cdot S_{2,r_2} \cdot S_{3,r_3}$$

$$\ll_a m^{\frac{3}{2}} \prod_{i=1}^{3} \left(\frac{T}{\sqrt{R_i}} \sqrt{\log m} \right),$$

where the r_i and r_i' are positive integers, and

$$S_{1,r_1} := \mu^2(r_1)\,(2/3)^{\widehat{\omega}(r_1)} \left(\frac{a^{-1}}{r_1} \right)_3, \quad S_{2,r_2} := \mu^2(r_2) \left(\frac{a^{-1}m}{r_2} \right), \quad S_{3,r_3} := \mu^2(r_3)\,(1/2)^{\omega(r_3)} \left(\frac{-3}{r_3} \right).$$

Proof. Using the coprimality condition $\gcd(6am, r_1 r_2 r_3) = 1$, we may reformulate the given triple sum in terms of characters with explicit conductors that we shall use when applying the Pólya-Vinogradov inequality (3.11). Namely, we have

$$(3.12) \qquad\qquad \Psi_m^{(a)}(R_1, R_2, R_3; T) = G_1 \cdot G_2 \cdot G_3,$$

where, for each i, we have

$$G_i := \sum_{\substack{r_i r_i' \leq 2T/R_i \\ \gcd(r_i', 6am)=1}} \widetilde{S}_{i,r_i},$$

with

$$\widetilde{S}_{1,r_1} := \mu^2(r_1)\,(2/3)^{\widehat{\omega}(r_1)} \left(\frac{216a^2 m^3}{r_1} \right)_3, \quad \widetilde{S}_{2,r_2} := \mu^2(r_2) \left(\frac{36am}{r_2} \right),$$

$$\widetilde{S}_{3,r_3} := \mu^2(r_3)\,(1/2)^{\omega(r_3)} \left(\frac{-12a^2 m^2}{r_3} \right).$$

The non-zero summands correspond to cases where $r_1 \in \mathbb{Z}[\omega]$ is square-free, and r_2 and r_3 are square-free in $\mathbb{Z}$. Therefore, the fact that $\sum_{d|n} \mu(d) = 1$ for $n = 1$, and 0 otherwise, allows us to

rewrite this sum as[6]

$$G_1 := \sum_{\substack{r_1' \leq 2T/R_1 \\ \gcd(r_1', 6am)=1}} \sum_{r_1 \leq 2T/r_1'} \sum_{\substack{l_1^2 | r_1 \\ r_1 = s_1 l_1^2}} \mu(l_1) \, (2/3)^{\widehat{\omega}(r_1)} \left(\frac{216a^2m^3}{r_1} \right)_3,$$

$$G_2 := \sum_{\substack{r_2' \leq 2T/R_2 \\ \gcd(r_2', 6am)=1}} \sum_{r_2 \leq 2T/r_2'} \sum_{\substack{l_2^2 | r_2 \\ r_2 = s_2 l_2^2}} \mu(l_2) \left(\frac{36am}{r_2} \right),$$

$$G_3 := \sum_{\substack{r_3' \leq 2T/R_3 \\ \gcd(r_3', 6am)=1}} \sum_{r_3 \leq 2T/r_3'} \sum_{\substack{l_3^2 | r_3 \\ r_3 = s_3 l_3^2}} \mu(l_3) \, (1/2)^{\omega(r_3)} \left(\frac{-12a^2m^2}{r_3} \right).$$

Note that we can view the cubic residue character $\left(\frac{216a^2m^3}{\cdot} \right)_3$ as a non-principal Dirichlet character of order 3 with conductor dividing $N(216a^2m^3) = 216^2 \cdot |a^4 m^6|$. Furthermore, $\left(\frac{36am}{\cdot} \right)$, and $\left(\frac{-12a^2m^2}{\cdot} \right)$ are non-principal characters with conductors dividing $36 \cdot |am|$ and $12 \cdot a^2m^2$, respectively. Using the Pólya-Vinogradov inequality (3.11) and partial summation, we have that the inner sums of G_1, G_2, and G_3 are bounded by $\ll_a m^3(\log m), \sqrt{m}(\log m)$, and $m(\log m)$, respectively. Depending on the comparative sizes of R_i and m (i.e. m large), we can also bound the inner sum trivially by $\ll \frac{R_i}{l_i^2}$. Hence, we have

$$G_1 \ll_a \sum_{\substack{r_1' \leq 2T/R_1 \\ \gcd(r_1', 6am)=1}} \sum_{l_1 \leq \sqrt{2T/r_1'}} \min \left(\frac{R_1}{l_1^2}, m^3(\log m) \right) \ll_a m^{\frac{3}{4}} \frac{m}{\sqrt{R_1}} \sqrt{\log T}.$$

Using the same calculation, we have

$$G_2 \ll_a m^{\frac{1}{4}} \frac{T}{\sqrt{R_2}} \sqrt{\log m} \quad \text{and} \quad G_3 \ll_a m^{\frac{1}{2}} \frac{T}{\sqrt{R_3}} \sqrt{\log m}.$$

The proof now follows from (3.12). $\qquad \qquad \square$

Using this lemma, we obtain the following average value result for $\rho_m^{(a)}(\cdot)$.

Lemma 3.6. *Assume the hypotheses in Theorem 3.1. If $T = o(X^{\frac{1}{16}})$ and $\gcd(h, 4N^{(a)}) = 1$, then as $X \to +\infty$, we have*

$$\sum_{\substack{M \leq m \leq 2M \\ m \equiv h \pmod{4N^{(a)}}}} \sum_{\substack{T \leq t \leq 2T \\ \gcd(t, 6am)=1}} \rho_m^{(a)}(t^2) \asymp_a X^{\frac{1}{3}} T^{A+1} + O_a(X^{\frac{7}{24}} T^{\frac{7A}{8}+1} (\log X)^{\frac{39}{8}}).$$

Proof. We recall that $\rho_m^{(a)}(M)$ is multiplicative in M. Moreover, Lemma 3.2 (4) offers a particularly simple expression for $\rho_m^{(a)}(p^\alpha)$ for primes $p \geq 5$. To prove (1), we begin by restricting to $\gcd(6, t) = 1$. Lemma 3.3 gives

$$\Upsilon_h^{(a)}(M, T) := \sum_{\substack{M \leq m \leq 2M \\ m \equiv h \pmod{4N^{(a)}}}} \sum_{\substack{T \leq t \leq 2T \\ \gcd(t, 6am)=1}} \rho_m^{(a)}(t^2) = \sum_{\substack{M \leq m \leq 2M \\ m \equiv h \pmod{4N^{(a)}}}} \sum_{\substack{T \leq t \leq 2T \\ \gcd(t, 6am)=1}} \sum_{\substack{\theta | t \\ r_i | t, i=2,3}} S_{1,\theta} \cdot S_{2,r_2} \cdot S_{3,r_3},$$

---

[6]The condition $r_i = s_i l_i^2$ includes all factorizations (modulo choices of roots of unity) of r_i over $\mathbb{Z}[\omega]$ when $i = 1$, and r_2 and r_3 over $\mathbb{Z}^+$.

where we recall that

$$S_{1,\theta} = \mu^2(\theta) \left(\frac{2}{3}\right)^{\widehat{\omega}(\theta)} \left(\frac{a^{-1}}{\theta}\right)_3, \quad S_{2,r_2} = \mu^2(r_2)\left(\frac{a^{-1}m}{r_2}\right), \quad S_{3,r_3} = \mu^2(r_3)\left(\frac{1}{2}\right)^{\omega(r_3)} \left(\frac{-3}{r_3}\right).$$

For convenience, we let

$$\Upsilon_h^{(a)}(M,T) = Y_{h,0}^{(a)}(M,T) + Y_{h,1}^{(a)}(M,T),$$

where $Y_{h,0}^{(a)}(M,T)$ consists of the summands where $\theta = r_2 = r_3 = 1$, and $Y_{h,1}^{(a)}(M,T)$ denotes the remaining terms. We find that $Y_{h,0}^{(a)}(M,T)$ satisfies

$$Y_{h,0}^{(a)}(M,T) := \sum_{\substack{M \leq m \leq 2M \\ m \equiv h \pmod{4N^{(a)}}}} \sum_{\substack{T \leq t \leq 2T \\ \gcd(t,6am)=1}} 1 = \sum_{\substack{M \leq m \leq 2M \\ m \equiv h \pmod{4N^{(a)}}}} \left(T\frac{\varphi(6am)}{|6am|} + O(\tau(6am))\right)$$

$$\asymp_a MT + O_a((M+T)\log M).$$

Next, we estimate $Y_{h,1}^{(a)}(M,T)$, which consists of those summands with $\theta \cdot r_2 \cdot r_3 \neq 1 \pmod{\mathbb{Z}[\omega]^\times}$. Let $r_1 := \theta$. Then we separate the estimate of $Y_{h,1}^{(a)}(M,T)$ into two pieces by truncating the divisor of t: (1) $1 \leq r_i \leq R_i$ and (2) $r > R_i$. Hence, we can rewrite $Y_{h,1}^{(a)}(M,T)$

$$U_1 + U_2 := \sum_{\substack{M \leq m \leq 2M \\ m \equiv h \pmod{4N^{(a)}}}} \sum_{\substack{T \leq t \leq 2T \\ \gcd(t,6am)=1}} \left(\sum_{\substack{r_i|t,i=1,2,3 \\ 1 \leq r_i \leq R_i}} S_{1,r_1} \cdot S_{2,r_2} \cdot S_{3,r_3} + \sum_{\substack{r_i|t,i=1,2,3 \\ r_i \leq t/R_i}} S_{1,t/r_1} \cdot S_{2,t/r_2} \cdot S_{3,t/r_3}\right).$$

Moreover, we consider $t = r_i r_i'$ and rewrite U_2

$$\sum_{\substack{M \leq m \leq 2M \\ m \equiv h \pmod{4N^{(a)}}}} \sum_{\substack{r_i \leq 2T/R_i \\ \gcd(r_i,6am)=1}} \sum_{\substack{\max(T/r_i,R_i) \leq r_i' \leq 2T/r_i \\ \gcd(r_i',6am)=1}} S_{1,r_1'} \cdot S_{2,r_2'} \cdot S_{3,r_3'}.$$

Lemma [3.4] (1) asserts that

$$(3.13) \qquad U_1 \ll \sqrt{R_2}\log R_2 \sum_{T \leq t \leq 2T} \tau(t)^4 \ll T\sqrt{R_2}(\log X)^6.$$

We now estimate U_2 by splitting the sum into two parts.

$$U_2 = \sum_{\substack{M \leq m \leq 2M \\ m \equiv h \pmod{4N^{(a)}}}} \sum_{\substack{r_i \leq 2T/R_i \\ \gcd(r_i,6am)=1}} \sum_{\substack{\max(T/r_i,R_i) \leq r_i' \leq 2T/r_i \\ \gcd(r_i',6am)=1}} S_{1,r_1'} \cdot S_{2,r_2'} \cdot S_{3,r_3'}$$

$$\ll_a \sum_{\substack{M \leq m \leq 2M \\ a:\text{noncube, } am \neq \square}} \sum_{\substack{r_i \leq 2T/R_i \\ \gcd(r_i,6am)=1}} \sum_{\substack{\max(T/r_i,R_i) \leq r_i' \leq 2T/r_i \\ \gcd(r_i',6am)=1}} S_{1,r_1'} \cdot S_{2,r_2'} \cdot S_{3,r_3'} + \sum_{\substack{M \leq m \leq 2M \\ a:\text{cube, or } am=\square}} \sum_{\substack{r_i \leq 2T/R_i \\ \gcd(r_i,6am)=1}} \frac{T}{r_i}.$$

Moreover, since $m \leq 2M$ and $\log M \ll \log X$, Lemma 3.5 gives

$$(3.14) \qquad U_2 \ll_a M^{\frac{5}{2}} \prod_{i=1}^{3} \left(\frac{T}{\sqrt{R_i}} \sqrt{\log X} \right) + \sqrt{M} T^3 (\log X)^3.$$

To balance the exponents of M and $\log X$ in (3.13) and (3.14), we take $R_1 = R_2 = R_3 = M^{\frac{5}{4}}/(\log X)^{\frac{9}{4}}$, which in turn gives

$$Y_{h,1}^{(a)}(M, T) \ll_a M^{\frac{5}{8}} T^3 (\log X)^{\frac{39}{8}}.$$

By the hypothesis on T, we have $T^2 \ll M^{\frac{3}{8}}$, and so

$$Y_{h,1}^{(a)}(M, T) \ll_a M^{\frac{7}{8}} T (\log X)^{\frac{39}{8}}.$$

In view of the asymptotic for $Y_{h,0}^{(a)}(M, T)$, we see that $Y_{h,1}^{(a)}(M, T)$ is the error term for $\Upsilon^{(a)}(M, T)$, completing the proof. $\square$

3.3. **Proof of Theorem 3.1.** The claimed summatory formula for $N_h^{(a)}(d; X, T)$ counts the number of 3-tuples (m, n, t) satisfying (3.1-3.4), which guarantees that $(m^3 - an^6)/t^2$ is square-free and negative. We shall show that this count is well approximated by those tuples, where these values are not divisible by squares of small primes p. Namely, we let

$$(3.15) \qquad C_h^{(a)}(X, T) := \# \left\{ (m, n, t) \text{ satisfies } (3.1\text{-}3.4) \text{ and } p^2 \nmid \frac{(m^3 - an^6)}{t^2} \text{ for } p \leq \log X \right\}.$$

By hypothesis, for sufficiently large X, the dependence on the ranges for m and n on X guarantee that $m^3 - an^6$ is negative. Therefore, for large X, we find that $C_h^{(a)}(X, T)$ is a good approximation, provided that $E_{h,2}^{(a)}(X, T)$ and $E_{h,3}^{(a)}(X, T)$ are small, where $Z(X, T) := X^{\frac{1-C}{2}} (\log X)^{\frac{2}{3}}$ and

$$E_{h,2}^{(a)}(X, T) :=$$
$$\# \left\{ (m, n, t) \text{ satisfies } (3.1\text{-}3.4) \text{ and } p^2 \mid \frac{(m^3 - an^6)}{t^2} \text{ for some } \log X < p \leq Z(X, T) \right\},$$
$$E_{h,3}^{(a)}(X, T) := \# \left\{ (m, n, t) \text{ satisfies } (3.1\text{-}3.4) \text{ and } p^2 \mid \frac{(m^3 - an^6)}{t^2} \text{ for some } p > Z(X, T) \right\}.$$

We first obtain an asymptotic formula for $C_h^{(a)}(X, T)$. We define the product of small primes $P(X) := \prod_{p \leq \log X} p$. Then we have

$$C_h^{(a)}(X, T) = \sum_{m,t} \sum_{\substack{N \leq n \leq 2N \\ \gcd(n, am) = 1 \\ n \equiv 0 \pmod{4N^{(a)}} \\ an^6 \equiv m^3 \pmod{t^2}}} \sum_{l^2 \mid \gcd((an^6 - m^3)/t^2, P(X)^2)} \mu(l) = \sum_{m,t} \sum_{\substack{l \mid P(X) \\ \gcd(l, am) = 1}} \mu(l) \sum_{\substack{N \leq n \leq 2N \\ n \equiv 0 \pmod{4N^{(a)}} \\ an^6 \equiv m^3 \pmod{l^2 t^2}}} 1.$$

To be clear, the outer sum in both expressions above is over pairs (m, t) satisfying (3.1-3.4). Since $T \leq X^{\frac{1}{22}}$, for any $\varepsilon > 0$ we can bound the inner sum by

$$\frac{N}{4N^{(a)} l^2 t^2} \rho_m^{(a)}(l^2 t^2) + O_a(\rho_m^{(a)}(l^2 t^2)) = \frac{N}{4N^{(a)} l^2 t^2} \rho_m^{(a)}(l^2 t^2) + O_a(X^\varepsilon).$$

Here we used the fact that $\rho_m^{(a)}(t^2) = O_a(X^\varepsilon)$, which follows by multiplicativity and the fact that $\omega(t) = O(t^\varepsilon)$. Hence, we have

$$
\begin{aligned}
C_h^{(a)}(X,T) &= \sum_{(m,t)} \sum_{\substack{l|P(X) \\ \gcd(l,am)=1}} \mu(l) \left(\frac{N}{4N^{(a)}l^2t^2} \rho_m^{(a)}(l^2t^2) + O_a(X^\epsilon) \right) \\
&= \frac{N}{4N^{(a)}t^2} \sum_{m,t} \rho_m^{(a)}(t^2) \sum_{\substack{l|P(X) \\ \gcd(l,am)=1}} \frac{\mu(l)}{l^2} \rho_m^{(a)} \left(\frac{l}{\gcd(t,l)} \right) + O_a(\tau(P(X))X^\varepsilon) \\
&\asymp_a \frac{N}{T^2} \sum_{m,t} \rho_m^{(a)}(t^2) + O_a(X^\varepsilon).
\end{aligned}
$$

Applying Lemma 3.6, and by summing over m and t, we obtain

$$
C_h^{(a)}(X,T) \asymp_a \frac{MN}{T} + O_a(MTX^\varepsilon) \asymp_a X^{\frac{1}{2}}T^{A+B-1} + o_{a,\varepsilon}(X^{\frac{1}{3}+\varepsilon}T^{A+1}).
$$

Since the asymptotic for $C_h^{(a)}(X,T)$ above is the conclusion of the theorem, it suffices to show that $E_{h,2}^{(a)}(X,T)$ and $E_{h,3}^{(a)}(X,T)$ are of lower order. We now bound $E_{h,2}^{(a)}(X,T)$ by the following estimate

$$
\begin{aligned}
E_{h,2}^{(a)}(X,T) &= \sum_{m,t} \sum_{\log X \leq p \leq Z} \sum_{\substack{N \leq n \leq 2N \\ n \equiv 0 \pmod{4N^{(a)}} \\ an^6 \equiv m^3 \pmod{t^2p^2}}} 1 \ll_a \sum_{m,t} \sum_{\log X \leq p \leq Z} \left(\frac{N}{t^2p^2} \rho_m^{(a)}(t^2p^2) + O_a(\rho_m^{(a)}(t^2)) \right) \\
&\ll_a \sum_{m,t} \left(\frac{N\rho_m^{(a)}(t^2)}{T^2 \log X} + o_a \left(\left(\frac{X}{T} \right)^{\frac{1}{3}} \rho_m^{(a)}(t^2) \right) \right).
\end{aligned}
$$

We used the facts that $\rho_m^{(a)}(t^2p^2) \leq 6\rho_m^{(a)}(t^2)$ (see Lemma 3.2), $1/t^2 \leq 1/T^2$, $1/p^2 \leq 1/\log X$ and $(T/X)^{\frac{1}{3}} = o(1)$. Applying Lemma 3.6, and by summing over m and t, we have the lower order asymptotic

$$
E_{h,2}^{(a)}(X,T) \ll_a \frac{MN}{T \log X} + o_a \left(\frac{X^{\frac{1}{3}}}{T} \sum_{m,t} \rho_m^{(a)}(t^2) \right) \ll_a \frac{X^{\frac{1}{2}}T^{A+B-1}}{\log X} + o_a(X^{\frac{1}{3}}T^{-1}).
$$

Finally, we estimate $E_{h,3}^{(a)}(X,T)$ by using the arithmetic of number fields. Let $p > Z$ be prime, and suppose $d = p^2b$. Then we have $m^3 = an^6 - p^2bt^2$ and $b \ll \frac{X}{Z^2} = T/(\log X)^{\frac{4}{3}}$. Fix m in $[M, 2M]$ and with the condition of b, we claim that the number of choices for n and t is bounded by $o_a(m)$. Hence, by the claim, we have the lower order asymptotic

$$
E_{h,3}^{(a)}(X,T) \ll_a \frac{X}{Z^2} \sum_{M \leq m \leq 2M} \tau(m) \ll \frac{X}{Z^2}M \log X \ll_{a,\varepsilon} o_{a,\varepsilon}(X^{\frac{1}{3}+\varepsilon}T^{A+1}).
$$

Now, we prove the claim by factoring the equation $m^3 = an^6 - p^2bt^2$ in $\mathbb{Q}(\sqrt{a}, \sqrt{b})$; namely,

(3.16)
$$
(m)^3 = (\sqrt{a}n^3 + pt\sqrt{b})(\sqrt{a}n^3 - pt\sqrt{b}).
$$

Since $\gcd(m, n) = \gcd(m, a) = 1$ and m is odd, we have two coprime factors. Therefore, the number of choices for n and t is bounded by the total number of factorizations of the ideal (m), which is $o_a(m) = O(X^\varepsilon)$.

4. Proof of Theorems 1.2

We begin with an elementary lemma concerning the suitability of points on quadratic twists.

Lemma 4.1. *Assume the hypotheses of Theorem 3.1, and suppose that $T = o(X)$. Then the following are true.*

(1) *If $-D$ is odd, $Q_{-D} = (\frac{m}{n^2}, \frac{2t}{n^3}) \in E_{-D}^{(a)}(\mathbb{Q})$, where (m, n, t) satisfies (3.1-3.4) with $d = D$, then Q_{-D} is suitable in the sense of (1.7) when X is sufficiently large.*

(2) *If $-D = -4D_0$, where $D_0 \equiv 1, 2 \pmod 4$ is square-free, $Q_{-D} = (\frac{m}{n^2}, \frac{t}{n^3}) \in E_{-D}^{(a)}(\mathbb{Q})$, where (m, n, t) satisfies (3.1-3.4) with $d = D_0$, then Q_{-D} is suitable in the sense of (1.7) when X is sufficiently large.*

Remark. *Since we assume that v is even when $-D$ is odd, we choose to use m, n, and t instead of u, v, and w to avoid confusion and enjoy the convenience of working with a single equation.*

Proof. For brevity, we only consider when $-D$ is odd, as the same method applies to the other case. Recalling the convention in (1.2), by clearing denominators and dividing by 4 we obtain

$$(4.1) \qquad -Dt^2 = m^3 - an^6.$$

Furthermore, since Q_{-D} is suitable, we have

$$(4.2) \qquad (|m| + n^2) \exp\left(\delta(E^{(a)}) + d(E^{(a)})\right) < D < \frac{(|m| + n^2)^2 \max(|m|, n^2)^2}{16 t^4}.$$

We first consider the right hand inequality above using (4.1). We find that

$$t^4 < \frac{(|m| + n^2)^2 \max(|m|, n^2)^2}{16} \cdot \frac{t^2}{an^6 - m^3} \quad \iff \quad t^2 < \frac{(|m| + n^2)^2 \max(|m|, n^2)^2}{16(an^6 - m^3)}.$$

Recalling that $M := T^A X^{\frac{1}{3}}$ and $N := T^B X^{\frac{1}{6}}$ in (3.3), we have $N \gg_a \sqrt{M}$ as $X \to +\infty$. Therefore this inequality holds for sufficiently large X. For the left hand inequality in (4.2), the desired claim follows similarly from (4.1), as

$$t^2 < \frac{an^6 - m^3}{(|m| + n^2) \exp\left(\delta(E^{(a)}) + d(E^{(a)})\right)} \quad \iff \quad |t| < \sqrt{\frac{an^6 - m^3}{(|m| + n^2) \exp\left(\delta(E^{(a)}) + d(E^{(a)})\right)}}.$$

$\square$

We require an explicit lower bound for the ratio of constants defined by (1.3) and (1.4) for those points Q_{-D} considered in this lemma.

Lemma 4.2. *Assume the hypotheses of Theorem 3.1, and let $T = O(1)$. If X is sufficiently large, then Q_{-D} is suitable in the sense of (1.7), and we have*

$$c(E^{(a)}, Q_{-D}) > \frac{1}{5} \cdot \frac{c(E^{(a)})}{\log \log D}.$$

Remark. *The proof of Theorem 1.2 holds for any $T = o(X)$, giving $\gg_{a.\varepsilon} X^{\frac{1}{2}-\varepsilon}$ many discriminants with class number lower bounds. For example, we may let $T = (\log X)^C$, where $C > 0$. However the multiplicative constant in the effective class number lower bound would have to be modified by following the proof of Lemma 4.2.*

Proof. Lemma 4.1 guarantees that Q_{-D} is suitable for large X. Turning to the claimed inequality, we begin by noting that (1.3) and (1.4) give

$$\frac{c(E^{(a)}, Q_{-D})}{c(E^{(a)})} = \prod_{\substack{p \text{ prime} \\ p|n}} \left(1 - \frac{1}{|E^{(a)}(\mathbb{F}_p)|}\right).$$

As mentioned in the proof of Lemma 2.4, $|E^{(a)}(\mathbb{F}_p)|$ includes the point at infinity, and does not require that p is a prime of good reduction for $E^{(a)}$. For the small primes $p \in \{2, 3, 5\}$, we have $|E^{(a)}(\mathbb{F}_p)| = p + 1$. Therefore, the Hasse bound for trace of Frobenius for elliptic curves implies

$$\frac{c(E^{(a)}, Q_{-D})}{c(E^{(a)})} > \frac{5}{12} \cdot \prod_{\substack{p|n \\ p \geq 7 \text{ prime}}} \left(1 - \frac{1}{p + 1 - 2\sqrt{p}}\right) = \frac{5}{12} \cdot \prod_{\substack{p|n \\ p \geq 7 \text{ prime}}} \mathcal{F}(p) \cdot \left(1 - \frac{1}{p}\right),$$

where $\mathcal{F}(p) := \frac{p}{p-1}\left(1 - \frac{1}{p+1-2\sqrt{p}}\right)$. Since $0 < \mathcal{F}(p) < 1$ and rapidly monotonically tends to 1 as $p \to +\infty$, we have

$$\prod_{\substack{p|n \\ p \geq 7 \text{ prime}}} \mathcal{F}(p) > \prod_{p \geq 7 \text{ prime}} \mathcal{F}(p) > \frac{9}{20}.$$

Therefore, we have

$$\frac{c(E^{(a)}, Q_{-D})}{c(E^{(a)})} > \frac{3}{16} \cdot \prod_{\substack{p|n \\ p \geq 7 \text{ prime}}} \left(1 - \frac{1}{p}\right).$$

We are left with the problem of obtaining a lower bound for product over primes $p \geq 7$ (if any) which divide n above. Since the Euler factors increase monotonically to 1 with the primes, and $N \leq n \leq 2N$, we may bound this product from below with a product over sufficiently many consecutive primes $p \geq 7$. Namely, if $p_1 = 2$, $p_2 = 3, \ldots$ are the primes in order, then for large X we have

$$(4.3) \qquad \frac{c(E^{(a)}, Q_{-D})}{c(E^{(a)})} > \frac{3}{16} \cdot \prod_{i=4}^{\kappa(X)} \left(1 - \frac{1}{p_i}\right) = \frac{45}{64} \cdot \prod_{i=1}^{\kappa(X)} \left(1 - \frac{1}{p_i}\right),$$

where $\kappa(X) := [\log_2(2TX^{\frac{1}{2}})]$.

For $x > 1$, a classical theorem of Rosser and Schoenfeld [17, 18] unconditionally asserts that $\pi(x) \leq 1.255056 \cdot \frac{x}{\log x}$, where $\pi(x)$ is the usual prime counting function. Therefore, if X is sufficiently large, then the fact that $T = O(1)$ implies

$$(4.4) \qquad p_{\kappa(X)} \leq \frac{[\log_2(X^{\frac{1}{2}})]^2}{1.25} =: \lambda(X).$$

Let $x > 1$, then we recall the effective version of Merten's Theorem (see e.g. [17, Eq. (3.27)])

$$\prod_{p \leq x \text{ prime}} \left(1 - \frac{1}{p}\right) > \frac{e^{-\gamma}}{\log x} \left(1 - \frac{1}{\log^2 x}\right),$$

where $\gamma \approx 0.5772$ is the Euler-Mascheroni constant. Combining this with (4.3) and (4.4) gives

$$\frac{c(E^{(a)}, Q_{-D})}{c(E^{(a)})} > \frac{45}{64} \cdot \frac{e^{-\gamma}}{\log(\lambda(X))} \left(1 - \frac{1}{\log(\lambda(X))^2}\right) > 0.21586 \cdot \frac{1}{\log \log X}.$$

To complete the proof we must relate those discriminants $-D$ obtained from (3.1-3.4) to X. Namely, we need to consider the following equation

$$-dt^2 = m^3 - an^6,$$

where $d := D$ or D_0 depending on the parity of D. Since a is a positive integer and $T = O(1)$, the growth conditions of m and n imply

$$d = \frac{an^6 - m^3}{t^2} \geq \frac{aT^{6B}X - T^{3A}X}{4T^2} \gg_T X,$$

which in turn, for every $\varepsilon > 0$, gives $1/\log \log D \leq (1 + \varepsilon)/\log \log X$ for large X. Therefore, for large X we obtain

$$c(E^{(a)}, Q_{-D}) \geq 0.2158 \cdot \frac{c(E^{(a)})}{\log \log D}.$$

$\square$

Proof of Theorem 1.2. Suppose that a is a non-zero integer, and that $-D < 0$ is a fundamental discriminant for which there is a rational point $Q_{-D} = (\frac{m}{n^2}, \frac{2t}{n^3}) \in E_{-D}^{(a)}(\mathbb{Q})$, when D odd (resp. $Q_{-D} = (\frac{m}{n^2}, \frac{t}{n^3}) \in E_{-D}^{(a)}(\mathbb{Q})$, when $D = 4D_0$ even). We may assume that t is non-zero, and so Q_{-D} is not a 2-torsion point. Furthermore, it is well known that at most finitely many twists of $E^{(a)}$ (see Proposition 1 of [10]) have a torsion point with order $\neq 2$. Therefore, apart from possibly finitely many $-D$, we have that Q_{-D} has infinite order.

Recalling that our models are of the form (1.2), we find directly that (m, n, t) satisfies (3.1), giving a solution to

$$(4.5) \qquad\qquad -dt^2 = m^3 - an^6,$$

where $d := D$ or D_0 depending on the parity of D.

We let $W\left(E^{(a)}\right) \in \{\pm 1\}$ be the sign of the functional equation for the Hasse-Weil L-function $L(E^{(a)}, s)$. Recall that $N^{(a)}$ is the conductor of $E^{(a)}$. If we have $\gcd(-D, N^{(a)}) = 1$, then (see p. 3 of [10]) the sign of the functional equation for the quadratic twist $L(E_{-D}^{(a)}, s)$ is

$$(4.6) \qquad\qquad W\left(E_{-D}^{(a)}\right) = \left(\frac{-D}{N^{(a)}}\right) \cdot W\left(E^{(a)}\right).$$

Therefore, the Parity Conjecture implies that $r_{\mathbb{Q}}(E_{-D}^{(a)})$ is even when $\left(\frac{-D}{N^{(a)}}\right) = W\left(E^{(a)}\right)$. In particular, any triple (m, n, t) also satisfying (3.1-3.4) conditionally has $r_Q(E_{-D}^{(a)}) \geq 2$.

We now apply Theorem 3.1, with $A < 2B < 2/3$ and $T = O(1)$, with any $h \pmod{4N^{(a)}}$ for which (4.5) gives $\left(\frac{-d}{N^{(a)}}\right) = W\left(E^{(a)}\right)$. Theorem 3.1 and

$$(4.7) \qquad \sum_{1 \leq d \leq X} N_h^{(a)}(d; X, T) \asymp_a X^{\frac{1}{2}}.$$

By repeating the argument for (3.16), we have that $N_h^{(a)}(d; X, T) = O_\varepsilon(X^\varepsilon)$. Therefore, we obtain

$$\# \left\{ -X < -D < 0 \ : \ r_{\mathbb{Q}}(E_{-D}^{(a)}) \geq 1 \right\} \gg_{a,\varepsilon} X^{\frac{1}{2}-\varepsilon}.$$

Again, the Parity Conjecture allows us to further require that $r_{\mathbb{Q}}(E_{-D}^{(a)}) \geq 2$.

This lower bound produces $\gg_{a,\varepsilon} X^{\frac{1}{2}-\varepsilon}$ many discriminants $-X < -D < 0$ for which $E_{-D}^{(a)}$ has an explicit infinite order rational point Q_{-D}. Lemma 4.2 guarantees that Q_{-D} is suitable in the sense of (1.7), and also gives

$$c(E^{(a)}, Q_{-D}) \geq 0.2158 \cdot \frac{c(E^{(a)})}{\log \log D} > \frac{1}{5} \cdot \frac{c(E^{(a)})}{\log \log D}.$$

Therefore, Theorem 1.2 follows directly from Theorem 1.1. $\qquad\qquad\square$

REFERENCES

[1] A. Baker, *Linear forms in the logarithms of algebraic numbers*, Mathematika **13** (1966), 204–216.

[2] D. Buell, *Elliptic curves and class groups of quadratic fields*, J. London Math. Soc. **15** (1977), 19-25.

[3] D. Buell and G. Call, *Class pairings and isogenies on elliptic curves*, J. Numb. Th. **167** (2016), 31-73.

[4] N. Elkies, *February 23, 2016 email to NMBRTHRY list.*

[5] N. Elkies, *Private communication, May 19, 2020.*

[6] D. Goldfeld, *The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **3** (1976), 624-663.

[7] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Springer Lect. Notes **751** (1979), 108-118.

[8] D. Goldfeld, *Gauss' class number problem for imaginary quadratic fields*, Bull. Amer. Math. Soc. **13**, (1985), 23-37.

[9] M. Griffin and K. Ono, *Elliptic curves and lower bounds for class numbers*, J. Number Th., accepted for publication.

[10] F, Gouvêa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4** (1991), 1-23.

[11] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), 225-320.

[12] K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z., **56** (3) (1952), 227–253.

[13] A. Knapp, *Elliptic curves*, Princeton Univ. Press, 1992.

[14] J.-F. Mestre, *Rang des courbes elliptiques d'invariant donné,* C. R. Acad. Sci. Paris Sér. I **313** (1991), 171-174.

[15] J. Oesterlé, *Nombres de classes des corps quadratiques imaginaires*, Sem. Bourbaki **1983/1984**, No. 121-122 (1985), 309-323.

[16] G. Pólya, *Über die Verteilung der quadratischen Reste und Nichtreste*, Göttinger Nachrichten (1918), 21-29.

[17] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64-94.

[18] J. B. Rosser and L. Schoenfeld, *Sharper bounds for the Chebyshev functions $\theta(x)$ and $\Psi(x)$*, Math. Comp. **29** (1975), 243-269.

[19] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.0)*, 2020. https://www.sagemath.org.

[20] C. L. Siegel, *Über die Classenzahl quadratischer Zahlkörper*, Acta Arith. **1** (1935), 83–86.

[21] J. H. Silverman, *Heights and the specialization map for families of abelian varieties*, J. Reine Angew. Math. **342** (1983), 197-211.

[22] J. H. Silverman, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. **55** (1990), 723-743.

[23] R. Soleng, *Homomorphisms from the group of rational points on elliptic curves to class groups of quadratic number fields*, J. Numb. Th. **46** (1994), 214-229.

[24] K. Soundararajan, *Divisibility of class numbers of imaginary quadratic fields*, J. London Math. Soc. (2) **61** (2000), 681-690.

[25] H. M. Stark, *A complete determination of the complex quadratic fields of class number one*, Michigan Math. J. **14** (1967), 1–27.

[26] C. L. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc. **8** (1995), 943-973.

[27] I. M. Vinogradov, *Sur la distribution des résidus et des non-résidus des puissances*, J. Phys. Math. Soc. Univ. Perm. **1** (1918), 18-28.

Department of Mathematics, 275 TMCB, Brigham Young University, Provo, UT 84602
Email address: mjgriffin@math.byu.edu

Department of Mathematics, University of Virginia, Charlottesville, VA 22904
Email address: ken.ono691@virginia.edu
Email address: tsaiwlun@gmail.com