ELLIPTIC CURVES AND LOWER BOUNDS FOR CLASS NUMBERS

MICHAEL GRIFFIN AND KEN ONO

ABSTRACT. Ideal class pairings map the rational points of rank $r \geq 1$ elliptic curves $E/\mathbb{Q}$ to the ideal class groups $\mathrm{CL}(-D)$ of certain imaginary quadratic fields. These pairings imply that

$$h(-D) \geq \frac{1}{2}(c(E) - \varepsilon)(\log D)^{\frac{r}{2}}$$

for sufficiently large discriminants $-D$ in certain families, where $c(E)$ is a natural constant. These bounds are effective, and they offer improvements to known lower bounds for many discriminants.

1. INTRODUCTION AND STATEMENT OF RESULTS

Estimating 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 $-D$, is one of the oldest problems in number theory. Gauss conjectured that $h(-D) \to +\infty$ as $D \to \infty$. Heilbronn [12] confirmed this in the 1930s, and Siegel [17] shortly thereafter obtained a nearly definitive solution. For $\varepsilon > 0$, he proved that there are constants $c_1(\varepsilon), c_2(\varepsilon) > 0$ for which

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

Siegel's lower bound is inexplicit; there is no known formula for $c_1(\varepsilon)$. Therefore, his work could not even determine the class number 1 fundamental discriminants. Baker, Heegner, and Stark [1, 11, 21] later famously determined this list: $-D \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}$.

Thanks to work of Goldfeld, Gross and Zagier, modified and ingeniously optimized by Watkins, such lists are now known [22] for $h(-D) \leq 100$. The deep theorem of Goldfeld [7], published in 1976, offered effective class number lower bounds assuming the existence of an elliptic curve $E/\mathbb{Q}$ with analytic rank $r \geq 3$. Groundbreaking work by Gross and Zagier [9, 10] on the Birch and Swinnerton-Dyer Conjecture confirmed the existence of such curves ten years later, resulting in the effective lower bound [16]

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

Here we obtain effective lower bounds for certain discriminants using elliptic curves in a completely different way. Although we do not improve on (1.1) for all $-D$, the point of this note is to highlight and make use of an interesting interrelationship between class groups and elliptic curves that often leads to improved class number lower bounds. We 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 previously considered by Buell, Call, and Soleng [2, 3, 20]. The idea is quite natural. Throughout, suppose that $E/\mathbb{Q}$ is given

by

$$E: \quad y^2 = x^3 + a_4x + a_6, \tag{1.2}$$

where $a_4, a_6 \in \mathbb{Z}$, with j-invariant $j(E)$ and discriminant $\Delta(E)$, and suppose that $E(\mathbb{Q})$ has rank $r = r(E) \geq 1$. If $-D < 0$ is a fundamental discriminant, then let $E_{-D}/\mathbb{Q}$ be its quadratic twist[1]

$$E_{-D}: \ -D \cdot \left(\frac{y}{2}\right)^2 = x^3 + a_4x + a_6. \tag{1.3}$$

Furthermore, suppose that $Q_D = (u, v) \in E_{-D}(\mathbb{Q})$ is an integer point, where $v \neq 0$, with v even if $-D$ is odd.[2] Theorem 2.1 gives an explicit construction of the pairing. Therefore, the number of $\mathrm{SL}_2(\mathbb{Z})$-inequivalent forms obtained by pairing points in $E(\mathbb{Q})$ with Q_D gives a lower bound for $h(-D)$.

We derive lower bounds 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 (3.3)), and the torsion subgroup $E_{\mathrm{tor}}(\mathbb{Q})$. We define

$$c(E) := \frac{|E_{\mathrm{tor}}(\mathbb{Q})|}{\sqrt{R_{\mathbb{Q}}(E)}} \cdot \Omega_r, \tag{1.4}$$

and, in terms of the usual logarithmic heights (see Section 3) of $j(E)$ and $\Delta(E)$, we define

$$\delta(E) := \frac{1}{8}h_W(j(E)) + \frac{1}{12}h_W(\Delta(E)) + \frac{5}{3}. \tag{1.5}$$

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

$$T_E(D, Q_D) := \tfrac{1}{4}\log\left(\frac{D}{(1+|u|)^2}\right) - \delta(E). \tag{1.6}$$

Theorem 1.1. *Assuming the hypotheses above, if* $(1+|u|)^2\exp(4\delta(E)+d(E)) < D \leq \frac{(1+|u|)^2u^2}{v^4}$, *then*

$$h(-D) \geq \frac{c(E)}{2} \cdot \left(T_E(D, Q_D)^{\frac{r}{2}} - r\sqrt{d(E)} \cdot T_E(D, Q_D)^{\frac{r-1}{2}}\right).$$

Although the hypotheses for Theorem 1.1 are satisfied by many $E/\mathbb{Q}$ for each $-D$, we seek choices that improve (1.1). In view of (1.6), we require choices where the height of Q_D is small and where $c(E)$ is not too small. For each E, we offer a natural family of discriminants, those of the form $-D_E(t) := -4(t^3 + a_4t - a_6)$, with $t \in \mathbb{Z}$. In these cases, we choose $Q_{-D_E(t)} := (-t, 1)$.

Theorem 1.2. *If* $\varepsilon > 0$, *then there is an effectively computable constant* $N(E, \varepsilon) < 0$ *such that for negative fundamental discriminant of the form* $-D_E(t)$, *where* $t \in \mathbb{Z}$ *and* $-D_E(t) < N(E, \varepsilon)$, *we have*

$$h(-D_E(t)) \geq \frac{1}{2}\left(\frac{c(E)}{\sqrt{12^r}} - \varepsilon\right) \cdot \log(D_E(t))^{\frac{r}{2}}.$$

Remark. *Theorems 1.1 and 1.2 are stated under the assumption that the discriminants are fundamental for reasons of aesthetics. There is a straightforward modification that offers lower bounds for the class number of the corresponding imaginary quadratic field when* $-D$ *(resp.* $-D_E(t)$*) is not fundamental. We note that Theorem 2.1, which is the source of the lower bounds, holds for all discriminants. Namely, the proof gives lower bounds for the Hurwitz-Kronecker class*

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

[2] Goldfeld conjectures [8] that asymptotically half of the E_{-D} have rank 1, and so such points are plentiful. The integrality of Q_D is easily satisfied by changing models of E and E_{-D} by clearing denominators if necessary.

number $H(-D)$ (for example, see p. 273 [4]), the class number of discriminant $-D$ quadratic forms, which counts each class C with multiplicity $1/\mathrm{Aut}(C)$. Thankfully, Hurwitz class numbers satisfy a particularly nice multiplicative formula relative to class numbers with fundamental discriminant. If $-D = -D_0 f^2$, where $-D_0$ is a negative fundamental discriminant, then

$$H(-D) = \frac{h(-D_0)}{\omega(-D_0)} \cdot \sum_{d|f} \mu(d)\chi_{-D_0}(d)\sigma_1(f/d), \tag{1.7}$$

where $\mu(\cdot)$ is the Möbius function, $\omega(-D_0)$ is half the number of units in $\mathbb{Q}(\sqrt{-D_0})$, $\chi_{-D_0}(\cdot)$ is the corresponding Kronecker character, and $\sigma_1(n)$ is the sum of positive divisors of n. As a result, a lower bound for $H(-D)$ (resp. $H(-D_E(t))$) leads to a lower bound for the class number of the corresponding imaginary quadratic field.

Remark. *A classical theorem of Hooley (see Ch. IV of [13]) gives asymptotic formulas for the number of square-free values of irreducible cubic polynomials $f(t) \in \mathbb{Z}[t]$. Namely, it is generally the case (i.e. barring trivial obstructions arising from congruence conditions) that a positive proportion of the values of f at integer arguments are square-free. Using this fact we can quantify the frequency with which Theorem 1.2 improves on (1.1) for large $-D_E(t)$ (i.e. $t \to +\infty$) when $r(E) \geq 3$. A famous example of Elkies [5] has $r(E) \geq 28$, and so we obtain the effective lower bound*

$$h(-D) \gg_\varepsilon (\log D)^{14-\varepsilon}$$

which holds for $\gg_\varepsilon X^{\frac{1}{3}}$ many explicit fundamental discriminants $-X < -D < 0$.

Example. *For $E: \ y^2 = x^3 - 16x + 1$, we have*[3] *$|E_{\mathrm{tor}}(\mathbb{Q})| = 1$, $r(E) = 3$, and $R_E(\mathbb{Q}) \sim 0.930\ldots$. Therefore, for large fundamental discriminants of the form $-D_E(t) = -4(t^3 - 16t - 1)$, we have*

$$h(-D_E(t)) > \frac{1}{20} \cdot (\log(D_E(t))^{\frac{3}{2}}.$$

We give infinite families of $E/\mathbb{Q}$ using the discriminant $\Delta_{a,b} := -16(27b^4 - 4a^6)$ curves

$$E_{a,b} \ : \ y^2 = x^3 - a^2x + b^2. \tag{1.8}$$

For integers t, we let $D_{a,b}(t) := 4(t^3 - a^2t - b^2)$. For positive integers a, b, we let

$$c^{(2)}_{a,b} := \frac{\Omega_2}{12 \cdot \widehat{h}(P^{(2)}_{\max})} \quad \text{and} \quad c^{(3)}_{a,b^3} := \frac{\Omega_3}{24\sqrt{3} \cdot \widehat{h}(P^{(3)}_{\max})^{\frac{3}{2}}}, \tag{1.9}$$

where $P^{(2)}_{\max} \in \{(0,b),(-a,b)\} \subset E_{a,b}(\mathbb{Q})$ and $P^{(3)}_{\max} \in \{(0,b^3),(-a,b^3),(-b^2,ab)\} \subset E_{a,b^3}(\mathbb{Q})$ are chosen to have the largest canonical height.

Theorem 1.3. *If a and b are positive integers, then the following are true:*

(1) If $a \gg_b 1$ (resp. $b \gg_a 1$), then $r(E_{a,b}(\mathbb{Q})) \geq 2$. Moreover, if $\varepsilon > 0$, then for sufficiently large fundamental discriminants $-D_{a,b}(t) < 0$ in absolute value we have

$$h(-D_{a,b}(t)) \geq (c^{(2)}_{a,b} - \varepsilon) \cdot \log(D_{a,b}(t)).$$

(2) If $a \gg_b 1$ (resp. $b \gg_a 1$), then $r(E_{a,b^3}(\mathbb{Q})) \geq 3$. Moreover, if $\varepsilon > 0$, then for sufficiently large fundamental discriminants $-D_{a,b^3}(t) < 0$ in absolute value we have

$$h(-D_{a,b^3}(t)) \geq (c^{(3)}_{a,b^3} - \varepsilon) \cdot \log(D_{a,b^3}(t))^{\frac{3}{2}}.$$

[3] These calculations were performed using `SageMath`.

Three Remarks.
(1) Theorem 1.3 is effective. One can make explicit[4] $b \gg_a 1$ and $a \gg_b 1$. Moreover, we note that $-D_{n+1,n}(-1) = -8n$ covering all $-D \equiv 0 \pmod 8$. Using (1.7) and the remark after Theorem 1.2, we find that these curves cover all negative discriminants.

(2) Theorem 1.3 (1) often improves on (1.1) (e.g. for large $t \in \mathbb{Z}^+$ when a and b are small, or when $-D_{a,b}(t)$ is suitably composite).

(3) Theorem 1.3 (2) often provides a $\log D$ power improvement to (1.1). Florian Luca has noted, for each $0 < c < 1/2$, that the effective lower bound

$$h(-D) \gg_c \log(D)^{\frac{3}{2}-c}$$

holds for $\gg X^{\frac{1}{3}} \cdot \exp\left(\frac{4}{3}\log(X)^{\frac{c}{3}}\right)$ many explicit $-X < -D < 0$. The idea is that integers of the form $N = t^3 - a^2t - b^2$ have unique representations with $t \in [X/2, X]$, $a \in [y/2, y]$, and $b \in [z/2, z]$, where $y = o(X^{\frac{1}{3}})$ and $z = o(X^{\frac{1}{6}})$, and one then lets $y = z = \exp\left(\log(X)^{\frac{c}{3}}\right)$ and counts cubes b.

This note is organized as follows. In Section 2 we prove Theorem 2.1, a result which provides the ideal class pairings, and determines conditions guaranteeing $\mathrm{SL}_2(\mathbb{Z})$-inequivalence. Using this result, the proof of Theorem 1.2 is reduced to effectively counting rational points with bounded height, which we address in Section 3. In Section 4 we state and prove Theorem 4.1, a result which implies Theorem 1.2. Theorem 1.1 follows the proof of Theorem 4.1 *mutatis mutandis*. Finally, in Section 5 we prove Theorem 1.3.

Acknowledgements

The second author thanks the NSF (DMS-1601306) and the Thomas Jefferson fund at the U. Virginia. The authors thank the referee, N. Elkies, D. Goldfeld, B. Gross, F. Luca, K. Soundararajan, D. Sutherland and J. Thorner for useful comments concerning this paper.

2. Elliptic curves Ideal class pairings

Works by Buell, Call, and Soleng [2, 3, 20] offered elliptic curve ideal class pairings, which produce discriminant $-D$ integral positive definite binary quadratic forms from points on $E(\mathbb{Q})$ and $E_{-D}(\mathbb{Q})$. We offer a generalization and minor correction of Theorem 4.1 of [20].[5]

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[6]. Moreover, suppose that $v \neq 0$, with v even if $-D$ is odd. If we let $\alpha := |Aw^2 - uC^2|$ and $G := \gcd(\alpha, C^6v^2)$, then we shall show that there are integers ℓ for which $F_{P,Q}(X, Y)$ defined below is a discriminant $-D$ positive definite integral binary quadratic form.

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

[4]For example, Fujita and Nara [6] show for $b = 1$ that $a \geq 4$ suffices in Theorem 1.3 (2).

[5]This corrects sign errors in the discriminants in Theorem 4.1 of [20], and also ensures the resulting quadratic forms are integral when $C \neq 1$. Moreover, this theorem allows for both even and odd discriminants.

[6]Thanks to (1.3), every Q has such a representation where $\gcd(u, w^2)$ and $\gcd(v, w^3)$ divide D.

Theorem 2.1. *Assuming the notation and hypotheses above, $F_{P,Q}(X,Y)$ is well defined (e.g. there is such an ℓ) in $\mathrm{CL}(-D)$. 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 $\mathrm{SL}_2(\mathbb{Z})$-equivalent, then $\frac{\alpha_1}{G_1}=\frac{\alpha_2}{G_2}$ or $\frac{\alpha_1\alpha_2}{G_1G_2}>D/4$.*

Example. *For $E: y^2=x^3-4x+9$, we have points $P_1:=(0,3)$ and $P_2:=(-2,3)$. Using $Q:=(-3,1)\in E_{-24}(\mathbb{Q})$ and $\ell=2$, we obtain the inequivalent discriminant -24 forms $F_{P_1,Q}(X,Y)=3X^2+12XY+14Y^2$ and $F_{P_2,Q}(X,Y)=X^2+8XY+22Y^2$. It turns out $h(-24)=2$.*

Proof. A calculation shows that $F_{P,Q}(X,Y)$ has discriminant $-D$. We now show that there are integers ℓ for which $F_{P,Q}(X,Y)$ is integral, and that all such choices preserve $\mathrm{SL}_2(\mathbb{Z})$-equivalence. To this end, let $f(x):=x^3+a_4x+a_6$, so that $B^2=C^6f\left(\frac{A}{C^2}\right)$ and $-v^2D=4w^6f\left(\frac{u}{w^2}\right)$. Note that $\alpha=\left|w^2C^2\left(\frac{A}{C^2}-\frac{u}{w^2}\right)\right|$, which divides

$$w^6B^2+C^6v^2\tfrac{D}{4} \;=\; w^6C^6\left(f\left(\frac{A}{C^2}\right)-f\left(\frac{u}{w^2}\right)\right). \tag{2.2}$$

Since $G=\gcd(\alpha,C^6v^2)$, we have that $G\mid 4w^6B^2$. Let $H:=\gcd(2w^3B,C^3v)$. Then $G\mid H^2$, and so C^3v/H, which divides C^6v^2/G, is relatively prime to α/G. Choose $k\in\mathbb{Z}$ so that

$$\frac{\alpha k}{G}\equiv-\frac{2w^3B}{H}-\frac{C^3vD}{H} \pmod{\tfrac{2C^3v}{H}}.$$

If α/G is odd, k can be found by inverting $\alpha/G \pmod{\frac{2C^3v}{H}}$. If α/G is even, then $-C^3vD\equiv 2w^3B \pmod 2$, and so k may be found by inverting $\alpha/2G \pmod{\frac{C^3v}{H}}$. We take $\ell\equiv Hk \pmod{2C^3v}$ or $\pmod{C^3v}$ depending on whether k is defined $\pmod{\frac{2C^3v}{H}}$ or $\pmod{\frac{C^3v}{H}}$ respectively. The conditions on ℓ imply that the coefficient of XY in $F_{P,Q}(X,Y)$ has the same parity as $-D$. The numerator of the Y^2 term, $(2w^3B+\ell\alpha/G)^2+C^6v^2D$, is divisible by $4C^6v^2$. By (2.2), it is also divisible by 4α. Therefore, it is divisible by $4C^6v^2\alpha/G$, and so $F_{P,Q}(X,Y)$ is integral.

We now determine the inequivalence of $F_{P_1,Q_1}(X,Y)$ and $F_{P_2,Q_2}(X,Y)$. For $i=1$ and 2 we let A_i,B_i,C_i,α_i, and G_i be the corresponding quantities for these two pairs of points. Note that

$$F_{P_1,Q_1}(X,Y)=\frac{G_1}{\alpha_1}\left[\left(\frac{\alpha_1}{G_1}X+\frac{2w^3B_1+\ell\cdot\frac{\alpha}{G}}{2C_1^3v}Y\right)^2+\frac{D}{4}Y^2\right].$$

Since ℓ was chosen so that $\ell\cdot\frac{\alpha}{G}$ is defined modulo $2C^3v$, its choice does not affect $\mathrm{SL}_2(\mathbb{Z})$-equivalence. If $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\mathrm{SL}_2(\mathbb{Z})$ and $F_{P_2,Q_2}(X,Y)=F_{P_1,Q_1}(aX+bY,cX+dY)$, then the leading terms satisfy

$$\frac{\alpha_2}{G_2}=\frac{G_1}{\alpha_1}\left[\left(\frac{\alpha_1a}{G_1}+\frac{2w^3B_1+\ell\cdot\frac{\alpha}{G}}{2C_1^3v}c\right)^2+\frac{D}{4}c^2\right].$$

If $c=0$, then $a^2=1$, and the equation reduces to $\frac{\alpha_2}{G_2}=\frac{\alpha_1}{G_1}$. If $c\neq 0$, both terms inside the square brackets are positive, and together are at least $D/4$, so $\frac{\alpha_2}{G_2}\geq\frac{G_1}{\alpha_1}D/4$. □

3. Heights on elliptic curves

To deduce Theorem 1.2 from Theorem 2.1, we use estimates for the number of rational points on elliptic curves with bounded height. Here 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 $H(P) = H(x) := \max(|A|, |C^2|)$. The logarithmic height (or Weil height) is $h_W(P) = h_W(x) := \log H(P)$, and the canonical height is given by

$$\widehat{h}(P) = \tfrac{1}{2} \lim_{n\to\infty} \frac{h_W(nP)}{n^2}. \tag{3.1}$$

Logarithmic and canonical heights are generally close. A theorem of Silverman [19] bounds the differences between these heights in terms of the logarithmic heights of $j(E)$ and $\Delta(E)$.

Theorem 3.1 (Theorem 1.1 of [19]). *If $P \in E(\mathbb{Q})$, then*

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

Asymptotics for the number of rational points on an elliptic curve with bounded height are well known (for example, see [14, Prop 4.18]). If $E(\mathbb{Q})$ has rank $r \ge 1$ 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 $|E_{\rm tor}(\mathbb{Q})|$, we have

$$\#\{P \in E(\mathbb{Q}) \mid \widehat{h}(P) \le T\} \sim \frac{|E_{\rm tor}(\mathbb{Q})|}{\sqrt{R_{\mathbb{Q}}(E)}} \cdot \Omega_r T^{\frac{r}{2}} = c(E) T^{\frac{r}{2}}. \tag{3.2}$$

Using an argument of Landau which estimates the number of lattice points in r-dimensional spheres (for example, see [15]), one can show that the error term in the asymptotic is $\mathrm{O}(T^{\frac{r}{2}-1+\frac{1}{r+1}})$.

To prove Theorem 1.2, we require effective lower bounds for the number of points with bounded height. To this end, if $\{P_1, \dots, P_r\}$ is a basis of $E(\mathbb{Q})/E_{\rm tor}(\mathbb{Q})$, then its diameter is

$$d(E) = \max_{\delta_i \in \{\pm 1, 0\}} 2\widehat{h}\left(\sum_{i=1}^{r} \delta_i P_i\right). \tag{3.3}$$

It is the largest square-distance between any two vertices of the parallelopiped in $\mathbb{R}^r$ constructed from vectors $\mathbf{v}_1, \dots \mathbf{v}_r$ which have $\mathbf{v}_i \cdot \mathbf{v}_j = \langle P_i, P_j\rangle := \frac{1}{2}\left(\widehat{h}(P_i + P_j) - \widehat{h}(P_i) - \widehat{h}(P_j)\right)$.

Proposition 3.2. *Assume the notation and hypotheses above. If $d = d(E)$ is the diameter of any basis of $E(\mathbb{Q})/E_{\rm tor}(\mathbb{Q})$, then for $T > d(E)/4$ we have*

$$\#\{P \in E(\mathbb{Q}) \mid \widehat{h}(P) \le T\} \ge c(E)\left(T^{\frac{r}{2}} - r\sqrt{d}\cdot T^{\frac{r-1}{2}}\right).$$

Proof. Let $\mathcal{B} = \{P_1, \dots, P_r\}$ be any basis for $E(\mathbb{Q})$. We must count points on the lattice $\Lambda \in \mathbb{R}^r$, generated by $v_1, v_2, \dots, v_r$ for which $v_i \cdot v_j = \langle P_i, P_j\rangle$. The number of points in the subgroup of $E(\mathbb{Q})$ generated by $\mathcal{B}$ with canonical height bounded by T is the number of points in $\Lambda \cap B(T^{\frac{1}{2}})$, where $B(R)$ is the closed ball in $\mathbb{R}^r$ centered at the origin of radius R.

For each point $\lambda \in \Lambda$, let P_λ be the half-open parallelepiped given by

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

If P_λ intersects $B(T^{\frac{1}{2}} - d^{\frac{1}{2}})$, then $\lambda \in B(T^{\frac{1}{2}})$. Therefore, we have

$$\begin{aligned}\#\left(\Lambda \cap B(T^{\frac{1}{2}})\right) &\ge \frac{\mathrm{Vol}\left(B(T^{\frac{1}{2}} - d^{\frac{1}{2}})\right)}{\mathrm{Vol}(\mathcal{P}_\lambda)} = \frac{\Omega_r}{\mathrm{Vol}(\mathcal{P}_\lambda)} \cdot \left(T^{\frac{1}{2}} - d^{\frac{1}{2}}\right)^r \\ &\ge \frac{\Omega_r}{\mathrm{Vol}(\mathcal{P}_\lambda)} \cdot \left(T^{\frac{r}{2}} - r\sqrt{d}\cdot T^{\frac{r-1}{2}}\right).\end{aligned}$$

In the last inequality we used the binomial expansion and the fact that $T \geq d/4$. Since we have $R_{\mathbb{Q}}(E) := |\det(\langle P_i, P_j\rangle)_{1\leq i,j\leq r}|$, it follows that $\mathrm{Vol}(\mathcal{P}_\lambda) = \sqrt{R_E(\mathbb{Q})}$. To complete the proof, we note that torsion points have height zero, and so we may multiply the last estimate by $|E_{\mathrm{tor}}(\mathbb{Q})|$. □

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 $E(\mathbb{Q})$.

Proposition 3.3. *Assume the notation and hypotheses above. Suppose G is a subgroup of $E_{\mathrm{tor}}(\mathbb{Q})$, 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 $T > d(\mathcal{B})/4$, then*

$$\#\{P \in E(\mathbb{Q}) \mid \widehat{h}(P) \leq T\} \geq \frac{|G|}{\sqrt{\widehat{h}(P_m)^m}} \cdot \Omega_m \left(T^{\frac{m}{2}} - m^2 \sqrt{2\widehat{h}(P_m)} T^{\frac{m-1}{2}} \right).$$

Proof. The proof of Proposition 3.2 works with two modifications. Note that $d(\mathcal{B}) \leq 2m^2 \widehat{h}(P_m)$, and that the volume of the parallelopiped for $\mathcal{B}$ satisfies $\mathrm{Vol}(\mathcal{B}) \leq \prod_{i=1}^m \widehat{h}(P_i)^{1/2} \leq \widehat{h}(P_r)^{\frac{m}{2}}$. □

4. Proof of Theorems 1.1 and 1.2

Theorems 1.1 and 1.2 are proven in the same way. For simplicity, we first consider Theorem 1.2, which pertains to fundamental discriminants $-D_E(t) = -4(t^3 + a_4 t - a_6)$, and where we have chosen to pair the points in $E(\mathbb{Q})$ with $Q_t := (-t, 1) \in E_{-D_E(t)}(\mathbb{Q})$. We obtain the precise Theorem 4.1, which in turn implies Theorem 1.2.

We show that points $P \in E(\mathbb{Q})$ with canonical height $\widehat{h}(P) \leq T_E(t)$, where

$$T_E(t) := \frac{1}{4} \log \left(\frac{D_E(t)}{(t+1)^2} \right) - \delta(E), \tag{4.1}$$

map to inequivalent forms $F_{P,Q_t}(X, Y) \in \mathrm{CL}(-D)$.

Theorem 4.1. *Assume the hypotheses above. If $T_E(t) \geq d(E)/4$ and $-D_E(t)$ is a negative fundamental discriminant for which $(t+1)^2 \exp(4\delta(E) + d(E)) \leq D_E(t) \leq t^2(t+1)^2$, then*

$$h(-D_E(t)) \geq \frac{c(E)}{2} \left(T_E(t)^{\frac{r}{2}} - r\sqrt{d(E)} T_E(t)^{\frac{r-1}{2}} \right).$$

Remark. *Since $D_E(t)$ is cubic, the conclusion holds for all but finitely many $-D_E(t)$. Moreover, the proof works for any m independent points in $E(\mathbb{Q})$ thanks to Proposition 3.3.*

Deduction of Theorem 1.2 from Theorem 4.1. Due to the $(t+1)^2$ in (4.1), we have $T_E(t) \sim \log(D_E(t))/12$, and the result follows. □

Proof of Theorem 4.1. We suppose that $t \in \mathbb{Z}^+$ satisfies $(t+1)^2 \exp(4\delta(E) + d(E)) \leq D_E(t) \leq t^2(t+1)^2$. Proposition 3.2 implies that

$$\#\{P \in E(\mathbb{Q}) \mid \widehat{h}(P) \leq T_E(t)\} \geq \frac{|E_{\mathrm{tor}}(\mathbb{Q})|}{\sqrt{R_{\mathbb{Q}}(E)}} \cdot \Omega_r \left(T_E(t)^{\frac{r}{2}} - r\sqrt{d(E)} T_E(t)^{\frac{r-1}{2}} \right). \tag{4.2}$$

We show that these points map to inequivalent forms when paired with $Q_t = (-t, 1) \in E_{-D_E(t)}(\mathbb{Q})$.

Suppose that $P_1 = (\frac{A_1}{C_1^2}, \frac{B_1}{C_1^3}), P_2 = (\frac{A_2}{C_2^2}, \frac{B_2}{C_2^3}) \in E(\mathbb{Q})$ satisfy $\widehat{h}(P_i) \le T_E(t)$, and let $F_1 := F_{P_1,Q_t}(X,Y)$ and $F_2 := F_{P_2,Q_t}(X,Y)$. Since $\gcd(A_i, C_i) = 1$, their leading terms are $\frac{\alpha_i}{G_i} = \alpha_i = |A_i + tC_i^2|$. Thanks to Theorem 3.1, we have that

$$h_W(P_i) \le 2\left(\widehat{h}(P_i) + \tfrac{1}{8}h_W(j(E)) + \tfrac{1}{12}h_W(\Delta(E)) + 0.973\right) \le 2T_E(t) - \log(2) = \tfrac{1}{2}\log\left|\frac{D_E(t)}{4(t+1)^2}\right|.$$

We observe that $\alpha_i \le (t+1)H(P_i)$. By Theorem 3.1, we have $H(P_i) = \exp(h_W(P_i)) \le \frac{\sqrt{D_E(t)}}{2(t+1)}$, which gives $\alpha_i \le \frac{1}{2}\sqrt{D_E(t)}$. Hence, we find that $\alpha_1\alpha_2 \le \frac{1}{4}D_E(t)$, and so by Theorem 2.1, F_1 and F_2 are inequivalent unless $\alpha_1 = |A_1 + tC_1^2| = |A_2 + tC_2^2| = \alpha_2$. However, by hypothesis $D_E(t) \le t^2(t+1)^2$, and so $|A_i| \le H(P_i) \le \frac{t}{2}$. Since $C_i^2 > 0$, this means $\alpha_i = |A_i + tC_i^2| = A_i + tC_i^2$. If $\alpha_1 = \alpha_2$, then $A_1 \equiv A_2 \pmod{t}$, and by the bounds on $|A_i|$ we have that $A_1 = A_2$. This then implies that $C_1^2 = C_2^2$, and so $P_1 = \pm P_2$, which explains the further factor of $1/2$ that appears in the lower bound. This completes the proof. □

Proof of Theorem 1.1. We follow the proof of Theorem 4.1, noting instead that $Q_D = (u, v) \in E_{-D}(\mathbb{Q})$, with $u, v \in \mathbb{Z}$, where $v \neq 0$, and v is even if $-D$ is odd. Arguing as before, we find that F_1 and F_2 are inequivalent unless $\frac{\alpha_1}{G_1} = \frac{|A_1 - uC_1^2|}{G_1} = \frac{|A_2 - uC_2^2|}{G_2} = \frac{\alpha_2}{G_2}$, and that $|A_i| \le H(P_i) \le \frac{|u|}{2v^2} \le \frac{1}{2}|u|$. Since $C_i^2 > 0$, this implies that $A_1 - uC_1^2$ and $A_2 - uC_2^2$ have the same signs. If $\frac{\alpha_1}{G_1} = \frac{\alpha_2}{G_2}$, then

$$A_1G_2 - A_2G_1 = u(C_1^2G_2 - C_2^2G_1).$$

The left hand side is divisible by, but not exceeding, $|u|$; and so it must be 0. This implies $\frac{A_1}{G_1} = \frac{A_2}{G_2}$, and $\frac{C_1^2}{G_1} = \frac{C_2^2}{G_2}$, and so $\frac{A_1}{C_1^2} = \frac{A^2}{C_2^2}$. Hence, we have $P_1 = \pm P_2$, which explains the further factor of $1/2$ that appears in the lower bound. This completes the proof.

□

5. A nice family of elliptic curves

Theorem 1.3 is a simple consequence of the following proposition.

Proposition 5.1. *If a and b are positive integers, then the following are true:*

1. *If $a \gg_b 1$ (resp. $b \gg_a 1$), then $(0, b)$ and $(-a, b)$ are independent points in $E_{a,b}(\mathbb{Q})$.*
2. *If $a \gg_b 1$ (resp. $b \gg_a 1$), then $(0, b^3)$, $(-a, b^3)$, and $(-b^2, ab)$ are independent points in $E_{a,b^3}(\mathbb{Q})$.*

Proof. This follows easily from Silverman's specialization theorem for elliptic curves. Suppose that $E_t/\mathbb{Q}(t)$ is an elliptic curve which is not isomorphic over $\mathbb{Q}(t)$ to an elliptic curve defined over $\mathbb{Q}$. For $w \in \mathbb{Q}$, we let σ_w be the specialization map $(t \to w)$:

$$\sigma_w \,:\, E_t(\mathbb{Q}_t) \to E_w(\mathbb{Q}).$$

Generally, E_w is an elliptic curve over $\mathbb{Q}$. Silverman's theorem (see Th. C of [18]) states, for all but finitely many $w \in \mathbb{Q}$, that σ_w is an injective homomorphism between elliptic curves. The claims follows immediately by viewing a and b as indeterminates respectively.

□

Proof of Theorem 1.3. In view of Proposition 5.1 and Proposition 3.3, the proof follows the proof of Theorem 4.1 *mutatis mutandis*. □

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] H. Cohen, *Sums involving the values at negative integers of L-functions of quadratic characters*, Math. Ann. **217** (1975), 271-285.
[5] N. Elkies, History of elliptic curves ranks records (website: https://web.math.pmf.unizg.hr/ duje/tors/rk28.html).
[6] Y. Fujita and T. Nara, *The Mordell-Weil bases for the elliptic curve of the form* $y^2 = x^3 - m^2x + n^2$, Publ. Math. Debrecen **92** (2018), 79-99.
[7] 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.
[8] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Springer Lect. Notes **751** (1979), 108-118.
[9] D. Goldfeld, *Gauss' class number problem for imaginary quadratic fields*, Bull. Amer. Math. Soc. **13**, (1985), 23-37.
[10] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), 225-320.
[11] K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z., **56** (3) (1952), 227–253.
[12] H. Heilbronn, *On the class-number in imaginary quadratic fields*, Quart. J. Math. Oxford Ser. **5** (1934), 150–160.
[13] C. Hooley, *Applications of sieve methods to the theory of numbers*, Cambridge Univ. Press, Cambridge 1976.
[14] A. Knapp, *Elliptic curves*, Princeton Univ. Press, 1992.
[15] E. Landau, *Zur analytischen Zahlentheorie der definiten quadratischen Formen (Uber die Gitterpunkte in einem mehrdimensionalen Ellipsoid)*, Sitzber. Preuss. Akad. Wiss. **31**, (1915), 458–476.
[16] J. Oesterlé, *Nombres de classes des corps quadratiques imaginaires*, Sem. Bourbaki **1983/1984**, No. 121-122 (1985), 309-323.
[17] C. L. Siegel, *Über die Classenzahl quadratischer Zahlkörper*, Acta Arith. **1** (1935), 83–86.
[18] J. H. Silverman, *Heights and the specialization map for families of abelian varieties*, J. Reine Angew. Math. **342** (1983), 197-211.
[19] J. H. Silverman, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. **55** (1990), 723-743.
[20] 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.
[21] H. M. Stark, *A complete determination of the complex quadratic fields of class number one*, Michigan Math. J. **14** (1967), 1–27.
[22] M. Watkins, *Class numbers of imaginary quadratic fields*, Math. of Comp. **73** (2004), 907–938.

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

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