ALMOST ALL QUADRATIC TWISTS OF AN ELLIPTIC CURVE HAVE NO INTEGRAL POINTS

TIM BROWNING AND STEPHANIE CHAN

ABSTRACT. For a given elliptic curve E in short Weierstrass form, we show that almost all quadratic twists E_D have no integral points, as D ranges over square-free integers ordered by size. Our result is conditional on a weak form of the Hall–Lang conjecture in the case that E has partial 2-torsion. The proof uses a correspondence of Mordell and the reduction theory of binary quartic forms in order to transfer the problem to counting rational points of bounded height on a certain singular cubic surface, together with extensive use of cancellation in character sum estimates, drawn from Heath-Brown's analysis of Selmer group statistics for the congruent number curve.

CONTENTS

| 1. | Introduction | 1 |
|------------|--|----|
| 2. | Main results and moments | 4 |
| 3. | Counting points on a cubic surface | 6 |
| 4. | Integral points on quadratic twists with large $gcd(x, D)$ | 10 |
| 5. | Integral points on quadratic twists with small $gcd(x, D)$ | 11 |
| 6. | Character sum input | 17 |
| 7. | Quadratic twists with full two-torsion | 23 |
| 8. | Quadratic twists with partial two-torsion | 31 |
| References | | 37 |

1. Introduction

Given an elliptic curve defined over \mathbb{Z} , the aim of this paper is to establish the paucity of quadratic twists that contain integral points. Fixing A and B such that $4A^3 + 27B^2 \neq 0$, let E denote the elliptic curve $y^2 = x^3 + Ax + B$. We shall consider the quadratic twist family

$$E_D: y^2 = x^3 + AD^2x + BD^3, (1.1)$$

as D runs over square-free integers. Let $\mathcal{D} := \{D \in \mathbb{Z} \text{ square-free}\}$ and let

$$\mathcal{D}(N) := \{ D \in \mathcal{D} : |D| \leqslant N \},\$$

for any $N \ge 1$. Denote the set of integral points on E_D by

$$E_D(\mathbb{Z}) := \{(x, y) \in \mathbb{Z}^2 : y^2 = x^3 + AD^2x + BD^3\}.$$

If E has a rational 2-torsion point and α is an integer root of the polynomial $x^3 + Ax + B$, then every twist E_D has an integral point $(\alpha D, 0)$. Accordingly, we define

$$E_D^*(\mathbb{Z}) := E_D(\mathbb{Z}) \setminus E_D[2], \tag{1.2}$$

where $E_D[2]$ is the 2-torsion subgroup of $E_D(\mathbb{Q})$. Granville [13] has conjectured asymptotics for the density of elliptic curves that have a non-trivial integral point in a quadratic

Date: January 10, 2024.

²⁰¹⁰ Mathematics Subject Classification. 11D45 (11D25, 11G05).

twist family. (However, care should be taken when comparing the conjecture against our setting, since he considers the model $Dy^2 = x^3 + Ax + B$, which contains fewer integral points than E_D .) In our setting, we expect that

$$\#\{D \in \mathcal{D}(N) : E_D^*(\mathbb{Z}) \neq \varnothing\} \sim c_{A,B}N^{\frac{1}{2}},$$

as $N \to \infty$, for some constant $c_{A,B} > 0$ depending only on A and B. Our main goal is to show that the left hand side is o(N). Chan [7] has achieved this for the quadratic twist family of congruent number curves $y^2 = x^3 - D^2x$. Moreover, for a fixed square-free integer $k \neq 1$, Chan [8] has also proved that almost all elliptic curves in the cubic twist family of Mordell curves $y^2 = x^3 + kD^2$ have no integral point.

In the setting of quadratic twists of an arbitrary elliptic curve $y^2 = x^3 + Ax + B$, we shall need to work under the following hypothesis when the curve has partial 2-torsion.

Conjecture 1.1 (weak Hall–Lang). Let E be the elliptic curve $y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{Z}$ are such that $4A^3 + 27B^2 \neq 0$, and let $(x, y) \in E(\mathbb{Z})$. Then there exists constants $C, \varepsilon > 0$ such that $|x| \leq \exp\left(C \max\{|A|^{\frac{1}{2}}, |B|^{\frac{1}{3}}\}^{1-\varepsilon}\right)$.

The Hall-Lang conjecture is recorded by Lang [22] and predicts that a polynomial bound should hold. Thus the conjecture states that there exist constants $C, \kappa > 0$ such that

$$|x| < C \max\{|A|, |B|\}^{\kappa}.$$

Note that the analogue of this conjecture over $\mathbb{F}_q(t)$ is known, thanks to Schmidt [25]. Over \mathbb{Q} , on the other hand, we only have the exponential bound

$$|x| \leqslant \exp\left(C_{\varepsilon} \max\{|A|^{\frac{1}{2}}, |B|^{\frac{1}{3}}\}^{6+\varepsilon}\right),$$

for any $\varepsilon > 0$, which follows from work of Hajdu and Herendi [14].

We are now ready to reveal our main result.

Theorem 1.2. Let $\varepsilon > 0$. Let $A, B \in \mathbb{Z}$ such that $4A^3 + 27B^2 \neq 0$, and let E_D be given by (1.1). Assume that Conjecture 1.1 holds. Then

$$N^{\frac{1}{2}} \ll \#\{D \in \mathcal{D}(N) : E_D^*(\mathbb{Z}) \neq \varnothing\} \ll \frac{N}{(\log N)^{\frac{1}{8}-\varepsilon}},$$

where the implied constants depend at most on A, B and ε . Moreover, Conjecture 1.1 is only required in the proof of the upper bound, and only then when $x^3 + Ax + B$ has precisely one root over \mathbb{Q} .

When the underlying curve E_1 does not have rational two torsion, so that $E_D[2] = \emptyset$, not only is our work completely unconditional, but the upper bound holds with $\frac{1}{3}$ instead of $\frac{1}{8}$. A detailed summary of our results is presented in Section 2, which we shall build on to address moments of $\#E_D^*(\mathbb{Z})$. For comparison, for the full family of elliptic curves, Alpöge [1] has shown that the average number of integral points on elliptic curves ordered by height is bounded (by at most 66). More recently, Alpöge and Ho [2] have shown that the second moment is also bounded in the family of all elliptic curves. Restricting to the setting of quadratic twist families, we will apply recent work of Smith [28] to assess higher moments of $\#E_D(\mathbb{Z})$ in the case that $E_D[2] = \emptyset$.

Theorem 1.3. Let $A, B \in \mathbb{Z}$ such that $x^3 + Ax + B$ is irreducible over \mathbb{Q} . Then, for any positive integer $k \leq \log \log \log N$, we have

$$\frac{1}{\# \mathcal{D}(N)} \sum_{D \in \mathcal{D}(N)} \# E_D(\mathbb{Z})^k \ll \frac{1}{(\log N)^{\frac{1}{4}}},$$

where the implied constant depends at most on A and B.

Let us proceed by summarising our approach to Theorem 1.2. Our argument differs according to the size of $gcd(x_P, D) = g_P$, say, where $P = (x_P, y_P) \in E_D(\mathbb{Z})$. When g_P is large we shall reduce to a question about the solubility of $x^3 + Ax + B$ modulo g_P . When $x^3 + Ax + B$ is irreducible over \mathbb{Q} , the Chebotarev density theorem will allow us to control the density of primes p for which $x^3 + Ax + B$ has a root modulo p. Alternatively, when $x^3 + Ax + B$ is reducible over \mathbb{Q} , we shall reduce to a question about the solubility of a system of equations, for which character sum estimates will prove crucial.

When g_P is small, on the other hand, our approach makes crucial use of a construction by Mordell [24, Chapter 25], which associates a binary quartic form $f_P \in \mathbb{Z}[x_1, x_2]$ to any point $P \in E_D(\mathbb{Z})$. Building on the discriminant-lowering procedure adopted for binary cubic forms in [8], we will use the reduction theory of binary quartic forms, as explained by Cremona [9], in order to lower the discriminant of f_P . This will ultimately allow us to reduce the problem to counting rational points of bounded height on a certain singular cubic surface, which may be of independent interest.

Let $C \in \mathbb{Z}[x_1, x_2]$ be a separable binary cubic form and let $S \subset \mathbb{P}^3$ be the cubic surface

$$C(x_1, x_2) = x_3^2 x_4. (1.3)$$

This is a singular cubic surface containing six lines, and with an isolated singularity (0:0:0:1) of type \mathbf{D}_4 . The Manin conjecture [11] makes a precise prediction for the asymptotic behaviour of the quantity

$$N(U;B) = \# \left\{ x \in U(\mathbb{Q}) : H(x) \leqslant B \right\},\,$$

as $B \to \infty$, where H is standard height function on $\mathbb{P}^3(\mathbb{Q})$ and U is the Zariski open subset formed by deleting the six lines from S. A crude form of the conjecture predicts linear growth, so that $N(U; B) = O_S(B^{1+\varepsilon})$, for any $\varepsilon > 0$.

When the cubic form factorises as $C(x_1, x_2) = x_1 x_2(x_1 + x_2)$, the surface S has been studied by Browning [4], who established that

$$B(\log B)^6 \ll N(U; B) \ll B(\log B)^6.$$

This was later upgraded to an asymptotic formula for N(U; B) by Le Boudec [23]. For Theorem 2.1 we shall need to study S for any separable binary cubic form C. In fact, it will suffice to restrict to the locus of $(x_1 : x_2 : x_3 : x_4) \in S(\mathbb{Q})$ for which $\gcd(x_1, x_2, x_4) = 1$, as follows.

Theorem 1.4. Let $C \in \mathbb{Z}[x_1, x_2]$ be a binary cubic form that is separable over \mathbb{Q} . Let $N^{\circ}(B)$ be the number of $(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4$ with $\gcd(x_1, x_2, x_4) = 1$, $x_3x_4 \neq 0$, and $|x_i| \leq B$, such that (1.3) holds. Then

$$B \ll N^{\circ}(B) \ll B(\log B)^{\max\{\lambda,2\}},$$

where λ is the number of irreducible factors of C over \mathbb{Q} , and the implied constant depends at most on C.

The condition $x_3x_4 \neq 0$ places us on the open set U, so that $N^{\circ}(B) \leq N(U; B)$. The condition $\gcd(x_1, x_2, x_4) = 1$ corresponds to counting integral points on $S \setminus D$, with codimension 2 boundary divisor (0:0:1:0). This counting problem admits an interpretation through work of Chambert-Loir and Tschinkel [6].

Our method of proof is based on viewing the equation (1.3) as a congruence modulo x_3^2 and relies crucially on the particular coprimality condition that is assumed of the solutions. When C is irreducible we have N(S;B) = N(U;B) + O(1), since then none of the six lines are defined over \mathbb{Q} , and our work implies that $N(S;B) \gg B$. In this case it would be interesting to have a proof of the corresponding upper bound $N(S;B) \ll B$.

Acknowledgements. The authors are grateful to Roger Heath-Brown for useful comments. The first author was supported by FWF grant P 32428-N35.

2. Main results and moments

Let $A, B \in \mathbb{Z}$ such that $4A^3 + 27B^2 \neq 0$, and let E_D be given by (1.1). We recall the definition (1.2) of $E_D^*(\mathbb{Z})$. In this section we summarise our various results, which differ according to the factorisation properties of $x^3 + Ax + B$. The following three results will be deduced in Sections 5.4, 7 and 8, respectively.

Theorem 2.1. Assume that $x^3 + Ax + B$ is irreducible over \mathbb{Q} . Then

$$N^{\frac{1}{2}} \ll \#\{D \in \mathcal{D}(N) : E_D(\mathbb{Z}) \neq \varnothing\} \ll N(\log N)^{-\frac{1}{3}} \log \log N,$$

where the implied constants depend at most on A and B.

Theorem 2.2. Let $\varepsilon > 0$. Assume that $x^3 + Ax + B$ has three distinct roots over \mathbb{Q} . Then

$$N^{\frac{1}{2}} \ll \#\{D \in \mathcal{D}(N) : E_D^*(\mathbb{Z}) \neq \varnothing\} \ll N(\log N)^{-\frac{1}{8} + \varepsilon},$$

where the implied constants depend at most on A, B and ε .

Theorem 2.3. Assume that $x^3 + Ax + B$ factors as (x - r)Q(x), for some $r \in \mathbb{Q}$ and a polynomial Q that is irreducible over \mathbb{Q} . Assume that either Q(r) < 0, or $Q(r) \in \mathbb{Q}^2$, or else that Conjecture 1.1 holds. Then

$$N^{\frac{1}{2}} \ll \# \{ D \in \mathcal{D}(N) : E_D^*(\mathbb{Z}) \neq \emptyset \} \ll N(\log N)^{-\frac{1}{8}} \log \log N,$$

where the implied constants depend at most on A and B.

Assume that Q(r) > 0 and $Q(r) \notin \mathbb{Q}^2$. Then, as we shall see in Section 8, we shall also be able to give an unconditional proof of the upper bound

$$\#\left\{D\in\mathcal{D}(N): \begin{array}{l} x\cdot Q(r)\notin\mathbb{Q}^2 \text{ or } \gcd(x,D)< N(\log N)^{-\frac{49}{4}} \\ \text{for some } (x,y)\in E_D(\mathbb{Z}) \end{array}\right\}\ll N(\log N)^{-\frac{1}{8}}\log\log N,$$

where the implied constant depends at most on A and B.

Turning to moments, Theorem 1.3 is a straightforward consequence of the following general statement about moments of $\#E_D^*(\mathbb{Z})$.

Theorem 2.4. Suppose that

$$\#\{D \in \mathcal{D}(N) : E_D^*(\mathbb{Z}) \neq \varnothing\} \ll N(\log N)^{-\kappa},$$

for some $\kappa > 0$, where the implied constant depends at most on A, B and κ . Then for any positive integer $k \leq \log \log \log N$ and any $\varepsilon > 0$, we have

$$\frac{1}{\# \mathcal{D}(N)} \sum_{D \in \mathcal{D}(N)} \# E_D^*(\mathbb{Z})^k \ll (\log N)^{-\kappa + \varepsilon},$$

where the implied constants depend at most on A, B, κ and ε .

We obtain Theorem 1.3 by applying Theorem 2.1 in Theorem 2.4, with $\kappa = \frac{1}{3} - \frac{1}{24}$ and $\varepsilon = \frac{1}{24}$. Theorem 2.4 will be a consequence of Hölder's inequality and the following two results. The first is a special case of recent work by Smith [28, Theorem 1.1].

Theorem 2.5 (Smith). Let A, B be integers such that $4A^3 + 27B^2 \neq 0$, and let E_D be given by (1.1). Then there are real numbers C, C' > 0, depending only on A, B, such that for any m > 0 and N > C satisfying $m < C' \log \log \log N$, we have

$$\frac{1}{\# \mathcal{D}(N)} \sum_{D \in \mathcal{D}(N)} \exp(m \operatorname{rank} E_D(\mathbb{Q})) \leqslant \exp(Cm^2).$$

The second ingredient we require is a straightforward consequence of a result by Hindry and Silverman [20, Theorem 0.7].

Theorem 2.6. Let A, B be integers such that $4A^3 + 27B^2 \neq 0$, and let E_D be given by (1.1) for $D \in \mathcal{D}$. Then there exists an absolute constant c such that

$$#E_D(\mathbb{Z}) \leqslant c^{\omega(\gcd(A,B)) + (1+\operatorname{rank} E_D(\mathbb{Q}))\sigma_{E_D}},$$

where

$$\sigma_{E_D} = \frac{\log|discriminant\ of\ E_D|}{\log|conductor\ of\ E_D|}$$

is the Szpiro ratio of E/\mathbb{Q} .

Proof. If $y^2 = x^3 + AD^2x + BD^3$ gives a quasi-minimal model, so that any $p^4 \mid AD^2$ implies that $p^6 \nmid BD^3$, then the claim is immediate from [20, Theorem 0.7]. Otherwise, the model $y^2 = x^3 + AD^2x + BD^3$ is not quasi-minimal. Since $D \in \mathcal{D}$ is assumed to be square-free, any prime that satisfies both $p^4 \mid AD^2$ and $p^6 \mid BD^3$ must divide A and B. Let S be the set of primes dividing both A and B. Suppose that C is the largest integer satisfying both $C^4 \mid AD^2$ and $C^6 \mid BD^3$, then any prime dividing C must be in S. If $(x,y) \in \mathbb{Z}^2$ satisfies $y^2 = x^3 + AD^2x + BD^3$, then $(\frac{x}{C^2}, \frac{y}{C^3})$ gives an S-integral point on the quasi-minimal model

$$y^2 = x^3 + \frac{AD^2}{C^4}x + \frac{BD^3}{C^6}.$$

Therefore the result follows from [20, Theorem 0.7].

Proof of Theorem 2.4. The discriminant of E_D in (1.1) is $-16(4A^3 + 27B^2)D^6$ and the conductor is divisible by primes dividing the discriminant. Within a quadratic twist family, since $D \in \mathcal{D}$ is a square-free, we deduce that the Szpiro ratio is

$$\sigma_{E_D} \leqslant 6 + \frac{2\log 16|4A^3 + 27B^2|}{\log |D|}.$$

Thus $\sigma = \sup_{D \in \mathcal{D}} {\{\sigma_{E_D}\}} \ll 1$, for an implied constant that only depends on A and B. We shall apply Hölder's inequality with p, q > 1 such that $\frac{1}{p} + \frac{1}{q} = 1$. This yields

$$\sum_{D\in\mathcal{D}(N)} \#E_D^*(\mathbb{Z})^k \leqslant \#\{D\in\mathcal{D}(N): E_D^*(\mathbb{Z})\neq\varnothing\}^{\frac{1}{p}} \left(\sum_{D\in\mathcal{D}(N)} \#E_D(\mathbb{Z})^{qk}\right)^{\frac{1}{q}}.$$

Applying Theorem 2.6 and the assumption of the theorem, it follows that

$$\sum_{D \in \mathcal{D}(N)} \# E_D^*(\mathbb{Z})^k \ll \left(\frac{N}{(\log N)^{\kappa}}\right)^{\frac{1}{p}} c_1^k \left(\sum_{D \in \mathcal{D}(N)} (c^{qk\sigma})^{\operatorname{rank} E_D(\mathbb{Q})}\right)^{\frac{1}{q}},$$

where $c_1 = c^{\omega(\gcd(A,B))+\sigma}$ and the implied constant depends on A and B. We now apply Theorem 2.5 with $m = qk\sigma \log c$. Since $k \leq \log \log \log N$, by assumption, we have $m \ll \log \log \log N$ if we assume that $q \ll 1$. This gives

$$\sum_{D \in \mathcal{D}(N)} \#E_D^*(\mathbb{Z})^k \ll \frac{Nc_1^k c_2^{qk^2}}{(\log N)^{\frac{\kappa}{p}}},$$

where $c_2 = \exp(C(\sigma \log c)^2)$. We now specify the choice of p, q by imposing $q = \frac{1}{\varepsilon}$. Since $k \leq \log \log \log N$, this leads to

$$\sum_{D \in \mathcal{D}(N)} \# E_D^*(\mathbb{Z})^k \ll \frac{N}{(\log N)^{(1-\varepsilon)\kappa}} \cdot \exp\left(C_{\varepsilon}(\log\log\log N)^2\right),\,$$

for a suitable constant C_{ε} depending on A, B and ε . The statement of the theorem easily follows, on redefining ε .

3. Counting points on a cubic surface

3.1. **Preliminaries.** We begin by examining some properties of a binary cubic form C, which we assume to be separable over \mathbb{Q} and such that $C(1,0) \neq 0$. Denote the discriminant of C by $\Delta(C)$. Henceforth we allow all implied constants to depend on the coefficients of C. Since C is separable over \mathbb{Q} , there exist binary linear forms $L_1, L_2, L_3 \in \overline{\mathbb{Q}}[y_1, y_2]$ such that $C = L_1 L_2 L_3$, with no two factors proportional. We have the following simple result.

Lemma 3.1. Assume that $\mathbf{y} = (y_1, y_2) \in \mathbb{Z}^2$ such that $|L_1(\mathbf{y})| \leq |L_2(\mathbf{y})| \leq |L_3(\mathbf{y})|$. Then $L_2(\mathbf{y}) \gg |\mathbf{y}|$ and $L_3(\mathbf{y}) \ll |\mathbf{y}|$.

Proof. The upper bound is trivial. To see the lower bound, on renormalising and possibly interchanging the roles of y_1, y_2 , we may assume without loss of generality that $y_1 = 1$ and $y_2 = t$ for $t \in [-1, 1]$. Let $l_i(t) = L_i(1, t)$ for $1 \le i \le 3$. Thus there exist non-zero $\alpha_i, \beta_i \in \overline{\mathbb{Q}}$ such that

$$l_i(t) = \alpha_i + \beta_i t,$$

with $\alpha_i \beta_j - \alpha_j \beta_i \neq 0$. We wish to prove that $l_2(t) \gg 1$, where the implied constant is allowed to depend on the constants α_i, β_i . We suppose for a contradiction that, for any positive integer n, there exists $t_n \in [-1, 1]$ such that $|l_2(t_n)| < 1/n$. Then it follows that

$$\beta_1 l_2(t_n) = \beta_1 \alpha_2 - \alpha_1 \beta_2 + \beta_2 l_1(t_n).$$

Since $|l_1(t_n)| \leq |l_2(t_n)| < 1/n$, this therefore implies that

$$0 < |\beta_1 \alpha_2 - \alpha_1 \beta_2| \ll \frac{1}{n},$$

which is a contradiction for sufficiently large n.

Our remaining results in this section concern the solubility of C(x,1) and C(1,x) in residue classes. Define a multiplicative function

$$\rho(n) := \#\{x \in \mathbb{Z}/n\mathbb{Z} : C(x,1) \equiv 0 \bmod n\}. \tag{3.1}$$

It follows from Chebotarev density theorem and Burnside's lemma (see for example [26, Proposition 3.10 and Section 3.3.3.5]) that

$$\sum_{p \leqslant N} \frac{\varrho(p)}{p} = \lambda \log \log N + O(1), \tag{3.2}$$

where λ is the number of irreducible factors of C(x,1) over \mathbb{Q} . It follows from Hensel lifting that

$$\varrho(p) = \varrho(p^v)$$
, for any $v \geqslant 1$ and any prime $p \nmid \Delta(C)$. (3.3)

We may also define

$$\varrho'(n) := \#\{x \in \mathbb{Z}/n\mathbb{Z} : C(1, x) \equiv 0 \bmod n\}. \tag{3.4}$$

It follows from work of Huxley [21] that

$$\rho(p^v), \, \rho'(p^v) \leqslant 3p^{\frac{1}{2}v_p(\Delta(C))},$$
(3.5)

for any prime power p^{v} . We proceed by proving the following result.

Lemma 3.2. Let f be any multiplicative function satisfying

$$f(p^{v}) \begin{cases} = \varrho(p^{v}) & \text{if } p \nmid C(1,0)\Delta(C), \\ \in [0, \varrho(p^{v}) + \varrho'(p^{v})] & \text{if } p \mid C(1,0)\Delta(C). \end{cases}$$

Then we have

$$\sum_{n \le N} f(n) \asymp N(\log N)^{\lambda - 1}, \qquad \sum_{n \le N} \frac{f(n)}{n} \asymp (\log N)^{\lambda} \quad and \quad \sum_{n \le N} \frac{f(n)}{n^2} \asymp 1, \qquad (3.6)$$

where the implied constants depend only on C.

Proof. It follows from (3.5) that $f(p^v) \leq 6p^{\frac{1}{2}v_p(\Delta(C))} = O(1)$. Therefore, by [30, Satz 1], we have

$$\sum_{n \leq N} f(n) \approx \frac{N}{\log N} \exp\left(\sum_{p \leq N} \frac{f(p)}{p}\right). \tag{3.7}$$

The value of f(p) is always equal to $\varrho(p)$ unless $p \mid C(1,0)$, so

$$\sum_{p \leqslant N} \frac{f(p)}{p} = \sum_{p \leqslant N} \frac{\varrho(p)}{p} + O\left(\sum_{p \mid C(1,0)\Delta(C)} \frac{\varrho(p) + \varrho'(p)}{p}\right).$$

Since $C(1,0) \neq 0$, we deduce that the sum over $p \mid C(1,0)\Delta(C)$ has only finitely many terms. We now apply the estimate from (3.2), together with the trivial bound $\varrho(p)$, $\varrho'(p) \leq p$ for all $p \mid C(1,0)\Delta(C)$. Thus it follows that

$$\sum_{p \leqslant N} \frac{f(p)}{p} = \lambda \log \log N + O(1). \tag{3.8}$$

The first bound in (3.6) follows from combining (3.7) and (3.8). The second and third bounds in (3.6) can be deduced by partial summation.

3.2. Proof of the upper bound in Theorem 1.4. Recall our convention that all implied constants are allowed to depend on the coefficients of C. We begin by showing that it suffices to assume without loss of generality that $C(1,0) \neq 0$ in the proof. To see this, we first choose $a \in \mathbb{Z}$, with a = O(1), such that $C(1,a) \neq 0$. But then, on making the change of variables $(x_1, x_2) \mapsto (x_1, x_2 + ax_1)$, we obtain a new counting problem, in which B is replaced by $2 \max\{1, |a|\}B \ll B$ and the relevant binary cubic form has non-zero leading coefficient.

Consider a solution $(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4$ to (1.3). Write $h_1^2 h_2 = \gcd(x_1, x_2)$, where h_1, h_2 are positive integers and h_2 is square-free. The assumption that $\gcd(x_1, x_2, x_4) = 1$ implies that $(h_1^2 h_2)^3 \mid x_3^2$, so $h_1^3 h_2^2 \mid x_3$. Define

$$y_1 = \frac{x_1}{h_1^2 h_2}, \qquad y_2 = \frac{x_2}{h_1^2 h_2}, \qquad u = \frac{x_3}{h_1^3 h_2^2}, \qquad v = x_4.$$

Then (1.3) can be rewritten as

$$C(y_1, y_2) = h_2 u^2 v. (3.9)$$

First fix h_1, h_2 and define the quantity

$$N(Y, U, V) := \# \left\{ (y_1, y_2, u, v) \in \mathbb{Z}^4 : \begin{array}{l} Y \leqslant \max\{|y_1|, |y_2|\} < 2Y \\ U \leqslant |u| < 2U, \ V \leqslant |v| < 2V \\ \gcd(y_1, y_2) = 1, \ (3.9) \text{ holds} \end{array} \right\},$$
(3.10)

with Y, U, V in the range

$$Y < \frac{B}{h_1^2 h_2}, \qquad U < \frac{B}{h_1^3 h_2^2}, \qquad V < B.$$
 (3.11)

We shall estimate N(Y, U, V) using the geometry of numbers, by first proving that the equation (3.9) forces the solutions to lie on a small number of lattices.

Lemma 3.3. Let ϱ and ϱ' be given by (3.1) and (3.4), respectively. Define a multiplicative function f via

$$f(p^{v}) = \begin{cases} \varrho(p^{v}) & \text{if } p \nmid C(1,0), \\ \varrho'(p^{v}) & \text{if } p \nmid C(0,1), \\ \varrho(p^{v}) + \varrho'(p^{v}) & \text{if } p \mid \gcd(C(1,0),C(0,1)). \end{cases}$$
(3.12)

Then the solutions $(y_1, y_2) \in \mathbb{Z}^2$ to

$$C(y_1, y_2) \equiv 0 \mod d$$
.

such that $gcd(y_1, y_2) = 1$ are covered by at most f(d) many rank 2 lattices, each of determinant d.

Proof. By the Chinese remainder theorem, it suffices to consider the case when $d = p^v$. Since y_1 and y_2 are coprime, p divides at most one of y_1 and y_2 . Suppose $p \nmid y_2$, then we can rewrite the congruence $C(y_1, y_2) \equiv 0 \mod p^v$ as

$$C(y_1/y_2, 1) \equiv 0 \bmod p^v$$
.

Therefore the solutions (y_1, y_2) all lie in a lattice generated by $(p^v, 0)$ and $(\alpha, 1)$, where $\alpha \in \mathbb{Z}$ is a solution to $C(x, 1) \equiv 0 \mod p^v$. Moreover, there are $\varrho(p^v)$ many choices of α modulo p^v .

If $p \mid y_2$, then since $p \nmid y_1$, we must have $p \mid C(1,0)$. In this case, consider $C(1,y_2/y_1) \equiv 0 \mod p^v$. Then the solutions (y_1,y_2) lies in a lattice generated by $(0,p^v)$ and $(1,\beta)$, where $\beta \in \mathbb{Z}$ is a solution to $C(1,\beta) \equiv 0 \mod p^v$.

Therefore, the number of lattices is bounded by $\varrho(p^v)$ if $p \nmid C(1,0)$ and $\varrho(p^v) + \varrho'(p^v)$ if $p \mid C(1,0)$. By symmetry we obtain the statement in the lemma.

Using this result we can now proved the following bound.

Lemma 3.4. Fix non-zero $h_2, u \in \mathbb{Z}$. Then

$$\# \left\{ (y_1, y_2, v) \in \mathbb{Z}^4 : \gcd(y_1, y_2) = 1, \ V \leq |v| < 2V \\ (3.9) \ holds \right\} \ll f(h_2 u^2) \left(\frac{V}{Y} + 1\right),$$

where f is the multiplicative function defined in (3.12) and the implied constant depends only on C.

Proof. We begin by applying Lemma 3.3 to $d = h_2 u^2$, and proceed to bound the number of solutions (y_1, y_2) that lie in one of the f(d) lattices of determinant d. Note that (3.9) has no solution unless $h_2 \ll Y^3$ and $U \ll Y^{3/2}$. By symmetry, on multiplying by 3, we may assume that

$$|L_1(y_1, y_2)| \leq |L_2(y_1, y_2)| \leq |L_3(y_1, y_2)|.$$

It follows from Lemma 3.1 that any such solution must satisfy

$$L_1(y_1, y_2) \ll \frac{h_2 U^2 V}{V^2}.$$
 (3.13)

The region in \mathbb{R}^2 cut out by $\max\{|y_1|, |y_2|\} < 2Y$ and (3.13) can be placed inside an ellipse $\mathcal{R} \subset \mathbb{R}^2$ with area

$$\operatorname{vol}(\mathcal{R}) \ll Y \cdot \frac{h_2 U^2 V}{Y^2} = \frac{h_2 U^2 V}{Y}.$$

By [17, Lemma 2], there are

$$\ll \frac{h_2 U^2 V}{dY} + 1 \ll \frac{V}{Y} + 1$$

many lattice points in the ellipse such that $gcd(y_1, y_2) = 1$.

Lemma 3.5. In the notation of Theorem 1.4, we have $N^{\circ}(B) \ll B(\log B)^{\max\{\lambda,2\}}$.

Proof. Recall the definition (3.10) of N(Y, U, V). We apply Lemma 3.4 and sum over $U \leq |u| < 2U$. Lemma 3.2 implies that

$$\sum_{U \le |u| < 2U} f(|u|) \ll U.$$

Now it follows from combining the Chinese remainder theorem with (3.3) and (3.5) that $f(h_2u^2) \ll f(h_2)f(|u|)$. Hence we deduce that

$$N(Y, U, V) \ll \sum_{U \leq |u| < 2U} f(h_2 u^2) \left(\frac{V}{Y} + 1\right) \ll f(h_2) \cdot U \cdot \left(\frac{V}{Y} + 1\right).$$

Note that N(Y, U, V) = 0 unless $h_2U^2V \ll Y^3$, so we can impose $U \ll (Y^3/(h_2V))^{1/2}$. Now summing N(Y, U, V) over U, V, Y being powers of 2 subject to (3.11), we have

$$\sum_{U,V,Y} N(Y,U,V) \ll f(h_2) \sum_{Y,V} \left(\frac{V^{1/2}Y^{1/2}}{h_2^{1/2}} + \frac{B}{h_1^3 h_2^2} \right) \ll \frac{f(h_2)B}{h_1 h_2} + \frac{f(h_2)B}{h_1^3 h_2^2} (\log B)^2.$$

Finally, we sum over h_1, h_2 and apply Lemma 3.2 to bound

$$\sum_{h_2 \leqslant B} \frac{f(h_2)}{h_2} \quad \text{and} \quad \sum_{h_2 \leqslant B} \frac{f(h_2)}{h_2^2}.$$

This leads to the upper bound $N^{\circ}(B) \ll B(\log B)^{\max\{\lambda,2\}}$.

3.3. Proof of the lower bound in Theorem 1.4.

Lemma 3.6. In the notation of Theorem 1.4, we have $N^{\circ}(B) \gg B$.

Proof. For each positive integer x_3 that is coprime to $\Delta(C)$, it follows from (3.3) and the Chinese remainder theorem that there are $\rho(x_3^2) = \rho(x_3)$ solutions $\alpha \mod x_3^2$ to the congruence

$$C(x,1) \equiv 0 \mod x_3^2$$
.

Each α give rise to a lattice generated by $(x_3^2, 0)$ and $(\alpha, 1)$, which produces solutions to $C(x_1, x_2) \equiv 0 \mod x_3^2$. In each lattice, Minkowski's theorem implies that $C(x_1, x_2) \equiv 0 \mod x_3^2$ has at least one non-trivial solution (x_1, x_2) such that $x_1, x_2 \ll x_3$. With such a solution, write

$$C(x_1, x_2) = x_3^2 x_4.$$

Then $x_3^2x_4 = C(x_1, x_2) \ll x_3^3$, so $x_4 \ll x_3$. Varying x_3 over integers between 1 and B such that x_3 is coprime to $\Delta(C)$, it follows from Lemma 3.2 that

$$\sum_{\substack{1 \leqslant x_3 \leqslant B \\ \gcd(x_3, \Delta(C)) = 1}} \rho(x_3) \gg B$$

which thereby gives the lower bound.

Theorem 1.4 follows immediately from Lemmas 3.5 and 3.6.

4. Integral points on quadratic twists with large gcd(x, D)

Fix integers A, B such that $x^3 + Ax + B$ is irreducible over \mathbb{Q} . Define

$$E_D: y^2 = x^3 + AD^2x + BD^3,$$

where $D \in \mathcal{D}$. The discriminant of E_D is

$$\Delta(E_D) = -16(4A^3 + 27B^2)D^6.$$

We henceforth take C to be the binary cubic form such that

$$C(x,D) = x^3 + AD^2x + BD^3.$$

Note that $x^3 + Ax + B$ being irreducible implies that C is also irreducible.

Lemma 4.1. Assume that $C(x_1, x_2) \in \mathbb{Z}[x_1, x_2]$ is irreducible. Recall the definition of ϱ from (3.1). Then

$$\sum_{\substack{p \leqslant N \\ \varrho(p) \geqslant 1}} \frac{1}{p} \leqslant \frac{2}{3} \log \log N + O(1) \tag{4.1}$$

and

$$\#\{n \leqslant N : \varrho(n) \geqslant 1\} \ll N(\log N)^{-\frac{1}{3}}.$$
 (4.2)

Proof. Since C is irreducible, the Galois group of C(x,1) is either S_3 or C_3 . The density of primes such that $\varrho(p) \geqslant 1$ is $\frac{2}{3}$ when the Galois group of is S_3 , and $\frac{1}{3}$ instead when the Galois group is C_3 . The first claim (4.1) is a consequence of the Chebotarev density theorem. The second claim (4.2) follows from (4.1) and [30, Satz 1].

We first show that for almost all $D \in \mathcal{D}$, there is no integral point $(x, y) \in E_D(\mathbb{Z})$ with large gcd(x, D).

Lemma 4.2. Let $\kappa > 0$. We have

$$\# \left\{ D \in \mathcal{D}(N) : \begin{array}{l} \gcd(x(P), D) \geqslant N(\log N)^{-\kappa} \\ \text{for some } P \in E_D(\mathbb{Z}) \end{array} \right\} \ll_{\kappa} N(\log N)^{-\frac{1}{3}} \log \log N.$$

Proof. Suppose $(x, y) \in E_D(\mathbb{Z})$ is such that $g := \gcd(x, D) \geqslant N(\log N)^{-\kappa}$. Write $x = g\tilde{x}$, $D = g\tilde{D}$. Then from the equation for E_D , we see that $g^3 \mid y^2$. Since D is square-free, g must also be square-free, so $g^2 \mid y$. Write $y = g^2\tilde{y}$. Then we can rewrite the equation as

$$g\tilde{y}^2 = \tilde{x}^3 + A\tilde{D}^2\tilde{x} + B\tilde{D}^3 = C(\tilde{x}, \tilde{D}).$$

Since D is square-free, we have that $gcd(g, \tilde{D}) = 1$. Thus we deduce that $C(\tilde{x}/\tilde{D}, 1) \equiv 0 \mod g$, whence $\rho(g) \geqslant 1$.

Factorise |D| uniquely as a product |D| = ab, where a is the product of all prime divisors of D such that $\varrho(p) \geqslant 1$. Then g must be a divisor of a, so $b \leqslant N/g \leqslant (\log N)^{\kappa}$. Using (4.2) to bound the number of a, we get that the number of possible D is bounded by

$$2\sum_{b\leqslant (\log N)^{\kappa}}\sum_{\substack{a\leqslant N/b\\\rho(a)\geqslant 1}}1\ll \sum_{b\leqslant (\log N)^{\kappa}}\frac{N/b}{(\log(N/b))^{\frac{1}{3}}}\ll_{\kappa}\frac{N\log\log N}{(\log N)^{\frac{1}{3}}},$$

as claimed. \Box

5. Integral points on quadratic twists with small gcd(x, D)

5.1. **Preliminaries.** Consider a binary quartic form of the form

$$f(X,Y) = a_0 X^4 + 4a_1 X^3 Y + 6a_2 X^2 Y^2 + 4a_3 X Y^3 + a_4 Y^4, \quad a_i \in \mathbb{Z}.$$

The invariants of f are

$$I = I(f) = a_0 a_4 - 4a_1 a_3 + 3a_2^2$$
, and $J = J(f) = a_0 a_2 a_4 - a_0 a_3^2 - a_1^2 a_4 + 2a_1 a_2 a_3 - a_2^3$.

The discriminant of f is

$$\begin{split} \Delta(f) &= I^3 - 27J^2 \\ &= a_0^3 a_4^3 - 64a_1^3 a_3^3 - 18a_0^2 a_2^2 a_4^2 - 12a_0^2 a_1 a_3 a_4^2 - 6a_0 a_1^2 a_3^2 a_4 \\ &- 180a_0 a_1 a_2^2 a_3 a_4 + 81a_0 a_2^4 a_4 + 36a_1^2 a_2^2 a_3^2 - 27(a_0^2 a_3^4 + a_1^4 a_4^2) \\ &+ 54a_2 (-a_2^2 + 2a_1 a_3 + a_0 a_4)(a_4 a_1^2 + a_0 a_3^2). \end{split}$$

The seminvariants attached to the form are I, J, $a = a(f) = a_0$,

$$H = H(f) = a_1^2 - a_0 a_2,$$

and

$$R = R(f) = 2a_1^3 + a_0^2 a_3 - 3a_0 a_1 a_2.$$

In particular H is the leading coefficient of the quartic covariant

$$G_f(X) = (a_1^2 - a_0 a_2) X^4 + 2(a_1 a_2 - a_0 a_3) X^3 + (3a_2^2 - a_0 a_4 - 2a_1 a_3) X^2 + 2(a_2 a_3 - a_1 a_4) X + (a_3^2 - a_2 a_4),$$
(5.1)

and R is the leading coefficient of the sextic covariant of f. Comparing to the formulas in [9, Section 4.1.1], here we have removed a factor of -48 from H and the quartic covariant, a factor of 32 from R, a factor of 12 from I, a factor of 432 from their J, and a factor of $256 \cdot 27$ from Δ .

Given
$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \operatorname{SL}_2(\mathbb{Z})$$
, define $\gamma \cdot (X, Y) = (aX + bY, cX + dY)$ and $(\gamma \cdot f)(X, Y) = f(\gamma \cdot (X, Y)) = f(aX + bY, cX + dY)$.

Furthermore, define the action of $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ on $(f, (\alpha, \beta))$ by

$$\gamma \cdot (f, (\alpha, \beta)) = (\gamma \cdot f, \gamma^{-1} \cdot (\alpha, \beta)), \tag{5.2}$$

and observe that the value of $f(\alpha, \beta)$ is preserved under this action.

5.2. Quartic forms associated to integral points. Given $P = (x_0, y_0) \in E_D(\mathbb{Z})$, we may write down a corresponding quartic form

$$f_P(X,Y) = X^4 - 6x_0X^2Y^2 + 8y_0XY^3 + (-4AD^2 - 3x_0^2)Y^4.$$
 (5.3)

Here $\Delta(f) = \Delta(E_D) = -16(4A^3 + 27B^2)D^6$, $I(f) = -4AD^2$ and $J(f) = -4BD^3$. This construction is due to Mordell [24, Chapter 25]. (See also [2, Section 2.2].)

Lemma 5.1. Suppose $P = (x_0, y_0) \in E_D(\mathbb{Z})$. Let M be any integer such that $M \mid D$ and $gcd(M, 2x_0) = 1$. Take any integer k such that $k \equiv y_0x_0^{-1} \mod |M|$. Then

$$F_P(X,Y) = \frac{1}{M^3} f_P(MX + kY,Y)$$
 (5.4)

is integral and satisfies

- $F_P(1,0) = M$;
- $I = -4A(D/M)^2$ and $J = -4B(D/M)^3$;
- $\Delta(F) = \Delta(f)/M^6 = -16(4A^3 + 27B^2)(D/M)^6$.

Proof. It suffices to show that there exists an integer $k \equiv y_0 x_0^{-1} \mod |M|$ such that the properties of F_P hold, because any other choice of k would simply transform F_P by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \operatorname{SL}_2(\mathbb{Z})$, which preserves the integrality of F_P and its invariants.

 $\binom{1}{0} {n \choose 1} \in \operatorname{SL}_2(\mathbb{Z})$, which preserves the integrality of F_P and its invariants. Since $M \mid D$, we have $y_0^2 \equiv x_0^3 + AD^2x_0 \mod |M|^3$ from the equation for E_D . If $k \equiv y_0x_0^{-1} \mod |M|$, then $x_0 \equiv (y_0x_0^{-1})^2 \equiv k^2 \mod |M|$. By Hensel lifting, there exists some k such that $k \equiv y_0x_0^{-1} \mod |M|$ and

$$x_0 \equiv k^2 \bmod |M|^3, \tag{5.5}$$

provided M is odd. Now since $y_0 \equiv kx_0 \equiv k^3 \mod |M|$ and $y_0^2 \equiv x_0^3 \equiv k^6 \mod |M|^2$, we deduce that $y_0 \equiv k^3 \mod |M|^2$. Then, on solving

$$(k^3 + \lambda M^2)^2 \equiv y_0^2 \equiv x_0^3 + AD^2 x_0 \equiv k^6 + AD^2 k^2 \mod |M|^3$$

for $\lambda \in \mathbb{Z}/M\mathbb{Z}$, we see that

$$y_0 \equiv k^3 + \frac{AD^2}{2k} \mod |M|^3.$$
 (5.6)

Using (5.5) and (5.6), we can check that the new quartic form

$$F_P(X,Y) = \frac{1}{M^3} f_P(MX + kY,Y)$$

$$= MX^4 + 4kX^3Y + \frac{6(k^2 - x_0)}{M} X^2 Y^2$$

$$+ \frac{4(k^3 - 3x_0k + 2y_0)}{M^2} XY^3 + \frac{k^4 - 6x_0k^2 + 8y_0k - 4AD^2 - 3x_0^2}{M^3} Y^4,$$
(5.7)

is integral and has all the claimed properties.

Lemma 5.2. Fix $A, B \in \mathbb{Z}$ such that $4A^3 + 27B^2 \neq 0$. Fix a choice of integer $M \mid \frac{D}{\gcd(2x(P),D)}$, for every $P \in \bigcup_{D \in \mathcal{D}} E_D(\mathbb{Z})$. Then the map from

$$P \in \bigcup_{D \in \mathcal{D}} E_D(\mathbb{Z})$$

to

$$(F_P, (1,0)) / \operatorname{SL}_2(\mathbb{Z}),$$

with F_P as defined in (5.4) and the $SL_2(\mathbb{Z})$ -action as defined in (5.2), is well-defined and injective.

Proof. We first prove that the map is well-defined. Given $P \in E_D(\mathbb{Z})$ with the prescribed choice of M, suppose k and k' are two choices of integer such that $k \equiv k' \equiv y_0 x_0^{-1} \mod |M|$, so k' = k + bM for some $b \in \mathbb{Z}$. Then, with such choices, the corresponding F_P is

$$F'(X,Y) = \frac{1}{M^3} f_P(MX + k'Y,Y)$$
 and $F(X,Y) = \frac{1}{M^3} f_P(MX + kY,Y)$.

But

$$(F', (1,0)) = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \cdot (F, (1,0)),$$

so (F', (1,0)) and (F, (1,0)) are in the same $SL_2(\mathbb{Z})$ -equivalence class. Therefore we have checked that the image $(F_P, (1,0))$ does not depend on the choice of k, so the map is well-defined.

We now prove that the map is injective. Suppose $P, Q \in \bigcup_{D \in \mathcal{D}} E_D(\mathbb{Z})$ are such that

$$(F_P, (1,0)) = \gamma \cdot (F_Q, (1,0)). \tag{5.8}$$

The condition that $(1,0) = \gamma^{-1} \cdot (1,0)$ implies that the first column of γ must be (1,0), and so

$$\gamma = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

for some $b \in \mathbb{Z}$, since $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ must have determinant 1. Putting this back into (5.8), we have

$$F_P(X,Y) = (\gamma \cdot F_Q)(X,Y) = F_Q(X+bY,Y). \tag{5.9}$$

Observe from the properties given in Lemma 5.1 that $F_P(1,0) = F_Q(1,0)$ determines M, and $J(F_P) = J(F_Q)$ determines D/M, so it must be that $P,Q \in E_D(\mathbb{Z})$ for the same $D \in \mathcal{D}$. Write

$$F_P(X,Y) = \frac{1}{M^3} f_P(MX + k_P Y, Y)$$
 and $F_Q(X,Y) = \frac{1}{M^3} f_Q(MX + k_Q Y, Y)$, (5.10)

where $k_P, k_Q \in \mathbb{Z}$ and $M = F_P(1, 0) = F_Q(1, 0)$.

Combining (5.10) and (5.9), we have

$$f_P(MX + k_P Y, Y) = f_Q(M(X + bY) + k_Q Y, Y).$$

On replacing X by $(X - k_P Y)/M$, we deduce that

$$f_P(X,Y) = f_Q(X + (bM + k_Q - k_P)Y, Y).$$
(5.11)

Recall that the X^3Y -coefficients of f_P and f_Q are 0 by construction. Comparing the X^3Y -coefficients on the two sides of (5.11), we have

$$bM + k_Q - k_P = 0.$$

Therefore $f_P(X,Y) = f_Q(X,Y)$, and hence P = Q.

5.3. Bounding the number of equivalence classes of quartic forms. We apply Lemma 5.2 with

$$M = \frac{D}{\gcd(2x(P), D)},$$

for every $P \in \bigcup_{D \in \mathcal{D}} E_D(\mathbb{Z})$. To bound the size of the image of $\bigcup_{D \in \mathcal{D}(N)} E_D(\mathbb{Z})$ with $\gcd(x(P), D) \leqslant N(\log N)^{-\kappa}$, we bound the number of $\operatorname{SL}_2(\mathbb{Z})$ -equivalence classes of binary quartic forms F that can arise, and we will bound separately the number of solutions $(\alpha, \beta) \in \mathbb{Z}^2$ to the Thue inequality $|F(\alpha, \beta)| \leqslant N/G$, that comes from placing a dyadic interval of length G around $\gcd(x(P), D)$.

To bound the number of $SL_2(\mathbb{Z})$ -equivalence classes of binary quartic forms, we appeal to reduction theory, which allows us to choose a representative in each $SL_2(\mathbb{Z})$ -equivalence class with bounded seminvariants. In doing so, we will make use of the following bounds taken from work of Cremona [9].

Lemma 5.3 ([9, Propositions 11 and 14]). Every integral binary quartic form F with non-zero discriminat is $SL_2(\mathbb{Z})$ -equivalent to a form F_{red} with seminvariants in the range

$$a(F_{\text{red}}) \ll |\phi| + |I(F_{\text{red}})|^{\frac{1}{2}}$$
 and $H(F_{\text{red}}) \ll |\phi|^2 + |I(F_{\text{red}})|$,

where ϕ denotes the real root of $X^3 - \frac{I(F)}{4}X - \frac{J(F)}{4}$ with the largest absolute value.

We now reduce the problem about counting $SL_2(\mathbb{Z})$ -equivalence classes of quartic forms to a problem about counting points on a cubic surface.

Lemma 5.4. The number of $SL_2(\mathbb{Z})$ -equivalence classes of F_P in the image of

$$\{P \in E_D(\mathbb{Z}) : D \in \mathcal{D}, \gcd(x(P), D) < G\}$$

is bounded by the number of $(h, a, r, g) \in \mathbb{Z}^4$, where g is a positive square-free integer, and

$$h, a, r, g \ll_{A,B} G, \tag{5.12}$$

such that

$$h^3 + Aa^2h + Ba^3 = r^2g. (5.13)$$

Furthermore we can assume that $r \neq 0$ with $O_{A,B}(G(\log G)^6)$ -many exceptions.

Proof. For $P = (x_0, y_0) \in E_D(\mathbb{Z})$, write $g = \gcd(2x_0, D)$, so that D = Mg. Reduce every $F = F_P$ to an integral binary quartic form F_{red} with seminvariants in the bounded range given in Lemma 5.3. It follows from Lemma 5.1 that $I(F) = -4Ag^2$ and $J(F) = -4Bg^3$. Take ϕ_1 to be the real root of $X^3 + AX + B$ with the largest absolute value. Then $\phi = \phi_1 g$ is the real root of

$$X^{3} - \frac{1}{4}I(F)X - \frac{1}{4}J(F) = X^{3} + Ag^{2}X + Bg^{3}$$

with largest absolute value. Since $\phi \ll_{A,B} g$, Lemma 5.3 implies that

$$a(F_{\text{red}}) \ll_{A,B} g$$
 and $H(F_{\text{red}}) \ll_{A,B} g^2$. (5.14)

To count the number of $F/\operatorname{SL}_2(\mathbb{Z})$, it suffices to count the number of possible tuples (I, J, a, H, R) taken by F_{red} , such that the tuple satisfies the syzygy

$$H^{3} - \frac{I}{4}a^{2}H - \frac{J}{4}a^{3} = \left(\frac{R}{2}\right)^{2},\tag{5.15}$$

where $(I, J, a, H, R) = (I(F_{\text{red}}), J(F_{\text{red}}), a(F_{\text{red}}), H(F_{\text{red}}), R(F_{\text{red}}))$. Plugging in $I(F_{\text{red}}) = I(F) = -4Ag^2$ and $J(F_{\text{red}}) = J(F) = -4Bg^3$, (5.15) becomes

$$H^{3} + Ag^{2}a^{2}H + Bg^{3}a^{3} = \left(\frac{R}{2}\right)^{2}.$$
 (5.16)

We can check, by putting (5.7) into (5.1), that

$$G_F(X) = x_0 X^4 + \frac{4}{M} (-y_0 + x_0 k) X^3 + \frac{2}{M^2} (2AD^2 + 3x_0^2 + 3x_0 k^2 - 6y_0 k) X^2$$

$$+ \frac{4}{M^3} (AD^2 k + 3x_0^2 k - x_0 y_0 + x_0 k^3 - 3y_0 k^2) X$$

$$+ \frac{1}{M^4} (-4Ax_0 D^2 + 4AD^2 k^2 - 3x_0^3 + 6x_0^2 k^2 - 4x_0 y_0 k + x_0 k^4 + 4y_0^2 - 4y_0 k^3).$$

Every coefficient of $G_F(X)$ is divisible by g, so $g \mid G_F(X)$. Then we also know that $g \mid G_{F_{\text{red}}}(X)$ because G_F is a covariant of F. Hence H, being the leading coefficient of $G_{F_{\text{red}}}(X)$, must also be divisible by g. The left hand side of (5.16) is integral, so R must be even. From (5.16), we deduce that $g^3 \mid \left(\frac{R}{2}\right)^2$, so $g^2 \mid \frac{R}{2}$ since g is square-free. Therefore, on writing H = gh and $\frac{R}{2} = g^2r$, we see that (5.16) becomes (5.13). The bounds (5.14) on the variables becomes

$$a \ll_{A,B} g$$
 and $h \ll_{A,B} g$.

When g < 2G, this implies that (h, a, r, g) satisfies (5.12). Since (h, a, r, g) determines (I, J, a, H, R), it suffices to bound the number of such (h, a, r, g).

If r = R = 0, then $(H, \frac{1}{2}R)$ is a torsion point in $E_{ga}(\mathbb{Z})$, so $ga \mid H$. Writing $F_{red}(X, Y) = a_0 X^3 + a_1 X^2 Y + a_2 X Y^3 + a_3 Y^3$, we have $ga_0 \mid H = a_1^2 - a_0 a_2$, hence $a_0 \mid a_1^2$. Since a_0 or a_1^2 divides every term in the formula of $\Delta(F_{red})$, we see that $a_0 \mid \Delta(F_{red}) = -16(4A^3 + 27B^2)g^6$. Given each g, the number of possible $a = a_0$ is $\ll_{A,B} 7^{\omega(g)}$. There are at most 3 torsion point in $E_{ga}(\mathbb{Z})$, so the contribution of such forms is $\ll_{A,B} \sum_{g \ll G} 7^{\omega(g)} \ll G(\log G)^6$.

We record the following upper bound, due to Thunder [29], which allows us to count the number of solutions to Thue inequalities. **Lemma 5.5.** Suppose that F(X,Y) is an integral binary form with non-zero discriminant. Then for any positive integer m, we have

$$\#\{(X,Y)\in\mathbb{Z}^2: |F(X,Y)|\leqslant m\}\ll m^{\frac{2}{\deg(F)}},$$

where the implied constant only depends on the degree deg(F) of F.

Proof. To apply [29, Theorem 2], it suffices to check that the area

$$A_F = \text{vol}\{(X, Y) \in \mathbb{R}^2 : |F(X, Y)| \le 1\}$$

is finite. The finiteness of A_F follows from work of Bean [3, Corollary 1].

We are now ready to bound the contribution from integral points $(x, y) \in E_D(\mathbb{Z})$ with small gcd(x, D).

Lemma 5.6. For any $K \geqslant 1$, we have

$$\sum_{D \in \mathcal{D}(N)} \# \{ P \in E_D(\mathbb{Z}) : \gcd(x(P), D) < K \} \ll (NK)^{\frac{1}{2}} (\log K)^{\nu},$$

where ν is 3 when $E_D[2]$ is trivial over \mathbb{Q} and 6 otherwise.

Proof. We split the sum into dyadic intervals according to the size of gcd(x(P), D). Consider the points $P \in \bigcup_{D \in \mathcal{D}(N)} E_D(\mathbb{Z})$ such that $G \leq gcd(x(P), D) < 2G$.

It follows from Lemma 5.2 that we want to bound the number of $SL_2(\mathbb{Z})$ -equivalence classes of $(F_P, (1,0))$ from such P. Given any integral binary quartic form F, we can collect all F_P that are $SL_2(\mathbb{Z})$ -equivalent to F, which we write as $F_P \sim_{SL_2(\mathbb{Z})} F$. This allows us to transform $(F_P, (1,0))$ into $(F, (\alpha, \beta))$, where $(\alpha, \beta) \in \mathbb{Z}^2$. Then, since

$$F(\alpha, \beta) = F_P(1, 0) = M = \frac{D}{\gcd(2x(P), D)},$$

we see that (α, β) satisfies $|F(\alpha, \beta)| \leq N/G$. By Lemma 5.5, the number of solutions to the inequality $|F(X,Y)| \leq N/G$ is $\ll (N/G)^{1/2}$. Therefore, given any F, we have the upper bound

$$\sum_{D \in \mathcal{D}(N)} \#\{P \in E_D(\mathbb{Z}) : F_P \sim_{\mathrm{SL}_2(\mathbb{Z})} F, \ \gcd(x(P), D) \geqslant G\} \ll \left(\frac{N}{G}\right)^{1/2}. \tag{5.17}$$

Next we bound the number of $\mathrm{SL}_2(\mathbb{Z})$ -equivalence classes of F that can arise as the image of some $P \in \bigcup_{D \in \mathcal{D}} E_D(\mathbb{Z})$. By Lemma 5.4, it suffices to count $(h,a,r,g) \in \mathbb{Z}^4$ such that g is square-free, $h,a,g,r \ll G$ and $h^3 + Aa^2h + Ba^3 = gr^2$. First suppose that $r \neq 0$. Since g is square-free, it must be that $b \coloneqq \gcd(h,a,g) \mid r$. Hence we can bound the number of (h/b,a/b,r/b,g/b) using Theorem 1.4, because $\gcd(h/b,a/b,g/b) = 1$. Summing over $b \leqslant G$, we thereby obtain

$$\#\left\{(h,a,r,g)\in\mathbb{Z}^4:\begin{array}{l}g\text{ square-free, }h,a,g,r\ll G\\h^3+Aa^2h+Ba^3=gr^2,\ r\neq0\end{array}\right\}\ll\sum_{b\leqslant G}\frac{G}{b}(\log G)^{\max\{\lambda,2\}}\\\ll G(\log G)^{\max\{\lambda,2\}+1}.$$

If E_D has non-trivial two torsion, then we also have to include $O(G(\log G)^6)$ -many exceptions to account for the possibility that r = 0. Therefore the number of $SL_2(\mathbb{Z})$ -equivalence classes in

$$\bigcup_{P \in \mathcal{P}} \{ F_P : P \in E_D, \gcd(x(P), D) < 2G \}$$

is bounded by $\ll G(\log G)^{\nu}$.

Summing (5.17) over the $O(G(\log G)^{\nu})$ -many $SL_2(\mathbb{Z})$ -equivalence classes of F, we have

$$\sum_{D \in \mathcal{D}(N)} \#\{P \in E_D(\mathbb{Z}) : G \leqslant \gcd(x(P), D) < 2G\} \ll G(\log G)^{\nu} \left(\frac{N}{G}\right)^{\frac{1}{2}}$$

$$= (NG)^{\frac{1}{2}} (\log G)^{\nu}.$$
(5.18)

Finally, summing over G being powers of 2 and subject to $1 \leq G < K$, gives the desired result.

Remark 5.7. Heuristically, we expect the set $\{(X,Y) \in \mathbb{Z}^2 : |F(X,Y)| \leq m\}$ considered in Lemma 5.5 to have size $\sim A_F m^{\frac{2}{\deg(F)}}$, where

$$A_F = \text{vol}\{(X, Y) \in \mathbb{R}^2 : |F(X, Y)| \le 1\} \ll \Delta(F)^{-\frac{1}{\deg(F)(\deg(F)-1)}}$$

by [3, Corollary 1]. When F is of degree 4 with discriminant $\Delta(F) = -16(4A^3 + 27B^2)g^6$, this gives an upper bound of $\ll \Delta(F)^{-\frac{1}{12}}m^{\frac{1}{2}} \ll_{A,B} g^{-\frac{1}{2}}m^{\frac{1}{2}}$. Such a bound would replace (5.17) by $(N/G^2)^{\frac{1}{2}}$, and replace (5.18) by $\ll N^{\frac{1}{2}}(\log G)^{\nu}$. Summing over dyadic intervals of length $G \leqslant N$ would then give

$$\sum_{D \in \mathcal{D}(N)} \# E_D(\mathbb{Z}) \ll N^{\frac{1}{2}} (\log N)^{\nu+1}.$$

However, in general, we cannot expect to be able to prove strong point-wise bounds of the form $\ll A_F m^{\frac{2}{\deg(F)}}$ on the number of solutions to Thue inequalities when m is small relative to $\Delta(F)$. As we will see in Lemma 5.8, there are infinitely many integral points in the family E_D , which implies that there are integral binary quartic forms f_P taking the form (5.3) with arbitrary large $\Delta(f_P)$, and $f_P(1,0)=1$.

5.4. Completing the proof of Theorem 2.1. Taking $K = N(\log N)^{-\kappa}$ in Lemma 5.6, we obtain

$$\sum_{D \in \mathcal{D}(N)} \# \{ P \in E_D(\mathbb{Z}) : \gcd(x(P), D) < N(\log N)^{-\kappa} \} \ll N(\log N)^{3 - \frac{1}{2}\kappa}.$$

The upper bound in Theorem 2.1 therefore follows from combining this with Lemma 4.2, on taking $\kappa = 7$. The lower bound is achieved in the following result.

Lemma 5.8. Fix $A, B \in \mathbb{Z}$ such that $x^3 + Ax + B$ is separable over \mathbb{Q} . Then

$$\#\{D \in \mathcal{D}(N) : E_D(\mathbb{Z}) \setminus E_D[2] \neq \varnothing\} \gg_{A,B} N^{\frac{1}{2}}.$$

Proof. As before, take C to be the binary cubic form such that $C(x,1) = x^3 + Ax + B$. Take $F(X,Y) = Y \cdot C(X,Y)$, which has leading coefficient 1 and must have non-zero discriminant, because C is separable over \mathbb{Q} . Appealing to work of Xiao [31, Theorem 1.2], we conclude that

$$\# \{ D \in \mathcal{D}(N) : F(\alpha, \beta) = D \text{ for some } (\alpha, \beta) \in \mathbb{Z}^2 \} \gg_F N^{\frac{1}{2}}.$$

If $F(\alpha, \beta) = \beta \cdot C(\alpha, \beta) = D$, then $\beta \mid D$ and we may write $D = \beta d$, for a suitable $d \in \mathbb{N}$. Hence $C(\alpha, \beta) = d$, and so $C(\alpha d, \beta d) = d^4$, which thereby gives a point $(\alpha d, d^2) \in E_D(\mathbb{Z})$.

6. Character sum input

The techniques developed by Heath-Brown in [18, 19] allow us to prove the following result to handle sums of products of quadratic characters. Our proof will also incorporate some refinements made in [10]. We have chosen to extract a general form of the result since we will need to apply it several times in different contexts.

Theorem 6.1. Let \mathcal{I} be a non-empty finite set and fix some subsets $\mathcal{J}_1, \ldots, \mathcal{J}_r$ of \mathcal{I} . Define a function $\Phi: \mathcal{I} \times \mathcal{I} \to \mathbb{F}_2$ such that $\Phi(i, i) = 0$ for all $i \in \mathcal{I}$. Fix $\kappa, \varepsilon, C > 0$. For each $i \in \mathcal{I}$:

- let $c_i \mid \beta_i$ be positive integers such that $c_i \leqslant C$, $\beta_i \leqslant (\log N)^{\kappa}$;
- let K_i/\mathbb{Q} be a Galois extension and let $\alpha_i \in K^{\times}$ such that $K_i(\sqrt{\alpha_i})$ is Galois over \mathbb{Q} of degree less than C and $\mathrm{Disc}(K_i(\sqrt{\alpha_i})/\mathbb{Q}) \mid \beta_i$;
- let χ_i be a multiplicative function such that for any prime p,

$$\chi_i(p) = \begin{cases} \left(\frac{\alpha_i}{\mathfrak{p}}\right) & \text{if } p \text{ splits completely in } K_i, \\ 0 & \text{otherwise,} \end{cases}$$

where \mathfrak{p} denotes a prime in K_i lying over p;

• let f_i be a multiplicative function such that for any $q \in \mathbb{Z}/c_i\mathbb{Z}$, there exists $f_{i,q} \in [0,1]$ such that $f_i(p) = f_{i,q}$ for every prime $p \equiv q \mod c_i$.

Define

$$\lambda := \max_{i \in \mathcal{I}} \frac{1}{\#(\mathbb{Z}/c_i\mathbb{Z})^{\times}} \sum_{q \in (\mathbb{Z}/c_i\mathbb{Z})^{\times}} f_{i,q}.$$

Let M be the maximum possible size of a subset $\mathcal{U} \subseteq \mathcal{I}$ such that $\Phi(i,j) + \Phi(j,i) = 0$ for every $i,j \in \mathcal{U}$. Let

$$S(N) := \sum_{(D_i)} \prod_{i \in \mathcal{I}} f_i(D_i) \chi_i(D_i) \prod_{i,j \in \mathcal{I}} \left(\frac{D_i}{D_j}\right)^{\Phi(i,j)},$$

where the sum is over all tuples of positive integers $(D_i)_{i\in\mathcal{I}}$ such that $\prod_i D_i \in \mathcal{D}(N)$, $\gcd(\prod_i D_i, 2\prod_i \beta_i) = 1$, and $\prod_{i\in\mathcal{I}\setminus\mathcal{J}_k} D_i \neq 1$ for every $k = 1, \ldots, r$. Then

$$S(N) = \sum_{\mathcal{U}} \sum_{(D_i)_{i \in \mathcal{U}}} \prod_{i \in \mathcal{U}} f_i(D_i) \chi_i(D_i) \prod_{i,j \in \mathcal{U}} \left(\frac{D_i}{D_j}\right)^{\Phi(i,j)} + O\left(N(\log N)^{(M-1)\lambda - 1 + \varepsilon}\right),$$

where the sum over \mathcal{U} is taken over all $\mathcal{U} \subseteq \mathcal{I}$ of size M satisfying all of the following:

- (P1) $\mathcal{U} \not\subseteq \mathcal{J}_k$ for every $k = 1, \ldots, r$.
- (P2) $\Phi(i,j) + \Phi(j,i) = 0$ for every $i,j \in \mathcal{U}$.
- (P3) For any $i \in \mathcal{U}$ such that $\Phi(i,j) = 0$ for all $j \in \mathcal{U}$, we have $\sqrt{\alpha_i} \in K_i(\zeta_{c_i})$, where ζ_{c_i} denotes a primitive c_i -th root of unity.
- (P4) For any distinct $i, j \in \mathcal{U}$ such that $\Phi(i, k) = \Phi(j, k)$ for all $k \in \mathcal{U}$, we have $\sqrt{\alpha_i \alpha_j} \in K_i(\zeta_{c_i}) \cdot K_j(\zeta_{c_j})$.

The implied constant depends at most on $\#\mathcal{I}, \kappa, \varepsilon, C, \lambda$.

The assumptions on f_i in Theorem 6.1 imply that

$$\sum_{p \leqslant N} \frac{f_i(p)}{p} \leqslant \lambda \log \log N + O(1) \tag{6.1}$$

for every i, by Mertens' theorem.

Definition 6.2 (Linked indices and admissible sets). Let \mathcal{I}, Φ be as in the setting of Theorem 6.1. We say that two indices $i, j \in \mathcal{I}$ are linked if $\Phi(i, j) + \Phi(j, i) = 1$, and unlinked if $\Phi(i, j) + \Phi(j, i) = 0$. We say that $\mathcal{U} \subseteq \mathcal{I}$ is an unlinked set of indices if any $i, j \in \mathcal{U}$ are unlinked. We say that an unlinked set \mathcal{U} is admissible if it satisfies both (P3) and (P4).

6.1. **Preliminaries.** We recall several results that we will need to prove Theorem 6.1. The first is a version of the Siegel-Walfisz theorem worked out by Goldstein [12].

Lemma 6.3. Let $\varepsilon > 0$. Let K/\mathbb{Q} be a Galois extension of degree n. Let χ be a non-trivial primitive finite Hecke character of K with conductor \mathfrak{f} such that

$$|\operatorname{Disc}(K/\mathbb{Q}) \cdot \operatorname{Norm}_{K/\mathbb{Q}}(\mathfrak{f})| \leq (\log N)^{\kappa}.$$

Then

$$\sum_{\substack{\mathfrak{p}\subset\mathcal{O}_K\ prime\\ \mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{p})\leqslant N}}\chi(\mathfrak{p})\ll N\exp\left(-(\log N)^{\frac{1}{3}}\right),$$

where the implied constant depends only on n and κ .

The next result is on the double oscillation of characters. An important result of this type by Heath-Brown [16, Theorem 1] is enough for most cases, however the $(MN)^{\varepsilon}$ term that appears causes problem when N and M are of very different sizes. An alternative form of this result [18, Lemma 4] removes this issue and is sufficient for our application. The optimal power saving that follows from the argument of [18, Lemma 4] can be found in [10, Lemma 15], which takes the following form.

Lemma 6.4. Let a_m and b_m be complex numbers such that $|a_m|, |b_m| \le 1$. Then for every $M, N \ge 1$ and for every $\varepsilon > 0$, we have

$$\sum_{m \le M} \sum_{n \le N} a_m b_n \mu^2(2m) \left(\frac{n}{m}\right) \ll_{\varepsilon} MN(M^{-\frac{1}{2} + \varepsilon} + N^{-\frac{1}{2} + \varepsilon}).$$

Lemma 6.5 ([27, Theorem 1]). Let f be a non-negative multiplicative function that satisfies $f(n) \leq C^{\omega(n)}$, for some constant $C \geq 1$. Then we have

$$\sum_{X-Y < n \leqslant X} f(n) \ll_C \frac{Y}{\log X} \exp\left(\sum_{p \leqslant X} \frac{f(p)}{p}\right)$$

uniformly for $2 \leqslant X \exp(-\sqrt{\log X}) \leqslant Y < X$.

Lemma 6.6 ([15, Lemma A, p. 265]). Uniformly for positive integer ℓ and $X \geqslant 2$, we have

$$\#\{n \leqslant X : \omega(n) = \ell\} \ll \frac{X}{\log X} \cdot \frac{(\log \log X + C_0)^{\ell-1}}{(\ell-1)!},$$

where C_0 is an absolute constant.

6.2. **Dissection.** Define

$$\Omega := [e \cdot \# \mathcal{I} \cdot (\log \log N + C_0)],$$

where C_0 is the constant in Lemma 6.6. We will dissect the sum according to the size of each D_i with the dissection parameter

$$\Delta := 1 + (\log N)^{-\#\mathcal{I}}.$$

For each $i \in \mathcal{I}$, define a number A_i of the form $1, \Delta, \Delta^2, \ldots$ For each $\mathbf{A} = (A_i)_{i \in \mathcal{I}}$, define the restricted sum

$$S(N, \mathbf{A}) = \sum_{(D_i)} \prod_i f_i(D_i) \chi_i(D_i) \prod_{i,j} \left(\frac{D_i}{D_j}\right)^{\Phi(i,j)},$$

where the sum over (D_i) is subject to the conditions

$$\gcd(D_i, 2\prod_i \beta_i) = 1, \quad \omega(D_i) \leqslant \Omega, \quad A_i \leqslant D_i < \Delta A_i, \quad \prod_i D_i \in \mathcal{D}(N), \text{ and}$$

$$\prod_{i \in \mathcal{I} \setminus \mathcal{I}_k} D_i \neq 1 \text{ for every } k = 1, \dots, r.$$
(6.2)

If $A_i = 1$, the condition $A_i \leq D_i < \Delta A_i$ implies that $D_i = 1$. If $\prod_{i \in \mathcal{I} \setminus \mathcal{I}_k} A_i \neq 1$ for every $k = 1, \ldots, r$, the condition (6.2) can be dropped from the sum $S(N, \mathbf{A})$. If $\prod_{i \in \mathcal{I} \setminus \mathcal{I}_k} A_i = 1$ holds for some k, the condition (6.2) forces $S(N, \mathbf{A}) = 0$.

The number of possible A_i up to N is bounded by

$$\frac{\log N}{\log \Delta} = \frac{\log N}{\log(1 + (\log N)^{-\#\mathcal{I}})} \ll (\log N)^{1 + \#\mathcal{I}}.$$

Since there are $\#\mathcal{I}$ -many variables, the number of **A** such that $S(N, \mathbf{A})$ is non-trivial is

$$\ll (\log N)^{\#\mathcal{I}(1+\#\mathcal{I})}$$

We also define here two parameters

$$N^{\dagger} := (\log N)^{4(1+\#\mathcal{I}\cdot(1+\#\mathcal{I}))}$$
 and $N^{\ddagger} := \exp\left((\log N)^{\frac{1}{\#\mathcal{I}}\cdot\varepsilon}\right)$.

6.3. Number of prime factors of the variables. We bound the contribution from those (D_i) such that $\omega(D_i) \ge \Omega$ for some $i \in \mathcal{I}$.

Lemma 6.7.

$$S(N) = \sum_{\mathbf{A}} S(N, \mathbf{A}) + O(N(\log N)^{-1}),$$

where the sum is over A is such that

$$\prod_{i \in \mathcal{I}} A_i \leqslant N.$$

Proof. We bound each summand of S(N) that does not satisfy $\omega(D_i) < \Omega$ trivially by 1. If $\omega(D_i) \ge \Omega$ for some $i \in \mathcal{I}$, then setting $n = \prod_{i \in \mathcal{I}} D_i$, we must have $\omega(n) \ge \Omega$. Given n, each prime factor of n divides one of the $\#\mathcal{I}$ -many D_i . Therefore the contribution from such n is bounded by

$$\ll \sum_{\substack{n \leqslant N \\ \omega(n) \geqslant \Omega}} (\#\mathcal{I})^{\omega(n)}.$$

By Lemma 6.6, we can bound this sum by

$$\ll \frac{N}{\log N} \sum_{\ell \geqslant \Omega} \frac{(\#\mathcal{I})^{\ell} (\log \log N + C_0)^{\ell}}{\ell!}$$

$$\leqslant \frac{N}{\log N} \frac{(\#\mathcal{I})^{\Omega} (\log \log N + C_0)^{\Omega}}{\Omega!} \sum_{\ell \geqslant 0} \frac{(\#\mathcal{I})^{\ell} (\log \log N + C_0)^{\ell}}{\Omega^{\ell}}.$$

The last sum is a geometric series. Substituting $\Omega := \lceil e \cdot \# \mathcal{I} \cdot (\log \log N + C_0) \rceil$ and using Stirling's approximation, we get the upper bound $N(\log N)^{-1}$, as desired.

6.4. **Incomplete boxes.** We bound the contribution from

$$\mathcal{F}_1 := \left\{ \mathbf{A} : \prod_i A_i \geqslant \Delta^{-\#\mathcal{I}} N \right\}.$$

Bounding the summands of $S(N, \mathbf{A})$ trivially by 1, we have

$$\sum_{\mathbf{A}\in\mathcal{F}_1} |S(N,\mathbf{A})| \leqslant \sum_{\Delta^{-\#\mathcal{I}}N\leqslant n\leqslant N} (\#\mathcal{I})^{\omega(n)} \ll (1-\Delta^{-\#\mathcal{I}}) N(\log N)^{\#\mathcal{I}-1},$$

where the last expression follows from Lemma 6.5. Since $\Delta = 1 + (\log N)^{-\#\mathcal{I}}$, we have

$$\Delta^{-\#\mathcal{I}} = \left(1 + (\log N)^{-\#\mathcal{I}}\right)^{-\#\mathcal{I}} = 1 - \#\mathcal{I}(\log N)^{-\#\mathcal{I}} + O((\log N)^{-2\#\mathcal{I}}),$$

so inserting this gives

$$\sum_{\mathbf{A}\in\mathcal{F}_1} |S(N,\mathbf{A})| \ll N(\log N)^{-1}.$$
(6.3)

6.5. Few large indices. We want to bound the contribution from **A** with very few large indices. We will bound the contribution from the set

$$\mathcal{F}_2 := \left\{ \mathbf{A} : \# \{ i \in \mathcal{I} : A_i \geqslant N^{\ddagger} \} < M \right\}.$$

Let m be the product of those $D_i \geqslant N^{\ddagger}$ and let $\mathcal{W} = \{i \in \mathcal{I} : A_i \geqslant N^{\ddagger}\}$, then

$$\sum_{\substack{\mathbf{A} \in \mathcal{F}_2 \\ \#\mathcal{W} = r}} |S(N, \mathbf{A})| \leqslant \sum_{m \leqslant (N^{\ddagger})^{\#\mathcal{I} - r}} (\#\mathcal{I} - r)^{\omega(m)} \sum_{\substack{(D_i)_{i \in \mathcal{W}} \\ \prod_{i \in \mathcal{W}} D_i \leqslant \frac{N}{m}}} \prod_{i \in \mathcal{W}} f_i(D_i).$$

Applying Lemma 6.5, the inner sum becomes

$$\sum_{\substack{(D_i)_{i \in \mathcal{W}} \\ \prod_{i \in \mathcal{W}} D_i \leqslant \frac{N}{m}}} \prod_{i \in \mathcal{W}} f_i(D_i) \ll \frac{N}{m \log N} \exp \left(\sum_{p \leqslant N} \sum_{i \in \mathcal{W}} \frac{f_i(p)}{p} \right) \ll \frac{N}{m} (\log N)^{r\lambda - 1},$$

where we have applied (6.1). Then putting this back

$$\sum_{\substack{\mathbf{A} \in \mathcal{F}_2 \\ \#\mathcal{W} = r}} |S(N, \mathbf{A})| \ll N(\log N)^{r\lambda - 1} \sum_{m \leqslant (N^{\ddagger})^{\#\mathcal{I} - r}} \frac{(\#\mathcal{I} - r)^{\omega(m)}}{m} \ll N(\log N)^{r\lambda - 1 + \varepsilon}.$$

Summing over $r \leq M - 1$, we have

$$\sum_{\mathbf{A}\in\mathcal{F}_2} |S(N,\mathbf{A})| \ll N(\log N)^{(M-1)\lambda-1+\varepsilon}.$$
 (6.4)

6.6. Two large linked indices. Let

$$\mathcal{F}_3 := \{ \mathbf{A} : A_i, \ A_j \geqslant N^{\dagger} \text{ for some linked } i, j \} \setminus \mathcal{F}_1.$$

If i and j are linked, exactly one of $\left(\frac{D_i}{D_j}\right)$ and $\left(\frac{D_j}{D_i}\right)$ can appear in the sum. For any $\mathbf{A} \in \mathcal{F}_3$, we have

$$|S(N, \mathbf{A})| \ll \sum_{(D_u)_{u \in \mathcal{I} \setminus \{i,j\}}} \left| \sum_{A_i \leqslant D_i < \Delta A_i} \sum_{A_j \leqslant D_j < \Delta A_j} a(D_i) b(D_j) \left(\frac{D_i}{D_j} \right) \right|,$$

where

$$a(D_i) = f_i(D_i)\chi_i(D_i) \prod_{k \neq i,j} \left(\frac{D_i}{D_k}\right)^{\Phi(i,k)} \left(\frac{D_k}{D_i}\right)^{\Phi(k,i)},$$

$$b(D_j) = f_j(D_j)\chi_j(D_j) \prod_{k \neq i,j} \left(\frac{D_j}{D_k}\right)^{\Phi(j,k)} \left(\frac{D_k}{D_j}\right)^{\Phi(k,j)}.$$

It follows from the assumptions that $|a(D_i)|, |b(D_j)| \leq 1$. Apply Lemma 6.4, then since $A_i, A_j \geq N^{\dagger}$, we obtain

$$|S(N, \mathbf{A})| \ll N(N^{\dagger})^{-\frac{1}{2} + \varepsilon}.$$

Summing over $O((\log N)^{\#\mathcal{I}\cdot(1+\#\mathcal{I})})$ possible **A**, we conclude that

$$\sum_{\mathbf{A}\in\mathcal{F}_3} |S(N,\mathbf{A})| \ll N(N^{\dagger})^{-\frac{1}{2}+\varepsilon} (\log N)^{\#\mathcal{I}\cdot(1+\#\mathcal{I})} \ll N(\log N)^{-1}.$$
 (6.5)

6.7. One large and one small linked indices. Define

$$\mathcal{F}_4 = \{ \mathbf{A} : 2 \leqslant A_i < N^{\dagger}, \ A_i \geqslant N^{\dagger} \text{ for some linked } i, j \} \setminus (\mathcal{F}_1 \cup \mathcal{F}_3).$$

Any j that is linked to i must satisfy $A_j < N^{\dagger}$ since we assumed that $\mathbf{A} \notin \mathcal{F}_3$. Set

$$\chi(D_i) = \chi_i(D_i) \prod_{j \neq i} \left(\frac{D_i}{D_j}\right)^{\Phi(i,j)} \left(\frac{D_j}{D_i}\right)^{\Phi(j,i)}.$$

If i and j are linked, then exactly one of $\left(\frac{D_i}{D_j}\right)$ and $\left(\frac{D_j}{D_i}\right)$ appears non-trivially in the expression. If i and j are unlinked, then either $\Phi(i,j) = \Phi(j,i) = 0$, so neither symbol appears, or $\Phi(i,j) = \Phi(j,i) = 1$, in which case we collect the two symbols as

$$\left(\frac{D_i}{D_j}\right) \left(\frac{D_j}{D_i}\right) = (-1)^{\frac{D_i - 1}{2} \cdot \frac{D_j - 1}{2}} = \left(\frac{(-1)^{\frac{D_j - 1}{2}}}{D_i}\right).$$
(6.6)

Therefore χ lifts to a character in K_i with modulus

$$4\beta_i \prod_{j \text{ linked to } i} D_j < 4\beta_i (N^{\dagger})^{\#\mathcal{I}-1} < 4(\log N)^{\kappa} (N^{\dagger})^{\#\mathcal{I}},$$

where κ is as in the assumptions of Theorem 6.1. Then

$$S(N, \mathbf{A}) \ll \sum_{(D_j)_{j \in \mathcal{I} \setminus \{i\}}} \left| \sum_{D_i} f_i(D_i) \chi(D_i) \right|.$$

Now apply the assumption on the number of prime factors of D_i , so

$$S(N, \mathbf{A}) \ll \sum_{(D_j)_{j \in \mathcal{I} \setminus \{i\}}} \sum_{\ell=1}^{\Omega} \left| \sum_{\substack{D_i \\ \omega(D_i) = \ell}} f_i(D_i) \chi(D_i) \right|.$$

Recall from the assumptions that $f_i(p)$ only depends on the value of $p \mod c_i$. Write $D_i = p_1 \cdots p_\ell$ and $p_1 < p_2 < \cdots < p_\ell$. Then $\ell \leqslant \Omega$ and we have

$$S(N, \mathbf{A}) \ll \sum_{(D_j)_{j \in \mathcal{I} \setminus \{i\}}} \sum_{\ell=1}^{\Omega} \sum_{p_1, \dots, p_{\ell-1}} \max_{b \in (\mathbb{Z}/4c_i\mathbb{Z})^{\times}} \left| \sum_{\substack{p_\ell \equiv b \bmod 4c_i \\ p_\ell \nmid \prod_j \beta_j}} \mu^2 \left(2p_1 \dots p_\ell \prod_{j \in \mathcal{I} \setminus \{i\}} D_j \right) \chi(p_\ell) \right|,$$

where

$$(N^{\dagger})^{\frac{1}{\Omega}} < (A_i)^{\frac{1}{\ell}} < p_{\ell} < \frac{\Delta A_i}{p_1 \cdots p_{\ell-1}}.$$

We use a sum of Dirichlet characters ψ mod $4c_i$ to detect the condition $p_\ell \equiv b \mod 4c_i$. Take χ' to be the character in K_i such that $\chi'(\mathfrak{p}) = \chi \psi(\operatorname{Norm}_{K_i/\mathbb{Q}}(\mathfrak{p}))$ for any degree 1 prime \mathfrak{p} in K_i . At any prime p that splits completely in K_i/\mathbb{Q} , the value of χ' is independent of the choice of \mathfrak{p} above p. The number of prime ideals \mathfrak{p} in K_i of degree greater than 1 with norm up to X is bounded by $O(X^{\frac{1}{2}})$, since then $p^2 \mid \operatorname{Norm}_{K_i/\mathbb{Q}}(\mathfrak{p})$. Recall that χ is 0 at any prime p that does not split completely in K_i . Hence we obtain

$$\sum_{p \leqslant X} \chi(p) \psi(p) = \frac{1}{[K_i : \mathbb{Q}]} \sum_{\substack{\mathfrak{p} \subset \mathcal{O}_K \text{ prime} \\ \text{Norm}_{K : I, \Omega}(\mathfrak{p}) \leqslant X}} \chi'(\mathfrak{p}) + O(X^{\frac{1}{2}}).$$

Notice that χ' must be non-trivial because $D_j \ge 2$ for some j linked to i, and by assumption D_j is coprime to $4c_i$.

Now apply Lemma 6.3, noting that the modulus of the character χ' is less than $4(\log N)^{\kappa}(N^{\dagger})^{\#\mathcal{I}} = 4(\log N)^{\kappa+4\#\mathcal{I}(1+\#\mathcal{I}\cdot(1+\#\mathcal{I}))}$. Then, for any B>0, we obtain

$$\sum_{p_{\ell} \equiv \kappa \bmod 4c_i} \mu^2 \left(2p_1 \dots p_{\ell} \prod_{j \in \mathcal{I} \setminus \{i\}} D_j \right) \chi(p_{\ell}) \ll_B \frac{A_i}{p_1 \dots p_{\ell-1}} \left(\frac{1}{\Omega} \log N^{\ddagger} \right)^{-B} + \Omega,$$

where the last term comes from those p_{ℓ} that divide some $2p_1 \cdots p_{\ell-1} \prod_{j \neq i} D_j \prod_j \beta_j$. Summing over $p_{\ell-1}, \dots, p_1$, and then over $(D_j)_{j \in \mathcal{I} \setminus \{i\}}$, we have

$$S(N, \mathbf{A}) \ll_B N(\log N) \left(\frac{1}{\Omega} \log N^{\ddagger}\right)^{-B}.$$

Picking B large enough and summing over $O((\log N)^{\#\mathcal{I}\cdot(1+\#\mathcal{I})})$ possible **A**, we finally deduce that

$$\sum_{\mathbf{A}\in\mathcal{F}_4} |S(N,\mathbf{A})| \ll N(\log N)^{-1}.$$
(6.7)

6.8. **Inadmissible sets.** Define

$$\mathcal{F}_5 \coloneqq \bigcup_{\substack{\mathcal{U} \text{ unlinked inadmissible}}} \mathcal{F}_5(\mathcal{U}),$$

where

$$\mathcal{F}_5(\mathcal{U}) := \{ \mathbf{A} : A_k = 1 \text{ for all } k \notin \mathcal{U}, \ A_i \geqslant N^{\ddagger} \text{ for all } i \in \mathcal{U} \}.$$

If \mathcal{U} does not satisfy (P3), we can take $i \in \mathcal{U}$ such that $\Phi(i,j) = 0$ for all $j \in \mathcal{U}$ and $\sqrt{\alpha_i} \notin K_i(\zeta_{c_i})$ so that $\chi_i \psi$ is non-trivial for any Dirichlet character ψ mod c_i . Then the argument is similar to that for $\mathbf{A} \in \mathcal{F}_4$, but where b is instead taken from $(\mathbb{Z}/c_i\mathbb{Z})^{\times}$ and the sum is over $p_{\ell} \equiv b \mod c_i$.

If \mathcal{U} does not satisfy (P4), take $\{i, j\} \subseteq \mathcal{U}$ such that $\Phi(i, k) = \Phi(j, k)$ for all $k \in \mathcal{U}$, assume that $\sqrt{\alpha_i \alpha_j} \notin K_i(\zeta_{c_i}) \cdot K_j(\zeta_{c_i})$. Set

$$\varphi(D_i) = \prod_{k \in \mathcal{U} \setminus \{i,j\}} \left(\frac{D_i}{D_k}\right)^{\Phi(i,k)} \left(\frac{D_k}{D_i}\right)^{\Phi(k,i)}.$$

Notice that $\Phi(i,j) = \Phi(j,j) = 0$ and also $\Phi(j,i) = \Phi(i,i) = 0$ by assumption. Since the indices in \mathcal{U} are unlinked, it follows from (6.6) that $\varphi(D_i)$ is either $\left(\frac{-1}{D_i}\right)$ or trivial

depending on D_k and the values of $\Phi(i,k)$ for $k \in \mathcal{U} \setminus \{i,j\}$. Since $\Phi(i,k) = \Phi(j,k)$ for all $k \in \mathcal{U}$, we have

$$S(N, \mathbf{A}) \ll \sum_{(D_k)_{k \in \mathcal{U} \setminus \{i, j\}}} \left| \sum_{A_i \leqslant D_i < \Delta A_i} f_i(D_i) \chi_i(D_i) \varphi(D_i) \sum_{A_j \leqslant D_j < \Delta A_j} f_j(D_j) \chi_j(D_j) \varphi(D_j) \right|.$$

Since $\sqrt{\alpha_i \alpha_j} \notin K_i(\zeta_{c_i}) \cdot K_j(\zeta_{c_j})$, we deduce that $K_i(\sqrt{\alpha_i}) \cdot K_j(\sqrt{\alpha_j}) \not\subseteq K_i(\zeta_{c_i}) \cdot K_j(\zeta_{c_j})$ and $K_i(\sqrt{-\alpha_i}) \cdot K_j(\sqrt{-\alpha_j}) \not\subseteq K_i(\zeta_{c_i}) \cdot K_j(\zeta_{c_j})$. Therefore at least one of $K_i(\sqrt{\alpha_i}) \not\subseteq K_i(\zeta_{c_i})$ and $K_j(\sqrt{\alpha_j}) \not\subseteq K_j(\zeta_{c_j})$ holds, and similarly at least one of $K_i(\sqrt{-\alpha_i}) \not\subseteq K_i(\zeta_{c_i})$ and $K_j(\sqrt{-\alpha_j}) \not\subseteq K_j(\zeta_{c_j})$ holds. This allows us to take some $k \in \{i, j\}$ such that the character $\chi_k \varphi \psi$ is non-trivial for every Dirichlet character ψ mod c_k . Then the argument proceeds similarly as in the case for $\mathbf{A} \in \mathcal{F}_4$ by applying Lemma 6.3 to $\chi_k \varphi \psi$.

Therefore we conclude that

$$\sum_{\mathbf{A} \in \mathcal{F}_5} |S(N, \mathbf{A})| \ll N(\log N)^{-1}. \tag{6.8}$$

6.9. **Proof of Theorem 6.1.** By Lemma 6.7, (6.3),(6.4), (6.5), (6.7), and (6.8), it remains to consider

$$\sum_{\mathbf{A}\notin\mathcal{F}_1\cup\mathcal{F}_2\cup\mathcal{F}_3\cup\mathcal{F}_4\cup\mathcal{F}_5} S(N,\mathbf{A}).$$

Since $\mathbf{A} \notin \mathcal{F}_2$, there are at least M indices such that $A_i \geqslant N^{\ddagger}$. Call this set of indices \mathcal{U} . Any two indices in \mathcal{U} must be unlinked because $\mathbf{A} \notin \mathcal{F}_3$. The assumption that any unlinked set must have size $\leqslant M$ implies that \mathcal{U} must have size exactly M. Moreover any other indices not in \mathcal{U} must be linked to some indices in \mathcal{U} , and so we are forced to have $A_j = 1$ for any $j \notin \mathcal{U}$ because $\mathbf{A} \notin \mathcal{F}_3 \cup \mathcal{F}_4$.

Now if $\mathcal{U} \subseteq \mathcal{J}_k$ for some $k \in \{1, \ldots, r\}$, then $A_j = 1$ for all $j \in \mathcal{I} \setminus \mathcal{J}_k$. This would contradict the condition $\prod_{i \in \mathcal{I} \setminus \mathcal{J}_k} D_i \neq 1$. Therefore we can assume that $\mathcal{U} \not\subseteq \mathcal{J}_k$. Also $\mathbf{A} \notin \mathcal{F}_5$ allows us to assume that \mathcal{U} is admissible. Substituting $D_i = 1$ for all $i \notin \mathcal{U}$ gives the main term in Theorem 6.1.

7. QUADRATIC TWISTS WITH FULL TWO-TORSION

In this section, we will prove Theorem 2.2. The lower bound in Theorem 2.2 follows from Lemma 5.8, and so it remains to prove the upper bound. For convenience, we shall work with a different model for the elliptic curves. If a monic polynomial $f \in \mathbb{Z}[x]$ has three distinct roots $r_1 < r_2 < r_3$ over \mathbb{Q} , then $r_1, r_2, r_3 \in \mathbb{Z}$ and it follows that $f(x + r_1) = x(x - (r_2 - r_1))(x - (r_3 - r_1))$. Therefore, on using a linear transformation, it suffices to consider the integral points with respect to the model

$$E_D: y^2 = x(x - AD)(x - BD),$$
 (7.1)

where 0 < A < B are integers that are fixed, and $D \in \mathcal{D}$. Accordingly, we define

$$E_D^*(\mathbb{Z}) := E_D(\mathbb{Z}) \setminus E_D[2] = \{(x, y) \in \mathbb{Z}^2 : y \neq 0, \ y^2 = x(x - AD)(x - BD)\}.$$

The following result is a refinement of Theorem 2.2.

Theorem 7.1. Let $A, B \in \mathbb{Z}$ such that 0 < A < B and consider the model (7.1). Then

$$\#\{D \in \mathcal{D}(N) : E_D^*(\mathbb{Z}) \neq \varnothing\} \ll \begin{cases} N(\log N)^{-\frac{1}{4} + \varepsilon} & \text{if } AB \notin \mathbb{Q}^2 \text{ and } B(B - A) \notin \mathbb{Q}^2, \\ N(\log N)^{-\frac{1}{8} + \varepsilon} & \text{if } AB \in \mathbb{Q}^2 \text{ or } B(B - A) \in \mathbb{Q}^2, \end{cases}$$

where the implied constant depends at most on A, B and ε .

Define

$$\mathcal{D}^+ := \{D > 0 : D \in \mathbb{Z} \text{ square-free}\}\$$

and

$$\mathcal{D}^+(N) := \{ D \in \mathcal{D}^+ : D \leqslant N \}.$$

We may assume that gcd(A, B) = 1, since otherwise we can consider the larger family where A and B are replaced by A/gcd(A, B) and B/gcd(A, B). This assumption also implies that A, B, B - A are pairwise coprime. The main result of this section is the following proposition.

Proposition 7.2. Let $A, B \in \mathbb{Z}$ such that 0 < A < B and gcd(A, B) = 1, and consider the model (7.1). Fix $\kappa > 0$. Then

$$\#\left\{D \in \mathcal{D}^+(N) : \begin{array}{l} \gcd(x,D) \geqslant N(\log N)^{-\kappa} \\ for \ some \ (x,y) \in E_D^*(\mathbb{Z}) \end{array}\right\} \ll \begin{cases} N(\log N)^{-\frac{1}{4}+\varepsilon} & \text{if } AB \notin \mathbb{Q}^2 \\ N(\log N)^{-\frac{1}{8}+\varepsilon} & \text{if } AB \in \mathbb{Q}^2, \end{cases}$$

where the implied constant depend at most on A, B, κ and ε .

Suppose $(x,y) \in E_D^*(\mathbb{Z})$, so that $y \neq 0$. Let $g := \gcd(x,D)$ and write $x = g\tilde{x}$ and $D = g\tilde{D}$. Then from the equation for E_D , we see that $g^3 \mid y^2$. Since D is square-free, g must also be square-free, so $g^2 \mid y$ and we write $y = g^2\tilde{y}$. We may now rewrite the equation as

$$g\tilde{y}^2 = \tilde{x}(\tilde{x} - A\tilde{D})(\tilde{x} - B\tilde{D}). \tag{7.2}$$

Here $gcd(\tilde{x}, \tilde{D}) = 1$, so

$$\gcd(\tilde{x}, \tilde{x} - A\tilde{D}) \mid A$$
$$\gcd(\tilde{x}, \tilde{x} - B\tilde{D}) \mid B$$
$$\gcd(\tilde{x} - A\tilde{D}, \tilde{x} - B\tilde{D}) \mid B - A.$$

We proceed by rewriting the factors appearing on the right hand side of (7.2) as

$$\tilde{x} = G_1 y_1^2,$$

$$\tilde{x} - A\tilde{D} = G_2 y_2^2,$$

$$\tilde{x} - B\tilde{D} = G_3 y_3^2,$$

$$(7.3)$$

where G_1, G_2, G_3 are square-free integers and y_1, y_2, y_3 are non-zero integers, such that $G_1G_2G_3 = q(\delta_1\delta_2\delta_3)^2$ with

$$\delta_1 := \gcd(G_2, G_3) \mid B - A, \qquad \delta_2 := \gcd(G_3, G_1) \mid B, \qquad \delta_3 := \gcd(G_1, G_2) \mid A.$$

Since A, B, B-A are pairwise coprime, $\delta_1, \delta_2, \delta_3$ are also pairwise coprime. If $p \mid \gcd(\delta_i, \tilde{D})$, then $p \mid \tilde{x}$ by (7.3). But $\gcd(\tilde{x}, \tilde{D}) = 1$, and so it must be that $\gcd(\delta_1 \delta_2 \delta_3, \tilde{D}) = 1$. This observation, together with $\gcd(g, \tilde{D}) = 1$, implies that $\gcd(G_1 G_2 G_3, \tilde{D}) = 1$. Taking the difference between the equations in (7.3), the system can be rewritten as

$$G_1 y_1^2 - G_2 y_2^2 = A\tilde{D}$$

$$G_1 y_1^2 - G_3 y_3^2 = B\tilde{D}$$

$$G_2 y_2^2 - G_3 y_3^2 = (B - A)\tilde{D}.$$
(7.4)

We have seen that $(x, y) \in E_D^*(\mathbb{Z})$ gives a system of the form (7.4). For given distinct i and j, consider the map

$$\{(x,D): D \in \mathcal{D}, (x,y) \in E_D(\mathbb{Z}) \text{ for some } y \neq 0\} \to \mathbb{Z}_{\neq 0} \times \mathbb{Z}_{\neq 0},$$
 (7.5)

given by $(x, D) \mapsto (G_i y_i^2, G_j y_j^2)$. Given $(G_i y_i^2, G_j y_j^2)$, we can recover the value of \tilde{D} from the equations in (7.4), and then the value of $G_k y_k^2$, where $k \notin \{i, j\}$. Since $y_k \neq 0$ and G_k is square-free, this is enough to recover G_k . Similarly, we can recover G_i and G_j . We also get g from the square-free part of $G_1G_2G_3$. Finally we obtain a pair (x, D) through the identities $x = g\tilde{x} = gG_1y_1^2$ and $D = g\tilde{D}$.

The G_i we have constructed are square-free but not necessarily all positive. We now show the case with any negative G_i has negligible contribution. Over \mathbb{R} , the curve E_D has two connected components, we bound the number of integral points that lie in the compact component.

Lemma 7.3. Suppose B > A are coprime positive integers. Fix $\kappa > 0$.

$$\sum_{D \in \mathcal{D}^+(N)} \# \left\{ (x, y) \in E_D^*(\mathbb{Z}) : x < BD \text{ and } \gcd(x, D) \geqslant \frac{N}{(\log N)^{\kappa}} \right\} \ll (\log N)^{2\kappa},$$

where the implied constant depends at most on A, B.

Proof. If $(x,y) \in E_D^*(\mathbb{Z})$ is such that x < BD, then we have a solution (y_1, y_2, y_3) to (7.4) with $G_2, G_3 < 0$ and $G_1 > 0$. The condition $\gcd(x, D) \geqslant \frac{N}{(\log N)^{\kappa}}$ implies that $\tilde{D} \leqslant (\log N)^{\kappa}$. Looking at the second equation $G_1y_1^2 - G_3y_3^2 = B\tilde{D}$, the terms on the left are both positive, so $G_1y_1^2, G_3y_3^2 \ll (\log N)^{\kappa}$. This gives $\ll (\log N)^{2\kappa}$ possible $(G_1y_1^2, G_3y_3^2)$. Finally we use the fact that the map (7.5) has O(1) fibres above $(G_1y_1^2, G_3y_3^2)$, giving O(1) choices for y, x, D overall.

Lemma 7.3 allows us to restrict to the points with $G_1, G_2, G_3 > 0$ in the rest of our argument.

7.1. 2-Selmer elements from integral points with large gcd(x, D). We will use Theorem 6.1 to prove the following lemma.

Lemma 7.4. Suppose B > A are coprime positive integers. Fix $\kappa > 0$. Then

$$\# \left\{ D \in \mathcal{D}^+(N) : \begin{array}{l} x \geqslant BD \ and \\ \gcd(x,D) \geqslant N(\log N)^{-\kappa} \\ for \ some \ (x,y) \in E_D^*(\mathbb{Z}) \end{array} \right\} \ll \left\{ \begin{array}{ll} N(\log N)^{-\frac{1}{4}+\varepsilon} & \text{if } AB \notin \mathbb{Q}^2 \\ N(\log N)^{-\frac{1}{8}+\varepsilon} & \text{if } AB \in \mathbb{Q}^2, \end{array} \right.$$

where the implied constant depend at most on A, B, κ and ε .

We collect from (7.4) the local solvability conditions at the primes p dividing g, but not $AB(B-A)\tilde{D}$. Note that such primes are necessarily odd since AB(B-A) is even. These conditions may be written

$$\begin{cases}
\left(\frac{-A\tilde{D}G_2}{p}\right) = \left(\frac{-B\tilde{D}G_3}{p}\right) = 1 & \text{if } p \mid G_1, \\
\left(\frac{A\tilde{D}G_1}{p}\right) = \left(\frac{-(B-A)\tilde{D}G_3}{p}\right) = 1 & \text{if } p \mid G_2, \\
\left(\frac{B\tilde{D}G_1}{p}\right) = \left(\frac{(B-A)\tilde{D}G_2}{p}\right) = 1 & \text{if } p \mid G_3.
\end{cases}$$

For each i, define $\gamma_i = \gcd(AB(B-A), G_i)$ and n_i such that

$$G_i = n_i \gamma_i$$
.

Thus $gcd(n_i, AB(B-A)) = 1$ and n_i is square-free, since G_i is square-free. Define

$$R_{13} = -A\tilde{D} \cdot \gamma_2,$$
 $R_{12} = -B\tilde{D} \cdot \gamma_3,$ $R_{21} = -(B-A)\tilde{D} \cdot \gamma_3,$ $R_{23} = A\tilde{D} \cdot \gamma_1,$ $R_{32} = B\tilde{D} \cdot \gamma_1,$ $R_{31} = (B-A)\tilde{D} \cdot \gamma_2,$

and

$$R_{i0} = 1$$
, $R_{i4} = \prod_{k \in \{1,2,3\} \setminus \{i\}} R_{ik}$,

for $i \in \{1, 2, 3\}$.

We may now rewrite the local conditions at the primes dividing $n_1n_2n_3$ as

$$\begin{cases}
\left(\frac{R_{13}n_2}{p}\right) = \left(\frac{R_{12}n_3}{p}\right) = 1 & \text{if } p \mid n_1, \\
\left(\frac{R_{23}n_1}{p}\right) = \left(\frac{R_{21}n_3}{p}\right) = 1 & \text{if } p \mid n_2, \\
\left(\frac{R_{32}n_1}{p}\right) = \left(\frac{R_{31}n_2}{p}\right) = 1 & \text{if } p \mid n_3.
\end{cases}$$
(7.6)

Then, given $\gamma_1, \gamma_2, \gamma_3, \tilde{D}$, the latter conditions are satisfied by (n_1, n_2, n_3) if and only if the expression

$$\frac{1}{4^{\omega(n_1 n_2 n_3)}} \prod_{p|n_1} \left(1 + \left(\frac{R_{13} n_2}{p} \right) \right) \left(1 + \left(\frac{R_{12} n_3}{p} \right) \right) \\
\times \prod_{p|n_2} \left(1 + \left(\frac{R_{23} n_1}{p} \right) \right) \left(1 + \left(\frac{R_{21} n_3}{p} \right) \right) \prod_{p|n_3} \left(1 + \left(\frac{R_{32} n_1}{p} \right) \right) \left(1 + \left(\frac{R_{31} n_2}{p} \right) \right) \tag{7.7}$$

is equal to 1. We can expand the first product as

$$\prod_{p|n_1} \left(1 + \left(\frac{R_{13}n_2}{p} \right) \right) \left(1 + \left(\frac{R_{12}n_3}{p} \right) \right) = \sum_{n_1 = n_{10}n_{12}n_{13}n_{14}} \left(\frac{R_{13}n_2}{n_{13}n_{14}} \right) \left(\frac{R_{12}n_3}{n_{12}n_{14}} \right).$$

Similarly we expand the other products with indexing

$$n_1 = n_{10}n_{12}n_{13}n_{14}, \quad n_2 = n_{20}n_{21}n_{23}n_{24}, \quad n_3 = n_{30}n_{31}n_{32}n_{34}.$$

We will sum (7.7) over positive square free integers n_1, n_2, n_3 coprime to $AB(B-A)\tilde{D}$, with the exceptions

$$\begin{cases} n_1 n_2 = 1 & \text{if } \tilde{D} = 1, \ AB \text{ not square, } R_{32} \text{ and } R_{31} \text{ are squares,} \\ n_1 = 1 & \text{if } \tilde{D} = 1, \ AB, R_{32} \text{ are squares.} \end{cases}$$
 (7.8)

Lemma 7.5. Let $\kappa > 0$. Fix positive integers $\gamma_1, \gamma_2, \gamma_3 \mid AB(B-A)$ and take a square-free positive integer $\tilde{D} \leq (\log N)^{\kappa}$ that is coprime to $\gamma_1 \gamma_2 \gamma_3$. Let τ be the square-free part of $\gamma_1 \gamma_2 \gamma_3 \tilde{D}$. We have

$$\# \left\{ D \in \mathcal{D}^{+}(N) : \begin{array}{l} n_{1}, n_{2}, n_{3} \geqslant 1, \ n_{1}n_{2}n_{3}\tau = D \\ (7.6) \ holds, \ but \ (7.8) \ is \ not \ satisfied \\ \gcd(n_{1}n_{2}n_{3}, AB(B-A)) = 1 \end{array} \right\} \ll \frac{N}{\tilde{D}} (\log N)^{-\frac{1}{4} + \varepsilon},$$

where the implied constant depends at most on A, B, κ and ε .

Proof. Let R(N) denote the quantity that is to be estimated. Summing (7.7) over the (n_1, n_2, n_3) satisfying the assumptions, and then expanding the sum, we get

$$R(N) = \# \left\{ (n_1, n_2, n_3) \in \mathbb{Z}_{>0}^3 : \begin{array}{l} n_1 n_2 n_3 \tau \in \mathcal{D}(N) \\ (7.6) \text{ holds, but } (7.8) \text{ is not satisfied} \\ \gcd(n_1 n_2 n_3, AB(B - A)) = 1 \end{array} \right\}$$
$$= \sum_{(n_{ij})} \prod_{i} \frac{1}{4^{\omega(n_{i0})}} \prod_{j \neq 0} \frac{1}{4^{\omega(n_{ij})}} \left(\frac{R_{ij}}{n_{ij}} \right) \prod_{k \notin \{i, j\}} \prod_{0 \leqslant l \leqslant 4} \left(\frac{n_{kl}}{n_{ij}} \right),$$

where the sum is over tuples of positive integers (n_{ij}) such that $\prod_{ij} n_{ij} \in \mathcal{D}(\frac{N}{\tau})$, such that (7.8) does not hold, but $\gcd(\prod n_{ij}, AB(B-A)\tau) = 1$. We apply Theorem 6.1 with

$$\mathcal{I} = \{10, 12, 13, 14, 20, 21, 23, 24, 30, 31, 32, 34\},\$$

$$\mathcal{J} = \begin{cases} \{30, 31, 32, 34\} & \text{if } \tilde{D} = 1, \ AB \text{ not square, } R_{32} \text{ and } R_{31} \text{ are squares,} \\ \{20, 21, 23, 24, 30, 31, 32, 34\} & \text{if } \tilde{D} = 1, \ AB, R_{32} \text{ are squares,} \\ \varnothing & \text{otherwise.} \end{cases}$$

Furthermore, we take $\lambda = \frac{1}{4}$ and

$$\Phi(kl, ij) = \begin{cases} 1 & \text{if } k \notin \{i, j\} \text{ and } j \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

Finally, we take $f_i(n) = 4^{-\omega(n)}$ and $c_i = 1$ for all $i \in \mathcal{I}$. By [18, Lemma 9], the maximal unlinked sets in \mathcal{I} are of size 4, and those that are within \mathcal{I} are

$$\{i0, ij, ik, i4\}, \{i0, j0, ij, ji\}, \{ik, i4, jk, j4\},$$

where $i, j, k \in \{1, 2, 3\}$ denotes different non-zero indices. Therefore the error term in Theorem 6.1 becomes $O(\frac{N}{\tilde{D}}(\log N)^{-\frac{1}{4}+\varepsilon})$, which is satisfactory. It remains to treat the main term in Theorem 6.1. We claim that the only maximal unlinked sets that are admissible coincide with \mathcal{J} , so that the main term vanishes.

The first case to check is $\mathcal{U} = \{i0, ij, ik, i4\}$. Here $\Phi(u, v) = 0$ for all $u, v \in \mathcal{U}$, so for (P3) to hold, R_{ij} and R_{ik} are both squares. Since $R_{12}, R_{21}, R_{13} < 0$, the only possible case is when i = 3, and $R_{31} = (B - A)\tilde{D} \cdot \gamma_2$ and $R_{32} = B\tilde{D} \cdot \gamma_1$ are squares. Since \tilde{D} is coprime to $\gamma_1\gamma_2$ and square-free, it must be that $\tilde{D} \mid B$ and $\tilde{D} \mid B - A$. However by assumptions B and B - A are coprime, so $\tilde{D} = 1$. This possibility therefore lies in \mathcal{J} .

In the second case $\mathcal{U} = \{i0, j0, ij, ji\}$, and again $\Phi(u, v) = 0$ for all $u, v \in \mathcal{U}$. Thus (P3) implies that R_{ij} and R_{ji} are both squares. Since $R_{12}, R_{21}, R_{13} < 0$, the only possible case is when $\{i, j\} = \{2, 3\}$, and $R_{23} = A\tilde{D} \cdot \gamma_1$ and $R_{32} = B\tilde{D} \cdot \gamma_1$ are squares. Then $R_{23}R_{32}$ is a square, and so AB is a square. This means that A and B are squares, since $\gcd(A, B) = 1$. By construction \tilde{D} is square-free and coprime to γ_1 , but $\tilde{D}\gamma_1$ is a square and so we conclude that $\tilde{D} = 1$, which thereby leads us to \mathcal{J} .

For the third case, $\mathcal{U} = \{ik, i4, jk, j4\}$, and we can check that

$$\Phi(ik, i4) = \Phi(jk, j4) = 0$$

$$\Phi(ik, jk) = \Phi(ik, j4) = \Phi(i4, jk) = \Phi(i4, j4) = 1.$$

We check (P4) with $\{ik, i4\}$ or $\{jk, j4\}$. Then $R_{ik}R_{i4}$ and $R_{jk}R_{j4}$ are both squares, so R_{ij} and R_{ji} are both squares. This again force us into \mathcal{J} , similarly to the second case.

7.2. Exceptional points of the first kind. We now treat the first of the cases that were previously excluded, as listed in (7.8). The following result on simultaneous Pell equations [5, Theorem 1.2] will prove crucial.

Lemma 7.6. Let a, b be positive integers and u, v be non-zero integers. Then the number of positive integer solutions (x, y) to the equation $ax^2 - by^2 = u$, such that

$$cy^2 - dz^2 = v$$
 for some positive integers c, d, z satisfying $ab < cd$ and $cd \in \mathcal{D}(N)$,

is bounded by $O(\sqrt{N}(\log N)^2)$, where the implied constant depends at most on a, b, u, v.

Proof. Rescale the equations to

$$(ax)^2 - aby^2 = au,$$

$$(dz)^2 - cdy^2 = -dv.$$

First suppose that none of ab, cd and abcd are squares. Then by [5, Theorem 1.2], we have the upper bound

$$\max\{ax, y, dz\} \leqslant \max\{|au|, |dv|, 2\}^{C\sqrt{abcd}(\log ab)(\log cd)}, \tag{7.9}$$

for an absolute constant C > 0. Suppose we have a solution to the first equation and let ε be the fundamental unit of $\mathbb{Q}(\sqrt{ab})$. Then there exists a positive integer k such that

$$\varepsilon^k \leqslant ax + \sqrt{ab}y < \varepsilon^{k+1}.$$

We refer to $\alpha = \varepsilon^{-k}(ax + \sqrt{ab}y)$ as the base solution, noting that $1 \leqslant \alpha < \varepsilon$ and $|\overline{\alpha}| = |au/\alpha| \leqslant |au|$. In particular, the number of base solutions only depends on a, b, u. The solutions to the first equation all take the form

$$ax + \sqrt{ab}y = \alpha \varepsilon^l.$$

for positive integers l. Thus, given a base solution, it follows from (7.9) that

$$\varepsilon^l \ll \max\{|au|, |dv|, 2\}^{C\sqrt{abcd}(\log ab)(\log cd)}.$$

Taking logs and noting that $cd \leq N$, we have

$$l \ll \sqrt{abcd}(\log ab)(\log cd)(\log \max\{|au|, |dv|, 2\}) + 1 \ll \sqrt{N}(\log N)^2,$$

which gives the claimed upper bound.

It remains to check the case when one of ab, cd and abcd is a square. Since cd is square-free and $cd > ab \ge 1$, cd and abcd cannot be squares. If ab is a square, then we can factor the first equation as $(ax - \sqrt{ab}y)(ax + \sqrt{ab}y) = au$ over \mathbb{Q} . There are finitely many ways to factor au as two factors over \mathbb{Q} , from which we can solve for x and y. Therefore in this case the number of solutions (x, y) is bounded in terms of a and u.

The first case in (7.8) comes from integral points of the form $(BD,0)+2E_D(\mathbb{Q})$. In this case $\tilde{D}=n_1=n_2=1$, and $R_{32}=B\gamma_1$, $R_{31}=(B-A)\gamma_2$ are both squares, so G_1B and $G_2(B-A)$ are squares. Putting back to (7.3) we see that xBD and (x-AD)(B-A)D are squares.

Lemma 7.7. We have

$$\sum_{D \in \mathcal{D}^+(N)} \# \left\{ (x,y) \in E_D^*(\mathbb{Z}) : \begin{array}{l} xBD \in \mathbb{Q}^2, \ (x-AD)(B-A)D \in \mathbb{Q}^2, \\ \gcd(x,D) = D, \ x > BD \end{array} \right\} \ll \sqrt{N} (\log N)^2,$$

where the implied constant depends at most on A, B.

Proof. The conditions implies that $\tilde{x}B$ and $(\tilde{x}-A)(B-A)$ are squares. In the notation of (7.3), G_1 is the square-free part of B and G_2 is the square-free part of B-A. Substitute

$$BG_1y_1^2 = U^2$$
 and $(B-A)G_2y_2^2 = V^2$

into the first two equations of (7.4),

$$\begin{cases} (B-A)U^2 - BV^2 = AB(B-A) \\ U^2 - BG_3y_3^2 = B^2. \end{cases}$$

By Lemma 7.6, the number of positive integers (U, V) satisfying the equations is bounded by $\ll_{A,B} \sqrt{N} (\log N)^2$. We can recover the integral point $(x, \pm y)$ from each (U, V).

7.3. Exceptional points of the second kind. We proceed to treat the second case in (7.8), and so we assume that AB, R_{32} are squares, $\tilde{D}=1$ and $n_1=1$. In particular, D=g and $G_1=\gamma_1$. Since A, B are coprime, we can write $A=a^2$, $B=b^2$ for some integers a, b. Since $R_{32}=b^2\gamma_1$ is a square, we see that G_1 is a square and hence \tilde{x} is a square. Thus $x=g\tilde{x}=Du^2$ for some integer u. Finally the conditions $G_1,G_2,G_3>0$ are equivalent to x>BD. In this way we are led to tackle the following result.

Lemma 7.8. Let B > A be coprime positive integers that are both squares. We have

$$\sum_{D \in \mathcal{D}^{+}(N)} \# \{ (x, y) \in E_{D}^{*}(\mathbb{Z}) : xD \in \mathbb{Q}^{2}, \ x > BD \} \ll N(\log N)^{-\frac{1}{8} + \varepsilon},$$

where the implied constant depends at most on A, B.

Proof. Suppose $(x,y) \in E_D^*(\mathbb{Z})$ and $x = Du^2$, where u is a positive integer. Substituting $x = Du^2$ into the equation $y^2 = x(x - a^2D)(x - b^2D)$, we obtain

$$(u^2 - a^2)(u^2 - b^2) = Dt^2,$$

for some non-zero integer t, since $y \neq 0$. Then from the factorisation we can write

$$u - a = g_1 y_1^2,$$

$$u + a = g_2 y_2^2,$$

$$u - b = g_3 y_3^2,$$

$$u + b = g_4 y_4^2.$$
(7.10)

where g_1, g_2, g_3, g_4 are positive square-free integers such that $g_1g_2g_3g_4 = Dv^2$ for some integer v. If $p^k \mid v$ then we must have $p^k \mid \gcd(g_i, g_j)$ for some $i \neq j$. In this way, since a, b are assumed to be coprime, it follows that $v \mid 2ab(b^2 - a^2)$. Write

$$n_i = \frac{g_i}{\gcd(g_i, 2ab(b^2 - a^2))},$$

for $1 \leq i \leq 4$. We easily conclude that

$$\begin{cases}
\left(\frac{2ag_2}{p}\right) = \left(\frac{(b-a)g_3}{p}\right) = \left(\frac{(a+b)g_4}{p}\right) = 1 & \text{if } p \mid n_1, \\
\left(\frac{-2ag_1}{p}\right) = \left(\frac{-(a+b)g_3}{p}\right) = \left(\frac{(b-a)g_4}{p}\right) = 1 & \text{if } p \mid n_2, \\
\left(\frac{-(b-a)g_1}{p}\right) = \left(\frac{(a+b)g_2}{p}\right) = \left(\frac{2bg_4}{p}\right) = 1 & \text{if } p \mid n_3, \\
\left(\frac{-(a+b)g_1}{p}\right) = \left(\frac{-(b-a)g_2}{p}\right) = \left(\frac{-2bg_3}{p}\right) = 1 & \text{if } p \mid n_4.
\end{cases}$$
(7.11)

Note that $n_1 \cdots n_4 \mid g_1 \cdots g_4 = Dv^2$, whence $n_1 \cdots n_4 \leqslant N$, since n_1, \ldots, n_4 are coprime to v.

In order to prove the lemma we will first focus on bounding the quantity

$$R(N) = \# \left\{ (n_1, n_2, n_3, n_4) \in \mathbb{Z}^3_{>0} : \gcd(n_1 n_2 n_3 n_4, ab(b^2 - a^2)) = 1 \\ n_i n_j \neq 1 \text{ for all } \{i, j\} \subset \{1, 2, 3, 4\} \right\}.$$

We shall deal with the case in which $n_i n_j = 1$ for some $\{i, j\} \subset \{1, 2, 3, 4\}$ at the end of the proof. Clearly, there exist $R_i \mid a^2 b^2 (b^2 - a^2)^2$, for $1 \leq i \leq 4$, such that (7.11) can be rewritten as

$$\left(\frac{R_i n_i}{p}\right) = 1 \text{ if } p \mid n_j,$$

whenever $i \neq j$. Since there are only finitely many possible R_1, R_2, R_3, R_4 given a and b, we will view R_1, R_2, R_3, R_4 as fixed. The condition on all $p \mid n_1$ can be packaged as

$$\Pi_{1} = \frac{1}{8^{\omega(n_{1})}} \prod_{p|n_{1}} \left(1 + \left(\frac{R_{2}n_{2}}{p} \right) \right) \left(1 + \left(\frac{R_{3}n_{3}}{p} \right) \right) \left(1 + \left(\frac{R_{4}n_{4}}{p} \right) \right) \\
= \frac{1}{8^{\omega(n_{1})}} \sum_{n_{1} = \prod_{S \in \mathcal{P}(\{2,3,4\})} n_{1,S}} \left(\frac{R_{2}n_{2}}{n_{1,\{2\}}} \right) \left(\frac{R_{3}n_{3}}{n_{1,\{3\}}} \right) \left(\frac{R_{4}n_{4}}{n_{1,\{4\}}} \right) \left(\frac{R_{2}R_{3}n_{2}n_{3}}{n_{1,\{2,3\}}} \right) \\
\times \left(\frac{R_{2}R_{4}n_{2}n_{4}}{n_{1,\{2,4\}}} \right) \left(\frac{R_{3}R_{4}n_{3}n_{4}}{n_{1,\{3,4\}}} \right) \left(\frac{R_{2}R_{3}R_{4}n_{2}n_{3}n_{4}}{n_{1,\{2,3,4\}}} \right),$$

where \mathcal{P} denotes the power set. We define Π_2, Π_3, Π_4 similarly, and expand the products with indexing

$$n_1 = \prod_{S \in \mathcal{P}(\{2,3,4\})} n_{1,S}, \quad n_2 = \prod_{S \in \mathcal{P}(\{1,3,4\})} n_{2,S}, \quad n_3 = \prod_{S \in \mathcal{P}(\{1,2,4\})} n_{3,S}, \quad n_4 = \prod_{S \in \mathcal{P}(\{1,2,3\})} n_{4,S}.$$

Define

$$\Phi((i, S), (j, S')) = \begin{cases} 1 & \text{if } j \in S, \\ 0 & \text{otherwise,} \end{cases}$$

and take the set of indices to be

$$\mathcal{I} = \{(i, S) : i \in \{1, 2, 3, 4\}, S \in \mathcal{P}(\{1, 2, 3, 4\} \setminus \{i\})\}.$$

Then we may write

$$R(N) = \sum_{(n_{\mathbf{u}})} \Pi_1 \Pi_2 \Pi_3 \Pi_4 = \sum_{(n_{\mathbf{u}})} \prod_{\mathbf{u} \in \mathcal{I}} \frac{1}{8^{\omega(n_{\mathbf{u}})}} \left(\frac{R_{\mathbf{u}}}{n_{\mathbf{u}}}\right) \prod_{\mathbf{u}, \mathbf{v} \in \mathcal{I}} \left(\frac{n_{\mathbf{u}}}{n_{\mathbf{v}}}\right)^{\Phi(\mathbf{u}, \mathbf{v})},$$

where $R_{\mathbf{u}}$ depends on R_1, R_2, R_3, R_4 , and the sum is over tuples of positive integers $(n_{\mathbf{u}})$ such that $\prod_{\mathbf{u}} n_{\mathbf{u}} \in \mathcal{D}(N)$ and $\gcd(\prod n_{\mathbf{u}}, ab(b^2 - a^2)) = 1$, and such that $n_{\mathbf{u}}n_{\mathbf{v}} \neq 1$ for all distinct \mathbf{u}, \mathbf{v} . We apply Theorem 6.1 with $\lambda = \frac{1}{8}$ and

$$\mathcal{J}_{i,j} = \{(i,S) \in \mathcal{I}\} \cup \{(j,S) \in \mathcal{I}\} \text{ for } \{i,j\} \subset \{1,2,3,4\}.$$

Furthermore, we take $f_{\mathbf{u}}(n) = 8^{-\omega(n)}$ and $c_{\mathbf{u}} = 1$, for all $\mathbf{u} \in \mathcal{I}$. We can check that the maximal unlinked sets have size 8 and each of them is contained in one of the $\mathcal{J}_{i,j}$. Thus the sum over \mathcal{U} vanishes. Indeed, suppose that (i_1, S_1) is unlinked to (i_2, S_2) and (i_3, S_3) , where i_1, i_2, i_3 are distinct. Then, whether or not S_1 contains i_2 is determined by whether or not i_1 is contained in S_2 . Similarly, whether or not S_1 contains i_3 is determined by whether or not i_1 is in i_2 . This only leaves 2 possible choices for i_2 , given i_3 and i_4 . Hence the size of any unlinked indices, not of the form i_2 , is bounded by i_3 . Therefore, on putting i_4 and i_4 it follows from Theorem 6.1 that the sum is bounded by i_4 by i_4 is i_4 .

It remains to deal with the remaining cases not considered in R(N), in which two of n_1, n_2, n_3, n_4 are equal to 1. We assume that $n_i = n_j = 1$, with $\{i, j, k, l\} = \{1, 2, 3, 4\}$. Take the difference between the equations in (7.10) that are associated to n_i and n_j , and then the difference between those associated to n_k and n_k , in order to get

$$g_i y_i^2 - g_j y_j^2 = c_i - c_j,$$

$$q_k y_k^2 - q_l y_l^2 = c_k - c_l,$$

where $c_1 = -a, c_2 = a, c_3 = -b, c_4 = b$. Notice that $g_i, g_j \mid ab(b^2 - a^2)$ because $n_i = n_j = 1$. Therefore we can apply Lemma 7.6 to get the overall bound $O(\sqrt{N}(\log N)^2)$ in this case.

7.4. Conclusion.

Proof of Lemma 7.4. We apply Lemma 7.5. The exceptions in (7.8) are dealt with in Lemma 7.7 and Lemma 7.8.

Proof of Proposition 7.2. Combine Lemma 7.3 and Lemma 7.4.

Proof of Theorem 7.1. Apply Proposition 7.2 with $\kappa = 13$. For the points $(x, y) \in E_D^*(\mathbb{Z})$ with small gcd(x, D), we observe that $(X, Y) = (9x - 3(A + B)D, 27y) \in \mathbb{Z}^2$ gives a non-trivial integral point on the short Weierstrass model

$$Y^{2} = X^{3} - 27(A^{2} + B^{2} - AB)D^{2}X - 27(2B - A)(B - 2A)(A + B)D^{3}.$$

Moreover, the relation 9x = X + 3(A + B)D implies that $gcd(X, D) \mid 9 gcd(x, D)$. We may therefore apply Lemma 5.6 with $K = 9N(\log N)^{-\kappa}$ to bound the number of integral points with $gcd(x, D) \leq N(\log N)^{-\kappa}$. We conclude that

$$\#\left\{D \in \mathcal{D}^+(N): \begin{array}{l} \gcd(x,D) \leqslant N(\log N)^{-\kappa} \\ \text{for some } (x,y) \in E_D^*(\mathbb{Z}) \end{array}\right\} \ll N(\log N)^{-\frac{1}{2}\kappa+6},$$

which proves the desired upper bound for $D \in \mathcal{D}^+(N)$.

To treat negative $D \in \mathcal{D}(N)$, we instead consider the family

$$E_D: y^2 = x(x - (B - A)D)(x - BD),$$

with $D \in \mathcal{D}^+(N)$ Thus the role of A is replaced by B - A, and the argument runs as before, leading to the same conclusion.

8. Quadratic twists with partial two-torsion

To prove Theorem 2.3, we consider instead the model

$$E_D: y^2 = x(x^2 + ADx + BD^2),$$
 (8.1)

for integers A, B such that $A^2 - 4B \notin \mathbb{Q}^2$. For such curves, the only two-torsion points are the point at infinity and (0,0), so

$$E_D^*(\mathbb{Z}) = E_D(\mathbb{Z}) \setminus \{(0,0)\} = \{(x,y) \in \mathbb{Z}^2 : y^2 = x(x^2 + ADx + BD^2), \ y \neq 0\}.$$

The lower bound in Theorem 2.3 follows from Lemma 5.8, whereas the upper bound will follow from the next result.

Theorem 8.1. Let E_D be given by (8.1), for $A, B \in \mathbb{Z}$ such that $A^2 - 4B \notin \mathbb{Q}^2$. If B < 0 or $B \in \mathbb{Q}^2$, then

$$\# \{D \in \mathcal{D}(N) : E_D^*(\mathbb{Z}) \neq \emptyset \} \ll N(\log N)^{-\frac{1}{8}} \log \log N.$$

If B > 0 and $B \notin \mathbb{Q}^2$, then

$$\# \left\{ D \in \mathcal{D}(N) : \begin{array}{l} xB \notin \mathbb{Q}^2 \text{ or } \gcd(x,D) < N(\log N)^{-\frac{49}{4}} \\ D \in \mathcal{D}(N) : \text{ or } x < \exp(N(\log N)^{-\frac{99}{8}}) \\ \text{ for some } (x,y) \in E_D^*(\mathbb{Z}) \end{array} \right\} \ll N(\log N)^{-\frac{1}{8}} \log \log N.$$

The implied constants depend at most on A and B.

Conjecture 1.1 pertains to elliptic curves in short Weierstrass form. After a suitable change of variables, the equation (8.1) defining E_D can be transformed into an equation of the form $y^2 = x^3 + A'x + B'$, with $A', B' \in \mathbb{Z}$ such that $A' \ll D^2$ and $B' \ll D^3$. But then it follows from Conjecture 1.1 that there exists constants C > 0 and $\varepsilon > 0$ such that any $(x, y) \in E_D^*(\mathbb{Z})$ satisfies $x < \exp(CN^{1-\varepsilon})$, if $D \in \mathcal{D}(N)$. That Theorem 2.3 follows from Theorem 8.1 is now obvious.

Since Lemma 5.6 will be enough to deal with points with small gcd(x, D), we will focus our attention on the case when gcd(x, D) is large.

Proposition 8.2. Let E_D be given by (8.1), for $A, B \in \mathbb{Z}$ such that $A^2 - 4B \notin \mathbb{Q}^2$. Let $\kappa > 0$. Then

$$\#\left\{D\in\mathcal{D}^+(N): \begin{array}{l} \gcd(x,D)\geqslant N(\log N)^{-\kappa} \ and \ xB\notin\mathbb{Q}^2\\ for \ some \ (x,y)\in E_D^*(\mathbb{Z}) \end{array}\right\}\ll N(\log N)^{-\frac{1}{8}}\log\log N,$$

where implied constant depends at most on A, B and κ .

Moving to the two-division field $K := \mathbb{Q}(\sqrt{A^2 - 4B})$ of E_D , note that we can rewrite the equation as

$$y^2 = x(x - \alpha D)(x - \overline{\alpha}D),$$

where

$$\alpha := \frac{-A + \sqrt{A^2 - 4B}}{2}$$
 and $\overline{\alpha} := \frac{-A - \sqrt{A^2 - 4B}}{2}$.

Over \mathbb{R} , the curve E_D has two connected components if $A^2-4B>0$ and one if $A^2-4B<0$. If $A^2-4B<0$, the value of $x^2+ADx+BD^2$ is always positive and it follows that also x>0. If $A^2-4B>0$, on the other hand, then we must have $x>-\max\{|\alpha|,|\bar{\alpha}|\}D$ for any real point on E_D .

Suppose $(x,y) \in E_D^*(\mathbb{Z})$ and let $g := \gcd(x,D)$. We shall follow the opening steps in the proof of Proposition 7.2. Write $x = g\tilde{x}$ and $D = g\tilde{D}$, so that $y = g^2\tilde{y}$ for some integer \tilde{y} , as before. Then substituting this back into the equation, we obtain

$$g\tilde{y}^2 = \tilde{x}(\tilde{x}^2 + A\tilde{D}\tilde{x} + B\tilde{D}^2) = \tilde{x}(\tilde{x} - \alpha\tilde{D})(\tilde{x} - \overline{\alpha}\tilde{D}).$$

Observe that since $gcd(\tilde{x}, \tilde{D}) = 1$, we have

$$\delta \coloneqq \gcd(\tilde{x}, \tilde{x}^2 + A\tilde{D}\tilde{x} + B\tilde{D}^2) \mid B.$$

Thus we can factor \tilde{x} and $\tilde{x}^2 + A\tilde{D}\tilde{x} + B\tilde{D}^2$ over \mathbb{Q} as

$$\tilde{x} = g_1 \delta y_1^2 \tag{8.2}$$

$$(\tilde{x} - \alpha \tilde{D})(\tilde{x} - \overline{\alpha}\tilde{D}) = \tilde{x}^2 + A\tilde{D}\tilde{x} + B\tilde{D}^2 = g_2 \delta y_2^2, \tag{8.3}$$

where g_1, g_2, y_1, y_2 are integers such that $g_1g_2 = g$ and $y_1y_2 = \tilde{y}$. Substituting (8.2) into (8.3), we obtain

$$(g_1\delta y_1^2)^2 + A\tilde{D}g_1\delta y_1^2 + B\tilde{D}^2 = g_2\delta y_2^2.$$
(8.4)

In the next result, which is an analogue of Lemma 7.3, we bound the number of integral points that lie in the compact component when there are two connected components.

Lemma 8.3. Fix $\kappa > 0$. Let $A, B \in \mathbb{Z}$ such that $A^2 - 4B \notin \mathbb{Q}^2$ and $A^2 - 4B > 0$. Then

$$\sum_{D \in \mathcal{D}^+(N)} \# \left\{ (x,y) \in E_D^*(\mathbb{Z}) : \begin{array}{l} x < \max\{|\alpha|, |\overline{\alpha}|\}D \text{ and } \\ \gcd(x,D) \geqslant N(\log N)^{-\kappa} \end{array} \right\} \ll (\log N)^{2\kappa},$$

where implied constant depends at most on A, B and κ .

Proof. For such points $(x,y) \in E_D^*(\mathbb{Z})$ with $D = \gcd(x,D)\tilde{D}$, we have

$$|\tilde{x}| < \max\{|\alpha|, |\overline{\alpha}|\} \tilde{D} \ll (\log N)^{\kappa}.$$

There are $\ll (\log N)^{2\kappa}$ choices of \tilde{x} and \tilde{D} , which can be used to recover square-free g_1 and g_2 by (8.2) and (8.3), up to δ , since $y_1, y_2 \neq 0$ for non-torsion points.

When $A^2-4B<0$, the value of $x^2+ADx+BD^2$ is always positive. Thus g_2 and hence also g_1 must be positive. If $A^2-4B>0$, on the other hand, it is possible that both g_1,g_2 are negative. This happens precisely when $x=g\tilde{x}=g_2g_1^2\delta y_1^2$ is negative, but such points are handled by Lemma 8.3. Thus, in what follows, we can restrict our attention to the case in which g_1 and g_2 are both positive.

We collect from (8.4) the local solubility conditions at the primes dividing g_1 and g_2 , but not $B(A^2 - 4B)$. These may be written

$$\begin{cases} \left(\frac{B\delta g_2}{p}\right) = 1 & \text{if } p \mid g_1 \text{ and } p \nmid B, \\ \left(\frac{A^2 - 4B}{p}\right) = 1 & \text{if } p \mid g_2 \text{ and } p \nmid A^2 - 4B. \end{cases}$$

In the above we have used that $p \mid g_1g_2$ implies $p \nmid \tilde{D}$, because $D = g_1g_2\tilde{D}$ is square-free. For each $p \mid g_2$ and $p \nmid B(A^2 - 4B)$, the condition $\left(\frac{A^2 - 4B}{p}\right) = 1$ implies that p splits in K/\mathbb{Q} . From (8.3), we see that there is a prime \mathfrak{p} in \mathcal{O}_K above p such that $\tilde{x} \equiv \alpha \tilde{D} \mod \mathfrak{p}$, so substituting this into (8.2) yields $g_1 \delta y_1^2 \equiv \alpha \tilde{D} \mod \mathfrak{p}$, whence

$$\left(\frac{g_1\delta\alpha\tilde{D}}{\mathfrak{p}}\right) = 1.$$

Since p splits in K/\mathbb{Q} , we have

$$\left(\frac{g_1\delta\tilde{D}}{\mathfrak{p}}\right) = \left(\frac{g_1\delta\tilde{D}}{p}\right)$$

and

$$\left(\frac{B}{p}\right) = \left(\frac{B}{\mathfrak{p}}\right) = \left(\frac{\alpha\overline{\alpha}}{\mathfrak{p}}\right) = \left(\frac{g_1\delta\alpha\tilde{D}}{\mathfrak{p}}\right) \left(\frac{g_1\delta\overline{\alpha}\tilde{D}}{\mathfrak{p}}\right).$$

Therefore, if $\left(\frac{B}{p}\right) = -1$, then $\tilde{x} \equiv \alpha \tilde{D} \mod \mathfrak{p}$ is automatically satisfied by one of the two primes above p. If instead $\left(\frac{B}{p}\right) = 1$, then it is clear that $\left(\frac{\alpha}{\mathfrak{p}}\right)$ does not depend on the choice of prime above p. Define $L := K(\sqrt{\alpha})$. For any prime p that splits completely in $K(\sqrt{B})/\mathbb{Q}$, we define

$$\left(\frac{L/\mathbb{Q}}{p}\right) \coloneqq \left(\frac{\alpha}{\mathfrak{p}}\right),\,$$

viewed as an Artin symbol in $\operatorname{Gal}(L/\mathbb{Q})$, taking values in $\operatorname{Gal}(L/K(\sqrt{B})) \cong \mathbb{F}_2$. Next, we write

$$g_1 = n_1 \cdot \gamma_1$$
 and $g_2 = n_2 \cdot \gamma_2$,

where $\gamma_1 = \gcd(g_1, 2B(A^2 - 4B))$ and $\gamma_2 = \gcd(g_2, 2B(A^2 - 4B))$. Let

$$\mathcal{S}_d := \left\{ n \in \mathcal{D}^+ : 2 \nmid n, \ \left(\frac{d}{p}\right) = 1 \text{ for all } p \mid n \right\}.$$

Also define

$$\omega_d(n) := \#\left\{p \mid n : \left(\frac{d}{p}\right) = 1\right\}.$$

Fix a choice of $\delta \mid B$, $\gamma_1 \gamma_2 \mid 2B(A^2 - 4B)$, and \tilde{D} . Define

$$R_{21} = \tilde{D}\delta\gamma_1$$
 and $R_{12} = B\delta\gamma_2$.

We would like to count the number of pairs (n_1, n_2) such that $n_1 n_2 \gamma_1 \gamma_2 \tilde{D} \in \mathcal{D}^+(N)$, with $\gcd(n_1 n_2, 2B(A^2 - 4B)) = 1$ and $n_2 \in \mathcal{S}_{A^2 - 4B}$, and such that

$$\begin{cases}
\left(\frac{R_{12}n_2}{p}\right) = 1 & \text{if } p \mid n_1, \\
\left(\frac{L/\mathbb{Q}}{p}\right)\left(\frac{R_{21}n_1}{p}\right) = 1 & \text{if } p \mid n_2 \text{ and } \left(\frac{B}{p}\right) = 1.
\end{cases}$$
(8.5)

For $n_1 \in \mathcal{D}^+$ and $n_2 \in \mathcal{S}_{A^2-4B}$, we note that the expression

$$\prod_{p|n_1} \frac{1}{2} \left(1 + \left(\frac{R_{12}n_2}{p} \right) \right) \prod_{\substack{p|n_2 \\ \left(\frac{B}{p} \right) = 1}} \frac{1}{2} \left(1 + \left(\frac{L/\mathbb{Q}}{p} \right) \left(\frac{R_{21}n_1}{p} \right) \right)$$
(8.6)

is equal to 1 if (8.5) is satisfied by n_1, n_2 , and 0 otherwise.

Lemma 8.4. Let $\kappa > 0$. Fix positive integers $\delta \mid B$, $\gamma_1 \gamma_2 \mid 2B(A^2 - 4B)$. Take a square-free positive integer $\tilde{D} \leqslant (\log N)^{\kappa}$ that is coprime to $\gamma_1 \gamma_2$. We have

$$\# \left\{ D \in \mathcal{D}^{+}(N) : \begin{array}{l}
n_{1}, n_{2} \geqslant 1, \ n_{1}n_{2}\gamma_{1}\gamma_{2}\tilde{D} = D, \ (8.5) \ holds \\
\gcd(n_{1}n_{2}, 2B(A^{2} - 4B)) = 1 \\
n_{2} \neq 1 \ if \ R_{12} \in \mathbb{Q}^{2}
\end{array} \right\} \ll \frac{N}{\tilde{D}} (\log N)^{-\frac{1}{8}},$$

where implied constant depends at most on A, B and κ .

Proof. Let R(N) denote the quantity that is to be estimated. Summing (8.6) over (n_1, n_2) such that $n_2 \neq 1$ if $R_{12} \in \mathbb{Q}^2$, and then expanding the sum, we easily arrive at the expression

$$R(N) = \sum_{\substack{n_{10}, n_{12}, n_{20}, n_{21} \\ n_{20} n_{21} \in S_{A^2 - 4B} \\ n_{21} \in S_B}} \frac{1}{2^{\omega(n_{10}n_{12}) + \omega_B(n_{20}n_{21})}} \left(\frac{R_{12}n_{20}n_{21}}{n_{12}}\right) \left(\frac{L/\mathbb{Q}}{n_{21}}\right) \left(\frac{R_{21}n_{10}n_{12}}{n_{21}}\right),$$

where the sum is over all positive integers n_{10} , n_{12} , n_{20} , n_{21} such that

$$n_{10}n_{12}n_{20}n_{21}\gamma_1\gamma_2\tilde{D} \in \mathcal{D}^+(N),$$

with $gcd(n_{10}n_{12}n_{20}n_{21}, 2B(A^2 - 4B)) = 1$, $n_{20} \in \mathcal{S}_{A^2-4B}$, $n_{21} \in \mathcal{S}_B \cap \mathcal{S}_{A^2-4B}$, and additionally $n_{20}n_{21} \neq 1$ if $R_{12} \in \mathbb{Q}^2$.

We plan to apply Theorem 6.1 to estimate R(N). In order to facilitate this we define

$$R_{10} = R_{20} = 1.$$

Then, we shall apply Theorem 6.1 with the following parameters. Firstly, we shall take

$$\mathcal{I} = \{10, 12, 20, 21\}, \quad \mathcal{J} = \begin{cases} \{10, 12\} & \text{if } R_{12} \text{ is a square,} \\ \varnothing & \text{otherwise,} \end{cases}$$

and

$$\Phi(kl, ij) = \begin{cases} 1 & \text{if } k \neq i \text{ and } j \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

The relevant arithmetic functions are

$$f_{10}(n) = f_{12}(n) = \begin{cases} 2^{-\omega(n)} & \text{if } \gcd(n, 2B(A^2 - 4B)) = 1, \\ 0 & \text{otherwise,} \end{cases}$$

$$f_{20}(n) = \begin{cases} 2^{-\omega_B(n)} & \text{if } n \in \mathcal{S}_{A^2 - 4B} \text{ and } \gcd(n, 2B(A^2 - 4B)) = 1, \\ 0 & \text{otherwise,} \end{cases}$$

$$f_{21}(n) = \begin{cases} 2^{-\omega_B(n)} & \text{if } n \in \mathcal{S}_B \cap \mathcal{S}_{A^2 - 4B} \text{ and } \gcd(n, 2B(A^2 - 4B)) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

The relevant charaters are

$$\chi_{10}(\cdot) = \chi_{20}(\cdot) = 1, \quad \chi_{12}(\cdot) = \left(\frac{R_{12}}{\cdot}\right), \quad \chi_{21}(\cdot) = \left(\frac{L/\mathbb{Q}}{\cdot}\right) \left(\frac{R_{21}}{\cdot}\right),$$

so that $K_{10} = K_{20} = K_{12} = \mathbb{Q}$, $K_{21} = K$, $\alpha_{10} = \alpha_{20} = 1$, $\alpha_{12} = R_{12}$ and $\alpha_{21} = \alpha R_{21}$, But then we may take $\lambda = \frac{1}{2}$ and

$$c_{10} = c_{12} = 1$$
, $c_{20} = c_{21} = 2B(A^2 - 4B)$.

We easily check that the maximal unlinked sets are

$$\{10, 12\}, \{10, 20\}, \{12, 21\}, \{20, 21\}.$$

Taking M=2, we see that the error term in Theorem 6.1 becomes $O(\frac{N}{\tilde{D}}(\log N)^{-\frac{1}{2}+\varepsilon})$.

The sum in the main term in Theorem 6.1 is taken over all \mathcal{U} satisfying (P1)–(P4). Thus we need to check which maximal unlinked sets are admissible (so that they satisfy (P3) and (P4)) and yet are not contained in \mathcal{J} . Since $c_{12} = 1$, it follows from (P3) that the set $\{10, 12\}$ is only admissible if R_{12} is a square. Therefore, the sum in the main term is only over $\mathcal{U} \in \{\{10, 20\}, \{12, 21\}, \{20, 21\}\}$. (Indeed, if R_{12} is not a square then $\{10, 12\}$ is not admissible and it shouldn't appear in the main term; alternatively, if R_{12} is a square then $\{10, 12\}$ is admissible but contained in \mathcal{J} .) Taking $\varepsilon = \frac{5}{8}$, we may deduce that

$$R(N) = M(N) + O\left(\frac{N}{\tilde{D}}(\log N)^{-\frac{1}{8}}\right),$$

where

$$M(N) \ll \sum_{\mathcal{U}} \sum_{\substack{(D_i)_{i \in \mathcal{U}}}} \prod_{i \in \mathcal{U}} f_i(D_i)$$

$$\ll \sum_{\substack{n_{10}, n_{20} \\ n_{10}n_{20} \leqslant N/\tilde{D} \\ n_{20} \in \mathcal{S}_{A^2 - 4B}}} \frac{1}{2^{\omega(n_{10}) + \omega_B(n_{20})}} + \sum_{\substack{n_{12}, n_{21} \\ n_{12}n_{21} \leqslant N/\tilde{D} \\ n_{21} \in \mathcal{S}_{A^2 - 4B} \cap \mathcal{S}_B}} \frac{1}{2^{\omega(n_{12}) + \omega_B(n_{21})}} + \sum_{\substack{n_{20}, n_{21} \\ n_{20}n_{21} \leqslant N/\tilde{D} \\ n_{20}n_{21} \in \mathcal{S}_{A^2 - 4B} \\ n_{20} \in \mathcal{S}_{A^2 - 4B}}} \frac{1}{2^{\omega_B(n_{20}n_{21})}}.$$

On appealing to Lemma 6.5, we easily deduce that

$$M(N) \ll \frac{N}{\tilde{D}} \left((\log N)^{-\frac{1}{8}} + (\log N)^{-\frac{1}{4}} + (\log N)^{-\frac{3}{8}} \right) \ll \frac{N}{\tilde{D}} (\log N)^{-\frac{1}{8}},$$

which completes the proof of the lemma.

Let us comment briefly on the condition $n_2 \neq 1$ if $R_{12} \in \mathbb{Q}^2$, appearing in the counting function R(N) in the proof of Lemma 8.4. Dropping this condition would amount to taking \mathcal{J} to be the empty set in the proof. But then we would obtain a contribution from the admissible set $\{10,12\}$, which takes the shape $\sum_{n_{10}n_{12}\leqslant N/\tilde{D}} 2^{-\omega(n_{10}n_{12})}$. This sum has order $\frac{N}{\tilde{D}}\sqrt{\log N}$, which is much larger than the upper bound in Lemma 8.4.

Proof of Proposition 8.2. Lemma 8.3 allows us to restrict to points $(x, y) \in E_D^*(\mathbb{Z})$ that satisfy x > 0. Next, we sum the bound from Lemma 8.4 over $\tilde{D} \leq (\log N)^{\kappa}$, and over all choices of $\delta, \gamma_1, \gamma_2$. The integral points $(x, y) \in E_D^*(\mathbb{Z})$ that have not been handled satisfy $n_2 = 1$ and $R_{12} \in \mathbb{Q}^2$, hence $Bx = Bgg_1\delta y_1^2 = Bg_2\delta(g_1y_1)^2 = R_{12}(g_1y_1)^2$ is a square. This proves Proposition 8.2.

8.1. Exceptional points. To complete the proof of Theorem 8.1, it remains to deal with the set of exceptional points.

Lemma 8.5. Let $\kappa, \tau > 0$. If B < 0 or $B \in \mathbb{Q}^2$, then

$$\sum_{D \in \mathcal{D}^+(N)} \# \left\{ (x, y) \in E_D^*(\mathbb{Z}) : \gcd(x, D) \geqslant N(\log N)^{-\kappa} \text{ and } xB \in \mathbb{Q}^2 \right\} \ll (\log N)^{2\kappa}.$$

If B > 0 and $B \notin \mathbb{Q}^2$, then

$$\sum_{D \in \mathcal{D}^+(N)} \# \left\{ (x, y) \in E_D^*(\mathbb{Z}) : \begin{array}{l} \gcd(x, D) \geqslant N(\log N)^{-\kappa} \\ xB \in \mathbb{Q}^2 \\ x < \exp(N(\log N)^{-\kappa - \tau}) \end{array} \right\} \ll N(\log N)^{-\tau} (\log \log N)^{\frac{1}{2}}.$$

The implied constants depend at most on A, B and κ .

Proof. Lemma 8.3 allows us to restrict to points $(x,y) \in E_D^*(\mathbb{Z})$ that satisfy x > 0, so suppose that g_1, g_2 are positive integers in the notation of (8.3). Since $Bx = Bgg_1\delta y_1^2 = Bg_2\delta(g_1y_1)^2$ is a square, we deduce that g_2 is the squarefree part of B/δ and B > 0.

Recall that $gcd(\tilde{x}, \tilde{D}) = 1$. Hence the greatest common divisor of the ideals $(\tilde{x} - \alpha \tilde{D})$ and $(\tilde{x} - \overline{\alpha}\tilde{D})$ must divide $2\sqrt{A^2 - 4B}$. But then, in the light of (8.3), we may write

$$\tilde{x} - \alpha \tilde{D} = \mathfrak{ab}^2$$

for some ideals $\mathfrak{a} \mid 2B\sqrt{A^2-4B}$ and \mathfrak{b} of \mathcal{O}_K . Fix a representative for each ideal class of \mathcal{O}_K . Take \mathfrak{c} to be the representative for the ideal class of \mathfrak{b} . Then $\mathfrak{b}/\mathfrak{c}$ must be a principal fractional ideal. Therefore we may take $\mu \in \mathcal{O}_K$ and $\xi \in K$ such that $\mu \mathcal{O}_K = \mathfrak{a}\mathfrak{c}^2$ and $\xi \mathcal{O}_K = \mathfrak{b}\mathfrak{c}^{-1}$. Note that, given A and B, there are only finitely many possible μ . Then

$$\tilde{x} - \alpha \tilde{D} = \mu \xi^2. \tag{8.7}$$

Taking conjugates in K/\mathbb{Q} , we obtain

$$\tilde{x} - \overline{\alpha}\tilde{D} = \overline{\mu}\overline{\xi}^2. \tag{8.8}$$

Putting this back into (8.3), we see that $\overline{\mu}\mu(\overline{\xi}\xi)^2 = g_2\delta y_2^2 \in B \cdot \mathbb{Q}^2$. Therefore $\mathbb{Q}(\sqrt{\overline{\mu}\mu}) = \mathbb{Q}(\sqrt{B})$. Taking the difference of (8.7) and (8.8), we have

$$\overline{\mu}\overline{\xi}^2 - \mu \xi^2 = \alpha \tilde{D} - \overline{\alpha}\tilde{D} = \tilde{D}\sqrt{A^2 - 4B}.$$

Squaring gives

$$(\overline{\mu}\overline{\xi}^2 + \mu\xi^2)^2 - 4\overline{\mu}\mu(\overline{\xi}\xi)^2 = \tilde{D}^2(A^2 - 4B).$$

Let $\eta = |\overline{\mu}\overline{\xi}^2 + \mu\xi^2| + 2\sqrt{\overline{\mu}\mu}|\overline{\xi}\xi|$ and $\eta' = |\overline{\mu}\overline{\xi}^2 + \mu\xi^2| - 2\sqrt{\overline{\mu}\mu}|\overline{\xi}\xi|$, which are both in $\mathcal{O}_{\mathbb{Q}(\sqrt{B})}$ since $\overline{\mu}\overline{\xi}^2$, $\mu\xi^2 \in \mathcal{O}_K$ implies that $\overline{\mu}\overline{\xi}^2 + \mu\xi^2 \in \mathbb{Z}$ and $\overline{\mu}\mu(\overline{\xi}\xi)^2 \in \mathbb{Z}$. Given \tilde{D} and some $\delta \mid B$, each (η, η') can only correspond to at most two pairs of (x, D). Indeed, observe that $(\eta - \eta')^2 = 16\overline{\mu}\mu(\overline{\xi}\xi)^2 = 16g_2\delta y_2^2$, so (8.3) allows us to recover \tilde{x} as one of the two solutions to the quadratic equation, and hence g_1 from (8.2). Therefore it suffices to bound the number of η that satisfy the equation

$$\eta \eta' = \tilde{D}^2 (A^2 - 4B)$$

over $\mathbb{Q}(\sqrt{B})$.

First suppose B > 0 is a square and note that $\tau(d^2) \leqslant 3^{\omega(d)}$, for any $d \in \mathcal{D}^+$. We deduce that $\eta \in \mathbb{Z}$ divides $(A - 4B^2)\tilde{D}^2$, so there are $O(3^{\omega(\tilde{D})})$ choices for η . Summing over all $\tilde{D} \leqslant (\log N)^{\kappa}$, the contribution is bounded by $\ll (\log N)^{2\kappa}$, by Lemma 6.5.

Suppose next that B>0 is not a square. In this case η' is the conjugate of η in $\mathbb{Q}(\sqrt{B})$. There are $O(3^{\omega(\tilde{D})})$ choices of ideal $\mathfrak{d}=\eta\mathcal{O}_{\mathbb{Q}(\sqrt{B})}$ with norm $\tilde{D}^2|A^2-4B|$. Fixing the smallest generator β of \mathfrak{d} such that $\beta>1$, we see that η must be of the form $\beta\varepsilon^k$, where $k\geqslant 0$ is an integer and ε denotes the fundamental unit of $\mathbb{Q}(\sqrt{B})$. By assumption $1<\eta\ll x+\tilde{D}\ll \exp(N(\log N)^{-\kappa-\tau})$. Thus there are $O(N(\log N)^{-\kappa-\tau})$ possible η given each \mathfrak{d} . We claim that any $p\mid \tilde{D}$ satisfies $\left(\frac{B}{p}\right)=1$ or $p\mid B$. Indeed, if $p\mid \tilde{D}$ and $p\nmid B$, then it follows from (8.3) that $g_2\delta$ is a square modulo p, which in turn implies that B is

a square modulo p, since the first paragraph of the proof ensures that $Bg_2\delta$ is a square. Putting everything together, the total contribution is found to be

$$\ll N(\log N)^{-\kappa-\tau} \sum_{\substack{\tilde{D} \leqslant (\log N)^{\kappa} \\ p|\tilde{D} \Rightarrow \left(\frac{B}{p}\right) \neq -1}} 3^{\omega(\tilde{D})} \ll N(\log N)^{-\tau} (\log\log N)^{\frac{1}{2}},$$

by Lemma 6.5.

8.2. Conclusion.

Proof of Theorem 8.1. We apply Proposition 8.2 and Lemma 8.5 with $\kappa = \frac{49}{4}$ and $\tau = \frac{1}{8}$. We are then left with the points with $\gcd(x,D) < N(\log N)^{-\kappa}$, which we will handle with Lemma 5.6. Transforming the integral points $(x,y) \in E_D^*(\mathbb{Z})$ to the integral points $(X,Y) = (9x + 3AD, 27y) \in \mathbb{Z}^2$ on the short Weierstrass model

$$Y^2 = X^3 + 27(3B - A^2)x + 27A(2A^2 - 9B),$$

allows us to apply Lemma 5.6 with $K = 9N(\log N)^{-\kappa}$. It follows that

$$\#\left\{D \in \mathcal{D}^+(N): \begin{array}{l} \gcd(x,D) < N(\log N)^{-\kappa} \\ \text{for some } (x,y) \in E_D^*(\mathbb{Z}) \end{array}\right\} \ll N(\log N)^{-\frac{1}{2}\kappa+6}.$$

This shows that the contribution from those $D \in \mathcal{D}^+(N)$ fits into the upper bound.

For the contribution from $D \in \mathcal{D}^-(N)$, we simply replace A by -A and consider instead $E_D: y^2 = x(x^2 - ADx + BD^2)$ with $D \in \mathcal{D}^+(N)$.

References

- [1] L. Alpöge, The average number of integral points on elliptic curves is bounded. *Preprint*, 2014. arXiv:1412.1047.
- [2] L. Alpöge and W. Ho, The second moment of the number of integral points on elliptic curves is bounded. *Preprint*, 2022. arXiv:1807.03761.
- [3] M. A. Bean, An isoperimetric inequality for the area of plane regions defined by binary forms. *Compositio Math.* **92** (1994), 115–131.
- [4] T. D. Browning, The density of rational points on a certain singular cubic surface. *J. Number Theory* **119** (2006), 242–283.
- [5] Y. Bugeaud, Effective simultaneous rational approximation to pairs of real quadratic numbers. *Mosc. J. Comb. Number Theory* **9** (2020), 353–360.
- [6] A. Chambert-Loir and Y. Tschinkel, Igusa integrals and volume asymptotics in analytic and adelic geometry. *Confluentes Math.* **2** (2010), 351–429.
- [7] S. Chan, The average number of integral points on the congruent number curves. *Preprint*, 2023. arXiv:2112.01615.
- [8] S. Chan, Integral points on cubic twists of Mordell curves. Math. Ann., to appear.
- [9] J. E. Cremona, Reduction of binary cubic and quartic forms. LMS J. Comput. Math. 2 (1999), 64–94.
- [10] É. Fouvry and J. Klüners, On the 4-rank of class groups of quadratic number fields. *Invent. Math.* **167** (2007), 455–513.
- [11] J. Franke, Y. I. Manin and Y. Tschinkel, Rational points of bounded height on Fano varieties. *Invent. Math.* 95 (1989), 421–435.
- [12] L. J. Goldstein, A generalization of the Siegel-Walfisz theorem. Trans. Amer. Math. Soc. 149 (1970), 417–429.
- [13] A. Granville, Rational and integral points on quadratic twists of a given hyperelliptic curve. *Int. Math. Res. Not. IMRN* (2007), no. 8, Art. ID 027, 24 pp.
- [14] L. Hajdu and T. Herendi, Explicit bounds for the solutions of elliptic equations with rational coefficients. J. Symbolic Computation 25 (1998), 361–366.
- [15] G. H. Hardy and S. Ramanujan, The normal number of prime factors of a number n. Quart. J. Math. 48 (1917), 76–92.
- [16] D. R. Heath-Brown, A mean value estimate for real character sums. Acta Arith. 72 (1995), 235–275.

- [17] D. R. Heath-Brown, Diophantine approximation with square-free numbers. Math. Z. (1984) 187, 335–344.
- [18] D. R. Heath-Brown, The size of Selmer groups for the congruent number problem. *Invent. Math.* 111 (1993), 171–195.
- [19] D. R. Heath-Brown, The size of Selmer groups for the congruent number problem. II. *Invent. Math.* 118 (1994), 331–370.
- [20] M. Hindry and J. H. Silverman, The canonical height and integral points on elliptic curves. *Invent.* Math. 93 (1988), 419–450.
- [21] M. N. Huxley, A note on polynomial congruences. In *Recent progress in analytic number theory*, Vol. 1 (Durham, 1979), pp 193–196, Academic Press, London–New York, 1981.
- [22] S. Lang, Conjectured Diophantine estimates on elliptic curves. Arithmetic and geometry, Vol. I, 155–171, Progr. Math. 35, Birkhäuser Boston, Boston, MA, 1983.
- [23] P. Le Boudec, Affine congruences and rational points on a certain cubic surface. Algebra & Number Theory 8 (2014), 1259–1296.
- [24] L. J. Mordell, *Diophantine equations*. Pure and Applied Mathematics 30, Academic Press, London-New York, 1969.
- [25] W. Schmidt, Thue's equation over function fields. J. Austral. Math. Soc. 25 (1978), 385-422.
- [26] J.-P. Serre, Lectures on $N_X(p)$. CRC Research Notes in Mathematics 11, CRC Press, Boca Raton, FL. 2012.
- [27] P. Shiu, A Brun-Titchmarsh theorem for multiplicative functions. J. reine angew. Math. 313 (1980), 161–170.
- [28] A. Smith, The distribution of ℓ^{∞} -Selmer groups in degree ℓ twist families II. *Preprint*, 2023. arXiv:2207.05143.
- [29] J. L. Thunder, Decomposable form inequalities. Ann. of Math. 153 (2001), 767–804.
- [30] E. Wirsing, Das asymptotische Verhalten von Summen über multiplikative Funktionen. *Math. Ann.* **143** (1961), 75–102.
- [31] S. Y. Xiao, Power-free values of binary forms and the global determinant method. *Int. Math. Res. Not. IMRN* **16** (2017), 5078–5135.

IST Austria, Am Campus 1, 3400 Klosterneuburg, Austria

Email address: tdb@ist.ac.at

Email address: stephanie.chan@ist.ac.at