Quadratic Fields Admitting Elliptic Curves with Rational j-Invariant and Good Reduction Everywhere

Benjamin Matschke and Abhijit S. Mudigonda

Abstract. Clemm and Trebat-Leder (2014) proved a coarse asymptotic lower bound for the number of quadratic number fields with discriminant bounded by x over which there exist elliptic curves with good reduction everywhere and rational j-invariant. In this paper, we assume the abc-conjecture to show a fine asymptotic $\sim cx\log^{-1/2}(x)$ for this number in the real and imaginary case. Under a different hypothesis, we show that the constant c is greater in the real quadratic case than in the imaginary quadratic case, confirming an experimentally observed bias. Our method has three ingredients:

(1) We make progress towards a conjecture of Granville: Given a fixed elliptic curve $E/\mathbb{Q}$ with short Weierstrass equation $y^2 = f(x)$ for reducible $f \in \mathbb{Q}[x]$, we show that the number of integers d, $|d| \leq D$, for which the quadratic twist $dy^2 = f(x)$ has an integral non-2-torsion point is at most $D^{2/3+o(1)}$, assuming the abc-conjecture.

(2) We apply the Selberg–Delange method to obtain a Tauberian theorem which allows us to count integers which satisfy certain congruences while also being divisible only by certain primes.

(3) We show that for a polynomially sparse subset of the natural numbers, the number of pairs of elements with least common multiple at most x is $O(x^{1-\epsilon})$ for some $\epsilon > 0$. We also exhibit a matching lower bound.

1. Introduction

An elliptic curve defined over a number field K is said to have *good reduction everywhere* if it has good reduction at every prime ideal of the ring of integers of K. Tate showed that there are no such elliptic curves over $\mathbb{Q}$ [25], but this is not the case for all fields. For example, over $K := \mathbb{Q}(\sqrt{29})$ the elliptic curve

$$y^2 + xy + \left(\frac{5+\sqrt{29}}{2}\right)^2 y = x^3$$

has good reduction everywhere. The existence and properties of quadratic fields admitting such elliptic curves has been studied extensively [4–6,14,15,17,19–21,32,35,42], and extensions to higher-degree fields were considered by Takeshi [36,37]. Algorithms for computing such elliptic curves were given by Kida [18] for quadratic fields and by Cremona and Lingham [7] over general number fields. We will be interested in the following statistical question:

Question. *How often does a real (resp. imaginary) quadratic field admit an elliptic curve with good reduction everywhere and rational j-invariant?*

As with any such question, we must define "often" with respect to an ordering of quadratic fields. Let $R(x)$ (resp. $I(x)$) be the number of real (resp. imaginary) quadratic fields $K/\mathbb{Q}$ with discriminants of absolute value at most x and over which there exist elliptic curves with rational j-invariant and with good reduction at every prime of K. Setzer [33] gave an explicit criterion for m such that $\mathbb{Q}(\sqrt{m})$ admits an elliptic curve with rational j-invariant and good reduction everywhere. Coupling this criterion with a lower bound of Serre [31] on the sizes of particular sifted sets of integers, Clemm and Trebat-Leder [3] gave a lower bound on the quantities of interest.

The first author was supported by Simons Foundation grant #550023.

Theorem 1.1 ([3])**.**

$$R(x) \gg \frac{x}{\sqrt{\log x}} \quad \textit{and} \quad I(x) \gg \frac{x}{\sqrt{\log x}}.$$

1.1. **Main results.** Our main theorem is a sharp result for the asymptotic behavior of $R(x)$ and $I(x)$ assuming the *abc*-conjecture. Because the expressions for the constants are somewhat technical, we defer some of their descriptions to later in the paper.

Theorem A. *Assuming the abc-conjecture,*

$$R(x) \sim \frac{c_R x}{\sqrt{\log x}} \quad \textit{and} \quad I(x) \sim \frac{c_I x}{\sqrt{\log x}}$$

where

$$c_R = \sum_{\substack{d\in\mathbb{Z} \\ d \text{ good}}} \frac{c'_d c''_{d,R}}{|d| 2^{\omega(d)}} \quad \textit{and} \quad c_I = \sum_{\substack{d\in\mathbb{Z} \\ d \text{ good}}} \frac{c'_d c''_{d,I}}{|d| 2^{\omega(d)}},$$

where the set of good d is defined in (7), c'_d is as in Corollary 4.9 and $c''_{d,R}$ and $c''_{d,I}$ are as in Lemma 5.1.

We may worry that the condition of "rational j-invariant" is too restrictive. However, conditionally complete tables of elliptic curves with bounded absolute discriminant and good reduction everywhere due to the first author[1] [24] suggest that most quadratic fields admitting any curves with good reduction everywhere admit at least one such curve with rational j-invariant. We discuss the possibility of extending these results to all j-invariants further in Section 1.3.

One ingredient in the proof of Theorem A is an upper bound on how often quadratic twists of some elliptic curves over $\mathbb{Q}$ have integral points. Consider an elliptic curve $E/\mathbb{Q}$ with short Weierstrass equation $y^2 = f(x)$. We are interested in counting the number of quadratic twists E_d of E – with models $dy^2 = f(x)$ – that have integral points. Note that if E has a two-torsion point, say $(a : 0 : 1)$, then every twist E_d will also have the two-torsion point $(a : 0 : 1)$. As such, we restrict our attention to determining the existence of a *nontrivial* integral point on E_d – an integral point that is not two-torsion.

Formally, we prove an upper bound on the quantity $|T_E(D)|$, where

$$T_E(D) := \{d \in \mathbb{Z} \colon |d| \leq D, d \text{ is squarefree and } E_d \text{ has a nontrivial integral point}\}. \tag{1}$$

Granville [11] showed the following conditional upper bound on the analogous quantity for hyperelliptic curves.

Theorem 1.2 ([11])**.** *Assume that the abc-conjecture is true. Let C be a hyperelliptic curve given by the integral model $y^2 = f(x)$ where $f \in \mathbb{Z}[x]$ has degree at least three (i.e. the genus is at least one) and is separable. Then,*

$$|T_C(D)| \leq D^{\frac{1}{\deg f - 2} + o(1)}.$$

We will be interested in the case where $\deg f = 3$, in which case Theorem 1.2 is trivial. However, Granville also conjectures that the $\deg f - 2$ in the denominator of the exponent can be replaced with $\deg f$.

Conjecture 1.3 ([11])**.** *Let C be a hyperelliptic curve given by the integral model $y^2 = f(x)$ where $f \in \mathbb{Z}[x]$ has degree at least three (i.e. the genus is at least one) and is separable. Then,*

$$|T_C(D)| \sim \kappa_f D^{\frac{1}{\deg f} + o(1)},$$

where κ_f is some constant that can be determined explicitly given f.

[1] The tables are complete assuming the generalized Riemann hypothesis.

Granville proves Conjecture 1.3 for polynomials f of degree at least 7 that split into linear factors over $\mathbb{Q}$. We make progress towards Conjecture 1.3 when the degree of f is 3.

Theorem B. *Assume that the abc-conjecture is true. Let E be an elliptic curve over $\mathbb{Q}$ with short Weierstrass equation $y^2 = f(x)$ where $f(x) \in \mathbb{Z}[x]$ is reducible*[2] *over $\mathbb{Q}$. Then,*

$$|T_E(D)| \leq D^{2/3+o(1)}.$$

We may apply Theorem B to the set of good d in Theorem A to show (among other things) that the sum in the statement of Theorem A converges. At a high level, this sum is actually a union bound over the good $d \in \mathbb{Z}$, and thus it yields an upper bound on the leading constant in Theorem A. To show the matching lower bound, we control the second term in the inclusion-exclusion sequence via a result on the sizes of pairwise least common multiples of "polynomially sparse" subsets. This result may be of independent interest.

Theorem C. *A set $S \subseteq \mathbb{N}$ of squarefree numbers is called β-polynomially sparse if there is a constant $\beta \in (0,1)$ such that*

$$\#\{n \leq x \colon n \in S\} \leq x^{1-\beta+o(1)}$$

as x approaches $+\infty$. For any such S, the set

$$\{(n, n') \colon n \in S, n' \in S, \operatorname{lcm}(n, n') \leq x\}.$$

is $\frac{\beta}{2-\beta}$-polynomially sparse. Furthermore, there are sets for which this is tight.

Corollary 1.4. *The set of pairwise least common multiples of a polynomially sparse set of squarefree numbers is polynomially sparse.*

The initial motivation for studying the constants c_R and c_I in Theorem A was the observation that most quadratic fields admitting curves with everywhere good reduction appear to be real. Assuming the *abc*-conjecture, we are able to prove numerical lower bounds on c_R and c_I.

Corollary D. *Assuming the abc-conjecture, Theorem A holds for*

$$c_R \geq 0.1254 \quad \text{and} \quad c_I \geq 0.01102.$$

We expect these values, obtained by evaluating the sum in Theorem A for many good d, to be very close to the truth. Indeed, the aforementioned tables of elliptic curves show that, under the generalized Riemann hypothesis, $R(20000) = 728$ and $I(20000) = 97$[3]. Writing $\tilde{c_R}$ and $\tilde{c_I}$ to denote the constants in Corollary D, we have $c_R \, x_0 \log^{-1/2} x_0 \approx 797$ and $c_I \, x_0 \log^{-1/2} x_0 \approx 70$, roughly in line with the true values.

Corollary E. *Let E be the elliptic curve given by the short Weierstrass equation $y^2 = x^3 - 1728$. Assume that $|T_E(D)| \leq 5D^{0.35}$. Then, Theorem A holds with*

$$0.1254 \leq c_R \leq 0.1393 \quad \text{and} \quad 0.01102 \leq c_I \leq 0.02483.$$

In particular, $c_R > c_I$ under this hypothesis.

Experimentally, we have checked (Section 7.1) that this hypothesis holds comfortably for all $D \leq 10000$. We also motivate this hypothesis using the aforementioned conjecture of Granville (Conjecture 1.3).

[2] Equivalently, E has a rational Weierstrass point.

[3] These numbers of fields become 852 and 97, respectively, if we drop the condition of rational j-invariants.

1.2. **Techniques and an overview of the proofs.** The first input used in proving Theorem A is a criterion of Setzer [33] for when $\mathbb{Q}(\sqrt{m})$ admits an elliptic curve with good reduction everywhere and rational j-invariant. We state the criterion formally as Theorem 2.6 but at a high level, it tells us that $\mathbb{Q}(\sqrt{m})$ admits such an elliptic curve if and only if m can be factored as nd for some d such that

(a) d is the squarefree part of $r^3 - 1728$ for r in some positive density subset of the integers;
(b) n is divisible only by primes satisfying certain quadratic residuosity conditions with respect to d. For any d, the set of primes satisfying this condition has natural density $\frac{1}{2}$;
(c) the image of n in $(\mathbb{Z}/4d\mathbb{Z})^\times$ lies in a specified subset.

We are interested in upper bounding $R(x)$, the number of real quadratic fields with discriminant at most x and which satisfy conditions (a), (b), and (c) (the same techniques apply to $I(x)$).

We first show, assuming the *abc*-conjecture, that the set of $d \in \mathbb{Z}$ which satisfy (a) is polynomially sparse. This is a corollary of Theorem B. The key idea motivating the proof of Theorem B is the relationship between squarefree parts and quadratic twists of elliptic curves. Consider (a) above. We have that d is the squarefree part of $r^3 - 1728$ if and only if for some integer t we have $dt^2 = r^3 - 1728$. This happens if and only if the quadratic twist by d of $E : t^2 = r^3 - 1728$ has an integral point. By definition, $T_E(D)$ ((1)) counts the nontrivial points and hence the number of nonzero d which arise as squarefree parts of $r^3 - 1728$.

Next, we fix some d satisfying (a) and study the asymptotics of $R_d(x)$, the contribution to $R(x)$ from those m which are divisible by this d. Then, we have

$$R(x) \leq \sum_{d \text{ sat. (a)}} R_d(x). \tag{2}$$

This approach is motivated by the lower bound of Clemm and Trebat-Leder [3] (Theorem 1.1). They chose a single value of d satisfying (a) and for which (c) is trivial. A result of Serre [31] implies a lower bound on the number of n satisfying (b) and shows that for this choice of d, $R_d(x) \gg \frac{x}{\sqrt{\log x}}$. This may seem surprising, as it means that even without considering multiple values of d they are already able to obtain the correct order of growth of $R(x)$! This happens because the set of d satisfying (a) is very sparse. Indeed, it turns out that for any such d,

$$R_d(x) \ll \frac{(1 + o_d(x))c_d x}{|d| \sqrt{\log x}}, \tag{3}$$

where c_d grows very slowly as $|d|$ goes to infinity. We prove (3) using Selberg-Delange theory (in particular, Theorem 4.8), which is also the general theory underlying the bound of Serre [31] used in the work of Clemm and Trebat-Leder. Selberg-Delange theory gives us a Tauberian theorem for Dirichlet series which can be expressed as $\zeta(s)^\rho G(s)$ for $\rho \in \mathbb{C}$ and $G(s)$ holomorphic in a neighborhood around $s = 1$. For ρ a nonzero real, it tells us that the sum of coefficients of the series up to x is asymptotically $cx \log^{\rho-1} x$ for some explicit constant c depending on F. To obtain our upper bound, we apply Selberg-Delange theory to the Dirichlet series $F(s)$ whose coefficients are the values of the characteristic function of (b) – since we just need an upper bound, it is fine to ignore (c) for now. It turns out that because the number of "valid" primes in (b) is half of all primes, $F(s) = \zeta(s)^{1/2} G(s)$ for some $G(s)$ holomorphic around $s = 1$. This then implies (3). Applying (3) to (2), we deduce

$$R(x) \ll \sum_{d \text{ sat. (a)}} \frac{(1 + o_d(x))c_d x}{|d| \sqrt{\log x - \log |d|}}. \tag{4}$$

Summation by parts shows that the sum of the reciprocals of the elements of a polynomially sparse set converges (Lemma 2.1), and applying this to the set of d satisfying (a) (which is polynomially sparse by Theorem B), we have that the series

$$\sum_{d \text{ sat. (a)}} \frac{c_d}{|d|}$$

converges. This allows us to uniformly bound the $o_d(x)$ terms in (4) and obtain

$$R(x) \ll \frac{x}{\sqrt{\log x}} \sum_{d \text{ sat. (a)}} \frac{c_d}{|d|} \ll \frac{x}{\sqrt{\log x}}. \tag{5}$$

In order to compute the implicit constant in (5), we start by computing the implicit constant in (3) (Lemma 5.1). To do this, we fix a d and count those n which satisfy (b) and (c). Selberg-Delange theory can be applied directly to obtain the exact constant if we are only interested in the Dirichlet series of (b). We need to study the Dirichlet series of (b)$\wedge$(c)[4], which is the (Rankin-Selberg) convolution of the Dirichlet series for (b) and the Dirichlet series for (c). However, (c) need not be a multiplicative property, and hence its Dirichlet series need not have an Euler product. We address this by expressing it as a linear combination of Dirichlet L-series and noting that only one term of the linear combination contributes to the overall asymptotics. We then apply Theorem 4.8 to this term to obtain our result on $R_d(x)$.

Observe that (2) is simply a union bound over the contributions of all d satisfying (a). By the principle of inclusion-exclusion, the sum of the first two terms in the inclusion-exclusion series are a lower bound on $R(x)$. The first term is simply the union bound that we have already computed. The second term is a sum over pairs (d, d'), both satisfying (a), where each term accounts for the contribution to $R(x)$ from those n which are divisible by $\operatorname{lcm}(|d|,|d'|)$. Thus, abusing notation, we want to upper bound

$$\sum_{d,d' \text{ sat. (a)}} R_{d,d'}(x), \tag{6}$$

where each term captures the contribution from n dividing both d and d'. As before, part of our proof involves showing that the sum

$$\sum_{d,d' \text{ sat. (a)}} \frac{c_{dd'}}{\operatorname{lcm}(|d|,|d'|)}$$

converges for some $c_{dd'}$ which grows slowly as $\operatorname{lcm}(|d|, |d'|)$ goes to infinity. Here, we use Theorem C, which tells us that the number of pairs of elements up to x in a polynomially sparse set with least common multiple at most x is $\ll x^{1-\kappa}$ for some $\kappa > 0$. By summation by parts, the sum in question converges. We use this to show that the second term in the inclusion-exclusion series is asymptotically negligible compared to the first term. Therefore, the constant we obtained from the union bound is actually the correct constant.

1.3. **Future work.**

There are several natural extensions. The first concerns the generalization of our result to elliptic curves with good reduction everywhere and arbitrary j-invariant.

Conjecture 1.5. *Theorem A holds even after removing the constraint that j is rational.*

To show this, we would want to show that the number of real and imaginary quadratic fields with discriminant of absolute value at most x and over which there exists an elliptic curve with good reduction everywhere but no elliptic curve with good reduction everywhere and rational j-invariant is $o(\frac{x}{\sqrt{\log x}})$. As mentioned, this conjecture is motivated by elliptic curve tables constructed by the first author [24] – of the 955 quadratic fields admitting an elliptic curve with good reduction everywhere, only 130 of the fields do not admit such a curve that also has rational j-invariant. While there is no criterion as explicit as that of Setzer's explicit criterion [33] that detects elliptic curves

[4] The Dirichlet series whose coefficient at n is 1 if and only if n satisfies (b) and (c)

with irrational j-invariant, there are two approaches that might be made work: 1.) The proof of Shavarevich's theorem [41] (c.f. Silverman [34, Thm. IX.6.1]) reduces the computation of elliptic curves over K with good reduction everywhere (or more generally, outside a finite set of primes) to the computation of integral points on finitely many associated Mordell curves. Cremona and Lingham [7] turned this into an algorithm, which still requires the possibly difficult computation of the Mordell–Weil bases of these Mordell curves. 2.) The Shafarevich–Parshin construction [26] reduces the computation of elliptic curves over K with good reduction everywhere to the S-unit equation over K with S being the set of primes above 2. This approach was used in the above mentioned computation of [24].

Another direction of improvement is to remove the dependence on the *abc*-conjecture. The dependence arises whenever we use Theorem 2.3 to bound the range of r for which it is possible for the squarefree part of $r^3 - 1728$ to be d. Removing this dependence would likely also yield progress towards Conjecture 1.3 and would be of independent interest

Lastly, it may be interesting to obtain criteria like that of Setzer for number fields of higher degrees. These criteria could then be used to derive statistical results for such families of number fields just as we have done in the quadratic case.

1.4. Organization.

Most preliminary content, including proofs of elementary results and references to the literature, are in Section 2. We prove our bound on how often twists of some elliptic curves have an integral point, Theorem B, in Section 3. In Section 4, we apply Selberg-Delange theory and Theorem B to prove Theorem 4.1, a version of Theorem A that is tight up to constants. In Section 5, we compute an upper bound on the leading constants in Theorem A. In Section 6, we prove Theorem C and use it to prove a matching lower bound on the leading constants of Theorem A, concluding the proof. In Section 7 we formulate an additional hypothesis based on Conjecture 1.3 to obtain good numeric estimates for c_R and c_I.

1.5. Acknowledgements.

The authors thank Ashwin Sah and Mehtaab Sawhney for an improvement to the upper bound in Theorem C and a matching lower bound. In addition, the authors benefited from helpful conversations with Daniel Fiorilli, Andrew Granville, Michael Kural, and Melanie Matchett Wood. The first author was supported by Boston University and by Simons Foundation grant #550023.

2. Preliminaries

2.1. Notation.

We write $\mathbb{N}$ to denote the positive integers. In general, p and q will be used to denote primes and $\prod_p$, $\prod_q$, $\sum_p$, and $\sum_q$ denote products and sums over primes. For p a prime, we write $|\cdot|_p$ to denote the p-adic norm. Given a number field $K/\mathbb{Q}$, we write Δ_K to denote its absolute discriminant.

Let n be an integer. We write $\omega(n)$ to denote the number of distinct prime factors of n. Generally, we will apply this in contexts where n is squarefree, in which case $\omega(n)$ is simply the number of prime factors of n.

If t is the largest integer for which t^2 divides n then we call $d := \frac{n}{t^2}$ the *squarefree part* of n and write $d = \operatorname{sqf}(n)$. The product of the distinct prime factors of n is the *radical* of n, which we denote by $\operatorname{rad}(n)$. Note that the squarefree part of n includes its sign but the radical does not. Given two positive integers m and n, we write (m, n) to denote their greatest common divisor.

Throughout, we use Vinogradov asymptotic notation. If $f \ll g$ then $\limsup_{x\to\infty} \frac{|f(x)|}{g(x)} < \infty$. If $f \gg g$ then $\limsup_{x\to\infty} \frac{|g(x)|}{f(x)} < \infty$. If $f \ll g$ and $g \ll f$ then $f \asymp g$. We will also occasionally make use of Bachmann-Landau asymptotic notation to concisely describe error. The expression $b(x) = c(x) + o(g(x))$ means that $\limsup_{x\to\infty} \frac{b(x)-c(x)}{|g(x)|} = 0$. Similarly, we write $b(x) = c(x) + O(g(x))$ when $b(x) - c(x) \ll g(x)$. A subscript on any such notation – for example, $\gg_\epsilon$ – means that the implicit function or constant may depend on the subscript. We may sometimes combine both notations in expressions like $f(x) \ll (1 + o_d(1))g(x)$ for some auxiliary variable d; this will be used if we wish to suppress the dependence on d for brevity but will need to address it later in the paper. In this context, we write $o'_d(1)$ to denote an error term $\varepsilon(d, x)$ such that

$$\varepsilon(d,x) \ll \left(1 - \frac{\log|d|}{\log x}\right)^{1/2} \left(1 + \frac{|d|^{1.001}}{x} \exp\left(-K \log^{1/2} \frac{x}{|d|}\right) + \frac{1}{x} \log^{-1} \frac{x}{|d|}\right) - 1$$

for some absolute constant K. Note that this expression goes to zero as $\frac{x}{|d|}$ goes to infinity.

Given complex numbers z and a, we define the power $z^a := e^{a \log z}$ with respect to the principal branch of the logarithm.

Throughout, we write $\left(\frac{\cdot}{\cdot}\right)$ to denote the Kronecker symbol.

We will often be concerned with Dirichlet characters of modulus 8. To this end, it will help to fix a notation for characters of $(\mathbb{Z}/8\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. Without loss of generality, let 3 (mod 8) correspond to $(1, 0) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, 5 (mod 8) to $(0, 1)$, and 7 (mod 8) to $(1, 1)$. We then define the characters χ_{ij}, for $i, j \in \{0, 1\}$, to be nontrivial on the first (resp. second) component when i (resp. j) is 1. For example, $\boldsymbol{\chi}_{11}$ takes values $1, -1, -1$, and 1 at arguments which are $1, 3, 5$, and 7 (mod 8).

2.2. **Some analytic facts.**

2.2.1. *Summation by parts.* The following lemma will allow us to convert results on the sparseness of a subset of the natural numbers to results on the sums of reciprocals of elements of that subset.

Lemma 2.1. *Let $\alpha \in (0, 1)$ and C be positive constants. Suppose that $f\colon \mathbb{N} \to \mathbb{N}$ is such that for all x, $\sum_{n=1}^{x} f(n) \le Cx^{1-\alpha}$. Then, if $\kappa + \alpha > 1$,*

(i) $\sum_{n=1}^{\infty} \frac{f(n)}{n^\kappa}$ converges;
(ii) For $m \ge 2$, $\sum_{n=m}^{\infty} \frac{f(n)}{n} \le \frac{C\kappa m^{-(\kappa+\alpha-1)}}{\kappa+\alpha-1}$.

Lemma 2.1 follows from a standard application of summation by parts or Stieljes integrals.

2.2.2. *L-functions and convolutions.* Given two functions $a, b\colon \mathbb{N} \to \mathbb{C}$ and associated Dirichlet series $F(s) = \sum_n a_n n^{-s}$ and $G(s) = \sum_n b_n n^{-s}$, their convolution is the formal Dirichlet series

$$F \otimes G(s) := \sum_n a_n b_n n^{-s}.$$

The convolution of L-series corresponds to the product of the coefficients in the same way that the product of L-series corresponds to the (Dirichlet) convolution of the coefficients.

2.2.3. *Kronecker symbols.* The Kronecker symbol is a generalization of the Legendre symbol which allows composite inputs in the top and bottom entries and is - with some exceptions - multiplicative in both the top and the bottom entries. It is defined in most number theory texts (for example, page 39 of [8]). Kronecker symbols are intimately related to real Dirichlet characters. The symbol $\left(\frac{D}{\cdot}\right)$ is a real Dirichlet character when $D \not\equiv 3 \pmod 4$, and every real Dirichlet character can be written as such a character. Furthermore, the primitive real Dirichlet characters are in $1-1$ correspondence with symbols $\left(\frac{D}{\cdot}\right)$ when D is a fundamental discriminant (i.e. when D is the discriminant of a quadratic number field).

2.3. **The *abc*-conjecture and some consequences.**

Recall the *abc*-conjecture.

Conjecture 2.2 (Oesterlé, Masser, Szpiro)**.** *For every $\epsilon > 0$ there exists a constant C_ϵ such that for any given non-zero coprime integers a, b, c with $a + b + c = 0$,*

$$\max(|a|, |b|, |c|) \le C_\epsilon \operatorname{rad}(abc)^{1+\epsilon}.$$

Theorem 2.3 (Corollary 1 of [10])**.** *Assume that the abc-conjecture (Conjecture 2.2) is true. Suppose that $g(x) \in \mathbb{Z}[x]$ is separable. Then, for any $r \in \mathbb{Z}$,*

$$\operatorname{rad} g(r) \gg_\epsilon |r|^{\deg g - 1 - \epsilon}.$$

For a hyperelliptic curve over $\mathbb{Q}$ with integral model $C\colon y^2 = f(x)$, we write C_d to denote its d^{th} quadratic twist with model $dy^2 = f(x)$. We will make essential use of the following theorem.

Theorem 2.4 (Theorem 1(i) of [11])**.** *Assume that the abc-conjecture is true. Suppose that $f(x) \in \mathbb{Z}[x]$ is separable and let C be the hyperelliptic curve with equation $y^2 = f(x)$. If $\deg f \geq 3$ then the integral points (r,t) on C_d satisfy*

$$|r| \ll_\epsilon |d|^{\frac{1}{\deg f - 2} + \epsilon}$$

and

$$|t| \ll_\epsilon |d|^{\frac{1}{\deg f - 2} + \epsilon}$$

for every $\epsilon > 0$.

Proof. Let $dt^2 = f(r)$. It follows from Theorem 2.3 that, under the *abc*-conjecture

$$|d|^{\frac{1}{2}} |r|^{\frac{\deg f}{2}} \gg_f |df(r)|^{\frac{1}{2}} = |dt| \geq \operatorname{rad}(dt) = \operatorname{rad}(f(r)) \gg_\epsilon |r|^{\deg f - 1 - \epsilon}$$

and the first part of the result follows. For the second part, note that

$$|dt^2| = |f(r)| \ll_f |r|^{\deg f} \ll_\epsilon |d|^{\frac{\deg f}{\deg f - 2} + \epsilon}. \qquad \square$$

2.4. **Identifying quadratic fields with good reduction everywhere.** The following definition is the formal statement of (a) from Section 1.2.

Definition 2.5. We say that $d \in \mathbb{Z}$ is *good* if $d = \operatorname{sqf}(r^3 - 1728)$ for r an element of the set

$$\{r \in \mathbb{Z}\colon \text{if } r \equiv 0 \pmod 2 \text{ then } r \equiv 0, 4 \pmod{16};\ \text{if } r \equiv 0 \pmod 3 \text{ then } n \equiv 12 \pmod{27}\}. \tag{7}$$

Given $d \in \mathbb{Z}$ squarefree, we write

$$\epsilon_d := \begin{cases} 1 & d \equiv 1 \pmod 4, \\ -1 & \text{otherwise.} \end{cases} \tag{8}$$

We may now state a criterion of Setzer [33] which tells us when a quadratic field $\mathbb{Q}(\sqrt{m})$ admits an elliptic curve with good reduction everywhere and rational j-invariant. This will formalize (b) and (c) from Section 1.2.

Theorem 2.6 (Theorem 2.2 of [3], correcting an error in Theorem 2 of [33])**.** *Let m be a squarefree integer. The field $\mathbb{Q}(\sqrt{m})$ admits an elliptic curve with good reduction everywhere and rational j-invariant if and only if the following conditions are satisfied for some integers d and n such that d is good ((7)) and $m = dn$.*

(i) $\epsilon_d d$ is a quadratic residue modulo n;
(ii) $-\epsilon_d n$ is a quadratic residue modulo d;
(iii) If $d \equiv \pm 3 \pmod 8$ then $m = dn \equiv 1 \pmod 4$;
(iv) If d is even then $n \equiv d + 1 \pmod 8$;
(v) $m > 0$ if $\epsilon_d d < 0$.

In the above, neither d nor n are restricted to being positive integers. Intuitively, (i) is (b) from Section 1.2, and (ii)-(v) comprise (c) from Section 1.2.

We will now define the primary quantities of interest. We write that an elliptic curve over a field $K/\mathbb{Q}$ has $\mathrm{GRE}_{\mathbb{Q}}$ if it has good reduction at every prime of $\mathcal{O}_K$ and j-invariant in $\mathbb{Q}$.

Definition 2.7. Following [3], we define for every positive x

$$R(x) := \#\{m\colon 0 < \Delta_{\mathbb{Q}(\sqrt{m})} \leq x, \mathbb{Q}(\sqrt{m}) \text{ admits an elliptic curve with } \mathrm{GRE}_{\mathbb{Q}}\}$$

and

$$I(x) := \#\{m\colon -x \leq \Delta_{\mathbb{Q}(\sqrt{m})} < 0, \mathbb{Q}(\sqrt{m}) \text{ admits an elliptic curve with } \mathrm{GRE}_{\mathbb{Q}}\}.$$

If d is good, we also define

$$R_d(x) := \#\{n\colon 0 < \Delta_{\mathbb{Q}(\sqrt{nd})} \leq x, \mathbb{Q}(\sqrt{nd}) \text{ admits an elliptic curve with } \mathrm{GRE}_{\mathbb{Q}}\},$$

and

$$I_d(x) := \#\{n\colon -x \leq \Delta_{\mathbb{Q}(\sqrt{nd})} < 0, \mathbb{Q}(\sqrt{nd}) \text{ admits an elliptic curve with } \mathrm{GRE}_{\mathbb{Q}}\}.$$

Intuitively, $R_d(x)$ and $I_d(x)$ measure the contribution of m which are divisible by d to $R(x)$ and $I(x)$ respectively. Note that our definitions of $R_d(x)$ and $I_d(x)$ differ somewhat from those of Clemm and Trebat-Leder [3] as they write $R_d(x)$ (and $I_d(x)$ analogously) to count the number of n up to x such that $\mathbb{Q}(\sqrt{nd})$ admits an elliptic curve with $\mathrm{GRE}_{\mathbb{Q}}$.

3. Twists of elliptic curves

Let E be an elliptic curve defined over $\mathbb{Q}$ with short Weierstrass equation $y^2 = f(x)$ for $f(x) \in \mathbb{Z}[x]$. We denote by E_d the d^{th} quadratic twist of E with the integral model $dy^2 = f(x)$. Then,

$$T_E(D) := \{d \in \mathbb{Z}\colon |d| \leq D, d \text{ is squarefree and } E_d \text{ has a nontrivial integral point}\}.$$

In this section, we will prove Theorem B, which we now recall.

Theorem B. *Assume that the abc-conjecture is true. Let E be an elliptic curve over $\mathbb{Q}$ with short Weierstrass equation $y^2 = f(x)$ where $f(x) \in \mathbb{Z}[x]$ is reducible*[5] *over $\mathbb{Q}$. Then,*

$$|T_E(D)| \leq D^{2/3+o(1)}.$$

It will be useful to reformulate bounding $T_E(D)$ as bounding the number of integers with absolute value up to D that arise as squarefree parts of $f(x)$. This is because the equation $dy^2 = f(x)$ has an integral point if and only if d is the squarefree part of $f(r)$ for some integer r. The squarefree part function is multiplicative but not totally multiplicative. Nonetheless, the following lemma will let us write the squarefree part of a separable polynomial as the product of the squarefree parts of its factors if we ignore the valuations at finitely many primes.

Lemma 3.1. *Suppose that $f \in \mathbb{Z}[x]$ is separable and that it factors as $f = \prod_i g_i$ for $g_i \in \mathbb{Z}[x]$. Then, for all but finitely many p and for all $r \in \mathbb{Z}$,*

$$|\operatorname{sqf}(f(r))|_p = \prod_i |\operatorname{sqf}(g_i(r))|_p$$

Proof of Lemma 3.1. If two distinct factors g_i and g_j share a root modulo a prime then the resultant of $\bar{g}_i$ and $\bar{g}_j$ in $\mathbb{F}_p$ must be 0, meaning that p must divide the resultant of g_i and g_j. By assumption, g_i and g_j have no shared roots over $\mathbb{C}$ and hence their resultant is a nonzero integer. This means that the reductions of g_i and g_j modulo a prime p can only share a root for the finitely many primes p that divide their resultant. Taking the union of these finite sets over all pairs of distinct i and j, we see that for p outside this finite union, if p divides $g_i(r)$ for some r then p does not divide $g_j(r)$ for all $j \neq i$. This means that the factors $g_i(r)$ are "coprime" outside our finite set of primes, and the lemma then follows from the multiplicativity of the squarefree part function. □

Proof of Theorem B. There are four cases depending on how $f(x)$ factors. In the definition of each case, a factorization of f in $\mathbb{Z}[x]$ into irreducible factors is given.

[5] Equivalently, E has a rational Weierstrass point.

(1) $\boldsymbol{f(x) = (x + a_1)(x + a_2)(x + a_3)}$: This case follows directly from the proof of Theorem 2 in [11]. For the reader's convenience, we include a sketch of Granville's proof. To get an upper bound on the number of squarefree d for which there exist (r, t) such that $f(r) = dt^2$, we will upper bound the number of pairs (r, t) such that t^2 divides $f(r)$ and $f(r)/t^2$ is squarefree. We will restrict to counting pairs (r, t) which satisfy the given conditions and for which $R < r \leq 2R$ and $Y < d \leq 2Y$ since summing over all these cases at the end only costs us a factor of $\log^2 D$ by Theorem 2.4. If R is small relative to D (for example, we can take $R \ll D^{4/9}$ in the proof), the range of possible values of t is small. We may then obtain an upper bound by summing over the possible values that t can take and for each, bounding the number of r in the relevant range such that $f(r) \equiv 0 \pmod{t^2}$. This ultimately nets us a bound of $\ll_\epsilon D^{1/3+\epsilon}$ for any $\epsilon > 0$.

When R is somewhat large relative to D – say, $D^{8/21} \ll R \ll_\epsilon D^{1+\epsilon}$ – and t has a large range of possible values, we instead argue that any t in a valid pair must have some divisor τ in the range $R^{1/3} < \tau \leq R^{2/3}$. We can thus sum over τ and bound the number of r in the relevant range such that $f(r) \equiv 0 \pmod{\tau^2}$. In this regime, this is better than the previous argument and we end up with a bound of $\ll R^{2/3} \log^3 3R$. By assumption, this can be made $\ll_\epsilon D^{2/3+\epsilon}$.

If we make the implicit constant above a sufficiently large function of $\frac{1}{\epsilon}$, we do not need to consider larger values of R by Theorem 2.4.

(2) $\boldsymbol{f(x) = (x + a)(x^2 + b)}$: We have

$$\operatorname{sqf}(f(r)) = \frac{1}{k(r)^2} \operatorname{sqf}(r + a) \operatorname{sqf}(r^2 + b),$$

where $k(r)$ is divisible only by primes which divide both $r + a$ and $r^2 - b$. By Lemma 3.1, the set S of primes p for which there exists an r such that p divides both $r + a$ and $r^2 + b$ is finite, and therefore

$$\operatorname{sqf}(f(r)) \leq \frac{1}{K^2} \operatorname{sqf}(r + a) \operatorname{sqf}(r^2 + b),$$

where $K := \prod_{p \in S} p$. Choose an $\epsilon > 0$, suppose the constant from Theorem 2.4 for this ϵ is C_ϵ, and let

$$T'_E(D) := \{r \colon |r| \leq C_\epsilon D^{1+\epsilon}, |\operatorname{sqf}(r + a) \operatorname{sqf}(r^2 + b)| \leq K^2 D\}.$$

Notice that $T_E(D)$ contains small values of d while $T'_E(D)$ contains those r for which $\operatorname{sqf}(f(r))$ is small. We claim that $|T_E(D)| \leq |T'_E(D)|$. This is because any $d \in T_E(D)$ is the squarefree part of $f(r)$ for some r. For this r, we have

$$|\operatorname{sqf}(r + a) \operatorname{sqf}(r^2 + b)| = c(r)^2 d \leq K^2 D$$

and hence $r \in T'_E(D)$. We only need to consider $|r| \leq C_\epsilon D^{1+\epsilon}$ by Theorem 2.4.

We will branch into two subcases. First, consider r such that $|\operatorname{sqf}(r + a)| \leq D^{2\delta}$ for some $\delta > 0$ that we will select later. For each squarefree number $m \leq D^{2\delta}$, there are at most $2\sqrt{\frac{C_\epsilon D^{1+\epsilon}}{m}}$ values of r such that $\operatorname{sqf}(r + a) = m$ and $|r| \leq C_\epsilon D^{1+\epsilon}$. Therefore, the contribution to $T'_E(D)$ from these r is at most

$$\begin{aligned} 2C_\epsilon^{1/2} \int_1^{D^{2\delta}} \left(\frac{D^{1+\epsilon}}{z}\right)^{1/2} dz &= 2C_\epsilon^{1/2} D^{1/2(1+\epsilon)} \int_1^{D^{2\delta}} z^{-1/2} dz \\ &\leq C_1 D^{1/2(1+\epsilon)+\delta}. \end{aligned}$$

for $C_1 \leq 4C_\epsilon^{1/2}$.

Second, we will count r contributing to $T'_E(D)$ for which $|\operatorname{sqf}(r+a)| > D^{2\delta}$. Because we require $|\operatorname{sqf}(f(r))| \le K^2 D$, we require that $|\operatorname{sqf}(r^2+b)| \le D^{1-2\delta}$. Fix an integer m such that $|m| \le D^{1-2\delta}$. We will bound the number of r for which $\operatorname{sqf}(r^2+b) = m$. For any such r, there is an $s \in \mathbb{Z}$ such that

$$r^2 - ms^2 = -b.$$

This is equivalent to requiring that $r + s\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ has norm $-b$. If m is negative then $\mathbb{Q}(\sqrt{m})$ is imaginary quadratic and by Dirichlet's unit theorem there are only finitely many elements of $\mathbb{Q}(\sqrt{m})$ which have this norm. Hence, when m is negative there are only finitely many values of r for which $\operatorname{sqf}(r^2+b) = m$.

If m is positive, let ϵ_m be the unique fundamental unit that exceeds 1 in the embedding of $\mathbb{Q}(\sqrt{m}) \hookrightarrow \mathbb{R}$ that sends $\sqrt{m} \mapsto \sqrt{m}$. Notice that after these choices $\epsilon_m > \frac{1}{2}(1+\sqrt{m})$. This is because, by standard properties of the fundamental unit, $\epsilon_m = y + z\sqrt{m}$ for $y, z > 0$ and also ϵ_m is an element of $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$.

If $r + s\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ has norm $-b$ then then any other element of $\mathbb{Q}(\sqrt{m})$ with this norm is, up to sign, a power of the fundamental unit ϵ_m times $r + s\sqrt{m}$. Suppose that α is an element (up to sign) of $\mathbb{Z}[\sqrt{m}]$ with norm $-b$ that has minimum Archimidean absolute value. Note that there is a unique minimum Archimedean absolute value because $\mathbb{Z}[\sqrt{m}]$ is discrete. Then, every element of $\mathbb{Z}[\sqrt{m}]$ with norm $-b$ is of form $\pm\alpha\epsilon_m^k$ for some $k \ge 0$. We know that $\epsilon_m > \frac{1}{2}(1+\sqrt{m}) > 1.2$. We want to show that the x-coordinate of $\alpha\epsilon_m^k$ grows exponentially in k, as this will imply that we cannot have too many values of r such that $\operatorname{sqf}(r^2+b) = m$. Writing $|\cdot|$ for the Archimedean absolute value, we see that if $r + s\sqrt{m} = \pm\alpha\epsilon_m^k$ then,

$$\begin{aligned}
|\alpha\epsilon_m^k| &= |r + s\sqrt{m}| \\
&\le |r| + |s\sqrt{m}| \\
&= |r| + \sqrt{r^2+b} \\
&\le 2|r| + \sqrt{b}.
\end{aligned}$$

Rearranging, this means that

$$\frac{\alpha\epsilon_m^k - \sqrt{b}}{2} \le |r|.$$

Because we require $|r| < C_\epsilon D^{1+\epsilon}$, we conclude that it is sufficient to look at

$$k < \frac{\log \frac{2C_\epsilon D^{1+\epsilon} + \sqrt{b}}{\alpha}}{\log \epsilon_m} \le C_{2,\epsilon} \log D$$

for some positive $C_{2,\epsilon}$, using in the second inequality that ϵ_m is lower bounded by a constant independent of m. The point is that the number of possible r that yield any given value of $\operatorname{sqf}(r^2+b)$ is small. Thus, the total number of possible r in this subcase is at most $C_{2,\epsilon} D^{1-2\delta} \log D$.

Putting the two subcases together, our total count is $C_{1,\epsilon} D^{\frac{1}{2}(1+\epsilon)+\delta} + C_{2,\epsilon} D^{1-2\delta} \log D$. Taking $\delta = \frac{1}{6}$, we can make our overall upper bound $(C_{1,\epsilon} + C_{2,\epsilon}) D^{\frac{2}{3}+\epsilon} \ll_\epsilon D^{\frac{2}{3}+\epsilon}$.

(3) $\boldsymbol{f(x) = (x+a)(x^2+b_1x+b_2)}$: We will reduce to the previous case via a pair of coordinate transformations which map integral points to integral points and work for any twist of $y^2 = f(x)$. Start with the equation $dy^2 = f(x)$. Define $x' := 2^2 x$, $y' := 2^3 y$, $a' := 2^2 a$, $b'_1 := 2^2 b_1$, and $b'_2 := 2^4 b_2$. We have

$$dy'^2 = (x'+a')(x'^2 + b'_1 x' + b'_2),$$

which looks the same as before but now b_1' is even. Thus, we may complete the square, taking $x'' := x' + 2^{-1}b_1'$, $y'' := y'$, $a'' := a' - 2^{-1}b_1'$, and $b'' := b_2' - 2^{-2}b_1'$ to obtain

$$dy''^2 = (x'' + a'')(x''^2 + b'').$$

Overall, we have $x'' = 2^2x + 2b_1$, $y'' = 2^3y$ and hence integral points map to integral points. Because the transformation is independent of d, we may apply the logic of the previous case to $f(x'') = (x'' + a'')(x''^2 + b'')$ to obtain an upper bound on the number of twists of our original equation with integral points.

(4) ***f* is not monic**: Suppose $f(x) = \sum_{i=0}^3 f_i x^i$. Consider $x' := f_3 x$, $y' := f_3 y$, and $f'(x) := x'^3 + f_x x'^2 + f_1 f_3 x' + f_0 f_3^2$. Then, $y'^2 = f'(x')$ and f' is monic. Furthermore, f' is reducible over $\mathbb{Q}$ because f is. Thus, by Gauss' Lemma f' is reducible over $\mathbb{Z}$ and we may pass to one of the previous cases as appropriate because integral points are mapped to integral points. □

4. The Asymptotics of $R(x)$ and $I(x)$ up to Constants

Our main theorem in this section will be a version of Theorem A which is correct up to constants.

Theorem 4.1. *Assume that the abc-conjecture is true. Then,*

$$R(x) \asymp \frac{x}{\sqrt{\log x}} \quad \text{and} \quad I(x) \asymp \frac{x}{\sqrt{\log x}}.$$

Because Clemm and Trebat-Leder proved the lower bound (Theorem 1.1), it is sufficient for us to prove the upper bound. Throughout this section, d will denote a squarefree integer. We will prove Theorem 4.1 by first proving the following lemma.

Recall the definitions of $R_d(x)$ and $I_d(x)$ from Definition 2.7, as well as the definition of $o_d'(1)$ from Section 2.1.

Lemma 4.2. *Let d be good. Then,*

$$R_d(x) \ll \frac{(1 + o_d'(1))c_d x}{|d|\sqrt{\log x}} \quad \text{and} \quad I_d(x) \ll \frac{(1 + o_d'(1))c_d x}{|d|\sqrt{\log x}},$$

where the implicit constant is absolute (independent of d) and c_d is as defined in Corollary 4.9.

We will then pass from Lemma 4.2 to Theorem 4.1 by summing $R_d(x)$ over all good d. By Theorem B, the set of good d is very sparse and therefore the asymptotic dependence on x stays the same. Notice that Lemma 4.2 is unconditional – we depend on the *abc*-conjecture in Theorem 4.1 only to prove Theorem B. We keep track of the $o_d'(1)$ error in Lemma 4.2 in order we ensure that its dependence on d is mild enough that summing over the set of good d does not change the dependence on x by more than a constant.

Throughout this section, we will compute all our bounds while pretending that our quadratic fields $\mathbb{Q}(\sqrt{m})$ (in both the real and imaginary settings) are ordered by $|m|$ rather than by $\Delta_{\mathbb{Q}(\sqrt{m})}$. This will not change any bound by more than a constant and thus is irrelevant to Lemma 4.2 and Theorem 4.1.

To prove Lemma 4.2, we will count those n which satisfy Theorem 2.6(i). This means that we want to count squarefree n which are divisible only by primes q for which $\epsilon_d d$ is a nonzero square modulo q. We do not actually need the squarefree condition to reach Theorem 4.1 but addressing it now will save us from repeating this work in Section 5.

Remark (Difficulties of the sieve). Sieve theory provides a general method for counting the numbers up to x which are divisible only by a subset S of the primes. When S has positive natural density α, sieve theory gives us an upper bound of $O(x \log^{\alpha-1} x)$ for this number – this follows from summation by parts and standard results[6]. However, in our setting S is the set of primes satisfying Theorem 2.6(i). By Chebotarev's density theorem applied to the multiquadratic extension $\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_r})$, one can check that S has natural density $\frac{1}{2} + o_d(1)$ and our sieve-theoretic upper bound on $R_d(x)$ and $I_d(x)$ would end up being

$$\ll \frac{x}{d \log^{1/2 + o_d(1)} x}.$$

This is insufficient to prove Lemma 4.2. Furthermore, without the generalized Riemann hypothesis (or some other means of bounding Siegel zeroes) we have no control over the dependence on d of the little-o term that arises from Chebotarev's density theorem and thus cannot easily bound the sum of these answers over all good d. One can do better by exploiting the additional structure that the set S has. Indeed, this is the idea behind the theorem of Serre [31] (whose proof Serre attributed to Raikov, Wintner, and Delange) which Clemm and Trebat-Leder used in their lower bound[7]. By using Selberg-Delange theory (Theorem 4.8) – which generalizes some of the ideas used in [31] – we can obtain the correct dependence on x, including the coefficient of $\frac{x}{\sqrt{\log x}}$, and bypass the issue of computing the density of S altogether.

Definition 4.3. We define $\chi_d \colon \mathbb{N} \to \mathbb{C}$ as the totally multiplicative function which on primes q is

$$\chi_d(q) := \begin{cases} \left(\frac{\epsilon_d d}{q}\right) & q \text{ odd}, \\ 1 & q = 2 \text{ and } d \text{ odd}, \\ 0 & q = 2 \text{ and } d \text{ even}. \end{cases}$$

where $\left(\frac{\cdot}{\cdot}\right)$ denotes the Kronecker symbol.

Observe that unless $\epsilon_d d \equiv \pm 3 \pmod 8$ (and hence $\epsilon_d d \equiv 5 \pmod 8$), χ_d agrees with the Kronecker symbol $\left(\frac{\epsilon_d d}{\cdot}\right)$ at all $n \in \mathbb{N}$. If $d \equiv \pm 3 \pmod 8$, we define $\chi_d(2) = 1$ but $\left(\frac{\epsilon_d d}{2}\right) = -1$. By the definition of ϵ_d, we see that $\epsilon_d d \not\equiv 3 \pmod 4$ and hence that $\left(\frac{\epsilon_d d}{\cdot}\right)$ is necessarily a quadratic Dirichlet character. Furthermore, this character will always be primitive, as either $\epsilon_d d \equiv 1 \pmod 4$, or $\epsilon_d d \equiv 2 \pmod 4$ and $\left(\frac{\epsilon_d d}{\cdot}\right) = \left(\frac{4\epsilon_d d}{\cdot}\right)$. As such, $L(s, \chi_d)$, the L-function associated to χ_d, is closely related to the L-function of some primitive quadratic Dirichlet character. The following lemma captures some features of χ_d which we will use repeatedly throughout the paper. Henceforth, we write m_d to denote the modulus of the Dirichlet character $\left(\frac{\epsilon_d d}{\cdot}\right)$.

Lemma 4.4.

(i) Let d be odd, and write $d = \pm p_1 \cdots p_r$. Then, for n odd, we have

$$\chi_d(n) = \prod_{p \mid d} \left(\frac{n}{p}\right) \quad \textit{and} \quad \chi_d(2n) = \chi_d(n).$$

Let d be even, and write $d = \pm 2 p_1 p_2 \cdots p_r$. Then, we have

$$\chi_d(n) = \begin{cases} \boldsymbol{\chi}_{01}(n) \prod_{1 \le i \le r} \left(\frac{n}{p_i}\right) & d \equiv 2 \pmod 8, \\ \boldsymbol{\chi}_{11}(n) \prod_{1 \le i \le r} \left(\frac{n}{p_i}\right) & d \equiv 6 \pmod 8. \end{cases}$$

[6] See for example Theorem A.1 of [9].

[7] Sieve-theoretic lower bounds which make much weaker assumptions on S exist [12, 23] but would have issues similar to those of the sieve-theoretic upper bounds were we to use them for our application.

(ii) We have

$$L(s,\chi_d) = \begin{cases} L(s, \left(\frac{\epsilon_d d}{\cdot}\right))\frac{1+2^{-s}}{1-2^{-s}} & d \equiv \pm 3 \pmod 8, \\ L(s, \left(\frac{\epsilon_d d}{\cdot}\right)) & \textit{otherwise.} \end{cases}$$

(iii) We have

$$m_d = \begin{cases} |d| & d \textit{ odd,} \\ 4|d| & d \textit{ even.} \end{cases}$$

Recall from Section 2.1 that $\boldsymbol{\chi}$ is used to refer to the quadratic characters modulo 8. In particular, $\boldsymbol{\chi}_{11}$ should not be confused with χ_d for $d = 11$, and the latter will never appear in this paper.

Proof sketch.

(i) This is a standard application of quadratic reciprocity.
(ii) If $d \not\equiv \pm 3 \pmod 8$, $\chi_d = \left(\frac{\epsilon_d d}{\cdot}\right)$. Otherwise, χ_d is multiplicative and agrees with $\left(\frac{\epsilon_d d}{\cdot}\right)$ except at 2, where it has value 1 instead of -1.
(iii) This is a standard property of the Kronecker symbol.

□

Definition 4.5. We define $N_d(y)$ to be the set of squarefree integers between 1 and y which are divisible only by primes q for which $\chi_d(q) = 1$.

We will ultimately use $N_d(\frac{x}{|d|})$ to upper bound $R_d(x)$ and $I_d(x)$. Let

$$a_n := \begin{cases} 1 & n \text{ is squarefree and divisible only by primes } q \text{ s.t. } \chi_d(q) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

We will obtain Lemma 4.2 by deriving the asymptotic behavior of $N_d(y) = \sum_{n \le y} a_n$. We can access the latter by studying the Dirichlet series defined on $\mathrm{Re}(s) > 1$ by

$$F_d(s) := \sum_{n \ge 1} a_n n^{-s}.$$

This next lemma is more general than we need in this section but we will use its full generality later.

Lemma 4.6. *If $L(s,\chi)$ is a Dirichlet L-series, we have*

$$F_d(s) \otimes L(s,\chi) = C(s) L(s,\chi)^{1/2} L(s, \chi_d\chi)^{1/2},$$

where

$$C(s) := L(2s,\chi^2)^{-1/2} \prod_{q \in S} (1 + \chi(q)q^{-s})^{-1/2} \prod_{q : \chi_d(q) = 1} (1 - \chi^2(q) q^{-2s})^{1/2}$$

extends to a holomorphic function on $\mathrm{Re}(s) > \frac{1}{2}$.

Proof. By the definition of convolution,

$$F_d(s) \otimes L(s,\chi) = \sum_{n \ge 1} a_n \chi(n) n^{-s}$$

is holomorphic on $\mathrm{Re}(s) > 1$. Because a_n is 0 whenever n is not squarefree, we have the Euler product

$$\begin{aligned} F_d(s) \otimes L(s,\chi) &= \prod_q (1 + \chi(q) a_q q^{-s}) \\ &= \prod_q (1 - \chi(q) a_q q^{-s})^{-1} \prod_q (1 - \chi^2(q) a_q^2 q^{-2s}). \end{aligned}$$

Because $a_q \in \{-1, 0, 1\}$ for all q, we have

$$\begin{aligned} &= \prod_q (1 - \chi(q) q^{-s})^{-1/2} (1 - \chi(q)\chi_d(q) q^{-s})^{-1/2} \\ &\qquad \times \prod_{q:\chi_d(q)=\text{-}1} (1 - \chi^2(q) q^{-2s})^{1/2} \prod_{q|m_d} (1 - \chi(q) q^{-s})^{1/2} \prod_q (1 - \chi^2(q) a_q^2 q^{-2s}). \end{aligned}$$

The first two terms are the local factors $L(s,\chi)^{1/2}$ and $L(s,\chi\chi_d)^{1/2}$. For the other three, we have

$$\begin{aligned} &\prod_{q:\chi_d(q)=\text{-}1} (1 - \chi^2(q) q^{-2s})^{1/2} \prod_{q|m_d} (1 - \chi(q) q^{-s})^{1/2} \prod_q (1 - \chi^2(q) a_q^2 q^{-2s}) \\ = &\prod_{q:\chi_d(q)=\text{-}1} (1 - \chi^2(q) q^{-2s})^{1/2} \prod_{q|m_d} (1 - \chi(q) q^{-s})^{1/2} \prod_{q:\chi_d(q)=1} (1 - \chi^2(q) q^{-2s}) \\ = &\prod_q (1 - \chi^2(q) q^{-2s})^{1/2} \prod_{q|m_d} (1 + \chi(q) q^{-s})^{-1/2} \prod_{q:\chi_d(q)=1} (1 - \chi^2(q) q^{-2s})^{1/2} \\ = &L(2s,\chi^2)^{-1/2} \prod_{q|m_d} (1 + \chi(q) q^{-s})^{-1/2} \prod_{q:\chi_d(q)=1} (1 - \chi^2(q) q^{-2s})^{1/2}, \end{aligned}$$

which is the expression for $C(s)$ in the lemma. This product converges absolutely and locally uniformly on $\mathrm{Re}(s) > \frac{1}{2}$ so we have holomorphicity on this region as desired. □

In this section, we will use the following simple corollary of Lemma 4.6.

Corollary 4.7. *Let $F_d(s)$ be as defined in Lemma 4.6. Then,*

$$F_d(s) = C_d(s) \zeta(s)^{1/2} L(s,\chi_d)^{1/2},$$

where

$$C_d(s) := \zeta(2s)^{-1/2} \prod_{q|m_d} (1 + q^{-s})^{-1/2} \prod_{q:\chi_d(q)=1} (1 - q^{-2s})^{1/2}$$

extends to a holomorphic function on $\mathrm{Re}(s) > \frac{1}{2}$.

Proof. Apply Lemma 4.6 with χ as the trivial character. □

To pass from the factorization of a Dirichlet series to a bound on the sum of its coefficients, we will use a Tauberian theorem given by the main theorem of Selberg-Delange theory.

Theorem 4.8 (Special case of Chapter II.5.3 Theorem 3 from [38])**.** *Suppose that $F(s) := \sum_n h_n n^{-s}$ is a Dirichlet series such that $h_n \geq 0$ for all n. Suppose further that for some $\rho \in \mathbb{C}$, $G(s) := F(s)\zeta(s)^{-\rho}$ can be analytically continued to a holomorphic function on the region* $\mathrm{Re}(s) \geq 1 - \beta$ *for some $\beta > 0$, and in this region satisfies the bound*

$$|G(s)| \leq M(1 + |\mathrm{Im}(s)|)^{1-\delta} \tag{9}$$

for some $M > 0$ and $0 < \delta \le 1$. Then,

$$\sum_{n\le x} h_n = \frac{x}{\log^{1-\rho} x}\left(\frac{G(1)}{\Gamma(\rho)} + O\big(Me^{-K\sqrt{\log x}} + \log^{-1} x\big)\right)$$

where K and the implicit constant are absolute.

With Theorem 4.8 in hand we may now pass from properties of $F_d(s)$ to the asymptotics of $N_d(y)$.

Corollary 4.9. *We have*

$$|N_d(y)| = \sum_{n\le y} a_n = \frac{(c_d' + \varepsilon_1(d,y))y}{\sqrt{\log y}}, \tag{10}$$

where

$$c_d' = \frac{1}{\Gamma(1/2)\zeta(2)^{1/2}} L(1,\chi_d)^{1/2} \prod_{q\mid m_d}\left(1+\frac{1}{q}\right)^{-1/2} \prod_{q:\chi_d(q)=1}\left(1-\frac{1}{q^2}\right)^{1/2}.$$

and

$$\varepsilon_1(d,y) \ll |d|^{1.001} e^{-K\sqrt{\log y}} + \log^{-1} y.$$

If $H(s) = A(s)F_d(s) = \sum_n h_n n^{-s}$ on $\mathrm{Re}(s) > 1$ for some $A(s)$ which extends to a bounded holomorphic function on $\mathrm{Re}(s) > \frac{1}{2}$,

$$\left|\sum_{n\le y} h_n\right| = \frac{(A(1)c_d' + \varepsilon_2(d,y))y}{\sqrt{\log y}}.$$

where again

$$\varepsilon_2(d,y) \ll |d|^{1.001} e^{-K\sqrt{\log y}} + \log^{-1} y.$$

We will need two simple bounds in the proof of Corollary 4.9.

Proposition 4.10. *Let χ be a nonprincipal Dirichlet character of modulus m. Let $s \in \mathbb{C}$.*

(i) If $\mathrm{Re}(s) > 0$, $|L(s,\chi)| \le m$.
(ii) $|L(1,\chi)| \ll \log m$.

Proof Sketch. Let $T(x) := \sum_{n<x} \chi(n)$. Proposition 4.10(i) follows by evaluating a Riemann-Stieljes integral via integration by parts and observing that $|T(x)| \le m$.

$$|L(s,\chi)| = \left|\int_1^\infty x^{-s} dT(x)\right| = \left|\int_1^\infty T(x) d(x^{-s})\right| \le m$$

Proposition 4.10(ii) follows similarly, as

$$|L(1,\chi)| \le \sum_{n\le m} \frac{1}{n} + \left|\int_m^\infty x^{-s} dT(x)\right| \ll \log m.$$

□

Theorem 4.11 ([30])**.** *For $n \in \mathbb{N}$, let $\sigma(n)$ denote the sum of the positive divisors of n. Then, for all $n \ge 3$,*

$$\sigma(n) < e^\gamma n \log\log n + \frac{0.6483n}{\log\log n},$$

where γ is the Euler-Mascheroni constant.

Corollary 4.12. *For $n \in \mathbb{N}$ squarefree and $s \in \mathbb{C}$ with $\mathrm{Re}(s) \ge 1 - \beta$ for $\beta \in [0,1)$,*

$$\left|\prod_{q\mid n}(1-q^{-s})\right| \le n^\beta \left(e^\gamma \log\log n + \frac{0.6483}{\log\log n}\right).$$

Proof.

$$\left|\prod_{q|n}(1-q^{-s})\right| \le \prod_{q|n}(1+q^{-(1-\beta)}) = \prod_{q|n}\frac{q^{1-\beta}+1}{q^{1-\beta}} \le \prod_{q|n}\frac{q+1}{q^{1-\beta}} \le \frac{\sigma(n)}{n^{1-\beta}},$$

and applying Theorem 4.11 yields the result. □

Proof of Corollary 4.9. Recall the factorization of $F_d(s)$ that we obtained from Corollary 4.7. We want to apply Theorem 4.8 with $\rho = \frac{1}{2}$ and

$$G(s) = L(s,\chi_d)^{1/2}C_d(s), \tag{11}$$

since we know that $L(s,\chi_d)$ can be analytically continued to $\mathbb{C}$ and C_d is holomorphic on the region $\mathrm{Re}(s) > \frac{1}{2}$. Fix $\beta = \frac{1}{4}$ (we could take any $\beta \in (0, \frac{1}{2})$). We need to bound $G(s)$ on the region $\mathrm{Re}(s) > 1-\beta$. By Proposition 4.10 we have $|L(s, \left(\frac{\epsilon_d d}{\cdot}\right))| \le m_d$, so Lemma 4.4 tells us that $|L(s,\chi_d)| \ll m_d$. By Corollary 4.12,

$$\left|\prod_{q|m_d}(1-q^{-s})^{1/2}\right| \ll \left(\log\log m_d + \frac{1}{\log\log m_d}\right)^{1/2}.$$

Lastly, observe that

$$\prod_{q:\chi_d(q)=\text{-}1}(1-q^{-2s})^{1/2} \le |\zeta(2(1-\beta))^{1/2}|.$$

This means that Theorem 4.8 can be applied with $M \ll |d|^{1.001}$, giving us (10) with constant

$$c_d' = \frac{G(1)}{\Gamma(1/2)}$$

and error

$$\varepsilon_1(d,y) \ll |d|^{1.001}e^{-K\sqrt{\log y}} + \log^{-1} y.$$

□

Proof of Lemma 4.2. Recall that $R_d(x)$ and $I_d(x)$ are the number of n of the appropriate sign which satisfy all of the criteria in Theorem 2.6. Because the lower bound is already known, all we need is an upper bound. The case $|x| \le |d|$ is trivial as $R_d(d) \le 1$, so we assume that $x > d$. It suffices to count those n which satisfy just 2.6(i). We give the proof for $R_d(x)$ but because this criterion is independent of the sign of n the same approach will work for $I_d(x)$.

Putting this together, we see that $R_d(x) \le N_d(\frac{x}{|d|})$ because we require that $|dn| \le x$.

Plugging this into Corollary 4.9, we have

$$R_d(x) \le \frac{(c_d' + \varepsilon_1(d, \frac{x}{|d|}))x}{|d|\sqrt{\log x - \log|d|}}.$$

We can replace $\sqrt{\log x - \log|d|}$ in the denominator with $\sqrt{\log x}$ by multiplying the numerator by

$$\sqrt{\frac{\log x}{\log x - \log|d|}} = \left(1 - \frac{\log|d|}{\log x}\right)^{-1/2}.$$

Then, we have

$$R_d(x) \le \frac{\left(c_d' + \varepsilon_1(d, \frac{x}{|d|})\right)\left(1 - \frac{\log|d|}{\log x}\right)^{-1/2} x}{|d|\sqrt{\log x}} \ll \frac{(1+o_d'(1))c_d' x}{|d|\sqrt{\log x}}$$

as desired. □

Proof of Theorem 4.1. We will give the proof for $R(x)$; the analogous proof works for $I(x)$. If $\mathbb{Q}(\sqrt{m})$ admits a curve with good reduction everywhere then some good d must divide m. There could be multiple good d that divide a given m, but at least as an upper bound we have

$$R(x) \leq \sum_{\substack{d \text{ good} \\ |d| \leq x}} R_d(x)$$

Per Lemma 4.2, we have for any $z \leq x$ that

$$\sum_{\substack{d \text{ good} \\ |d| \leq x}} R_d(x) \ll x \left(\sum_{\substack{d \text{ good} \\ |d| \leq z}} \frac{(1+o'_d(1))c'_d}{|d|\sqrt{\log x}} + \sum_{\substack{d \text{ good} \\ |d| \geq z}} \frac{1}{|d|} \right), \tag{12}$$

where for the second sum we have used that we always have a bound of $\frac{x}{|d|}$ on the number of natural numbers up to x which are multiples of $|d|$.

Theorem B tells us that the set of good d is $\frac{1}{3}$-polynomially sparse. Therefore, by Lemma 2.1(ii),

$$\sum_{\substack{d \text{ good} \\ |d| \geq z}} \frac{1}{|d|} \ll z^{-1/3}.$$

If we take $z := \log^{3/2+\delta}(x)$ for $\delta > 0$ the second term on the right-hand-side of (12) will be negligible compared to the first. By the definition of $o'_d(1)$ in Section 2.1, the error term in the numerator of the first term on the right-hand-side of (12) goes to zero as x goes to infinity when $|d| \leq z$.

Putting everything together, we can rewrite (12) as

$$\sum_{\substack{d \text{ good} \\ |d| \leq x}} R_d(x) \ll \frac{x}{\sqrt{\log x}} \sum_{\substack{d \text{ good} \\ |d| \leq y}} \frac{c'_d}{|d|}.$$

Now we upper bound c'_d. By applying Proposition 4.10(ii) (with $s = 1$) and Corollary 4.12 (with $\beta = 0$) to (4.9), we see that

$$c'_d \ll |d|^{0.001},$$

meaning we need to bound the sum of $\frac{1}{|d|^{.999}}$. Because $.999 + \frac{1}{3} > 1$, applying Lemma 2.1(i) with $\alpha = \frac{1}{3}$ and $\kappa = .999$ tells us that the sum in question converges. Therefore,

$$R(x) \ll \frac{x}{\sqrt{\log x}}.$$

as desired. □

5. An Upper Bound on the Constant

We are now ready to begin the proof of our main theorem, which we recall for convenience.

Theorem A. *Assuming the abc-conjecture,*

$$R(x) \sim \frac{c_R x}{\sqrt{\log x}} \quad \textit{and} \quad I(x) \sim \frac{c_I x}{\sqrt{\log x}}$$

where

$$c_R = \sum_{\substack{d \in \mathbb{Z} \\ d \text{ good}}} \frac{c'_d c''_{d,R}}{|d| 2^{\omega(d)}} \quad \textit{and} \quad c_I = \sum_{\substack{d \in \mathbb{Z} \\ d \text{ good}}} \frac{c'_d c''_{d,I}}{|d| 2^{\omega(d)}},$$

where the set of good d is defined in (7)*, c'_d is as in Corollary 4.9 and $c''_{d,R}$ and $c''_{d,I}$ are as in Lemma 5.1.*

In this section, we show that the expressions in Theorem A are upper bounds on the correct values of c_R and c_I.

The main lemma of this section gives a sharp version of Lemma 4.2. Once again recall the definition of $o'_d(1)$ from Section 2.1.

Lemma 5.1. *Let d be good. Then,*

$$R_d(x) = \frac{(1+o'_d(1))c'_d c''_{d,R} x}{|d|2^{\omega(d)}\sqrt{\log x}} \quad \text{and} \quad I_d(x) = \frac{(1+o'_d(1))c'_d c''_{d,I} x}{|d|2^{\omega(d)}\sqrt{\log x}},$$

where c'_d is as defined in Corollary 4.9,

$$c''_{d,R} := \begin{cases} 1 & d \equiv \pm 1 \pmod 8 \\ \frac{2}{3} & d \equiv \pm 3 \pmod 8 \\ \frac{1}{4} & d \equiv 2 \pmod 8 \quad \text{and} \quad d > 0 \\ \frac{1}{4} & d \equiv 6 \pmod 8 \\ 0 & \text{otherwise,} \end{cases}$$

$$c''_{d,I} := \begin{cases} 1 & d \equiv 1 \pmod 8 \quad \text{and} \quad d > 0 \\ 1 & d \equiv 7 \pmod 8 \quad \text{and} \quad d < 0 \\ \frac{2}{3} & d \equiv 3 \pmod 8 \quad \text{and} \quad d < 0 \\ \frac{2}{3} & d \equiv 5 \pmod 8 \quad \text{and} \quad d > 0 \\ \frac{1}{4} & d \equiv \pm 2 \pmod 8 \quad \text{and} \quad d < 0 \\ 0 & \text{otherwise.} \end{cases}$$

Remark. Notice that $c''_{d,R} \geq c''_{d,I}$ except when d is a negative number congruent to 2 (mod 8). Per Theorem A,

$$c_R - c_I = \sum_{d \text{ good}} \frac{c'_d(c''_{d,R} - c''_{d,I})}{|d|2^{\omega(d)}}.$$

This provides strong evidence that $c_R > c_I$ under the *abc*-conjecture, but does not provide a proof without better control over the distribution of good d and its correlation with $\frac{c'_d}{2^{\omega(d)}}$ than we are able to show. We prove $c_R > c_I$ in a different manner, assuming a different hypothesis, in Section 7.

In the proof of Lemma 4.2 it was sufficient to consider Theorem 2.6(i). Now, we will need to consider all five conditions. Observe that while 2.6(i) imposes a condition on the primes that are allowed to divide n, (ii)-(iv) constrain the value of n modulo the primes dividing d and modulo 4 or 8. These thus correspond to (c) in Section 1.2. As discussed then, the Dirichlet series (of the indicator function) for this property is not multiplicative, complicating any application of Theorem 4.8. We address this by expressing the series as a linear combination of Dirichlet-L-series. Intuitively, a Tauberian theorem can be thought of as telling us the "rate of divergence" at a pole, and hence only terms which possess a pole at $s = 1$ will contribute to the overall asymptotic.

Proof. We start with the bound for $R_d(x)$. If d is odd we write $d = \pm p_1 p_2 \dots p_r$ and if d is even we write $d = 2d' = \pm 2 p_1 p_2 \dots p_r$. We will count positive numbers n such that $\mathbb{Q}(\sqrt{dn\,\mathrm{sgn}(d)})$ has discriminant with absolute value at most x and admits an elliptic curve with good reduction everywhere and rational j-invariant. *Note that this n is different from the n in Theorem 2.6 as it is always positive.*

For any valid pair of (d, n), Theorem 2.6 tells us that the following conditions on n and d hold:

(a) n is coprime to d[8];
(b) n is squarefree;
(c) $\chi_d(q) = 1$ for every $q \mid n$;
(d) $\left(\frac{n}{p}\right) = \left(\frac{-\operatorname{sgn}(d)\epsilon_d}{p}\right)$ for every odd $p \mid d$.

Let us check what we need for these conditions to be compatible with one another. Assume that (a) and (b) hold for some d and n. By Lemma 4.4, (c) tells us the value of the product

$$\prod_{p|d} \left(\frac{q}{p}\right)$$

for each $q|n$. Similarly, (d) tells us something about

$$\prod_{q|n} \left(\frac{q}{p}\right) = \left(\frac{n}{p}\right)$$

for each $p|d$. Let M be a matrix with rows and columns indexed by $p_i|d$ and $q_j|n$ respectively and with entries $M_{ij} := \left(\frac{q_j}{p_i}\right)$. Then, (c) tells us what the product along each column ought to be and (d) tells us what the product along each row ought to be.

A necessary and sufficient condition for compatibility of (c) and (d) is that the product of all the row products must equal the product of all the column products, as they are both the product of all entries in M.

Let us now branch into three cases based on the additional conditions from Theorem 2.6 which are relevant to each: $d \equiv \pm 1 \pmod 8$, $d \equiv \pm 3 \pmod 8$, and $d \equiv \pm 2 \pmod 8$.

(1) $\boldsymbol{d \equiv \pm 1 \pmod 8}$: In this case, we have

$$\prod_{q|n}\prod_{p|d} \left(\frac{q}{p}\right) = \prod_{q|n} \chi_d(q) = 1, \tag{13}$$

where we have used that $\prod_{p|d} \left(\frac{2}{p}\right) = \boldsymbol{\chi}_{11}(|d|) = 1$.

We have incompatibility of (c) and (d) if

$$\prod_{p|d} \left(\frac{-\operatorname{sgn}(d)\epsilon_d}{p}\right) = -1,$$

which happens if and only if $\operatorname{sgn}(d)\epsilon_d = 1$ and an odd number of the p are congruent to $3 \pmod 4$. The latter condition is equivalent to $\operatorname{sgn}(d)\epsilon_d = -1$, so this is never an issue.

Because we are ordering the quadratic fields $\mathbb{Q}(\sqrt{m})$ by discriminant rather than by m, we must also keep track of the congruence class of n modulo 4 so that when $m = dn \operatorname{sgn}(d) \equiv 2, 3 \pmod 4$ we only take values of n up to $\frac{x}{4|d|}$. We thus distinguish the (sub)cases where $nd \operatorname{sgn} d \equiv 1 \pmod 4$, $nd \operatorname{sgn} d \equiv 3 \pmod 4$, and n even. Denote by $R_d(x)\big|_{a(k)}$ the number of n such that $dn \operatorname{sgn}(d) \equiv a \pmod k$ and such that $\mathbb{Q}(\sqrt{dn \operatorname{sgn}(d)})$ has discriminant at most x and admits an elliptic curve with $\mathrm{GRE}_{\mathbb{Q}}$. Let us start with $R_d(x)\big|_{1(4)}$, corresponding to the additional condition

(e) $\left(\frac{-4}{n}\right) = \left(\frac{-4}{d \operatorname{sgn}(d)}\right)$.

Let $(b_n)_{n\geq 1}$ be the sequence of coefficients of the Dirichlet series

$$\left(\frac{1}{2}\left(L(s, \boldsymbol{\chi}_2) + \left(\frac{-4}{d \operatorname{sgn}(d)}\right) L\left(s, \left(\frac{-4}{\cdot}\right)\right)\right)\right) \otimes \left(\bigotimes_{i=1}^{r-1} \frac{1}{2}\left(\zeta(s) + \left(\frac{-\operatorname{sgn}(d)\epsilon_d}{p_i}\right) L\left(s, \left(\frac{\cdot}{p_i}\right)\right)\right)\right), \tag{14}$$

[8] This condition is redundant in light of (c) but we include it for clarity.

where we write $\boldsymbol{\chi}_2$ to denote the (principal) Dirichlet character with modulus 2. Note that the big convolution is over only $r-1$ primes – we (arbitrarily) omit one of the prime factors of d. Consider any term in the big convolution. It corresponds to a Dirichlet series with a sequence of coefficients whose n^{th} term – assuming n is coprime to d – is 1 if $\left(\frac{n}{p}\right) = \left(\frac{-\operatorname{sgn}(d)\epsilon_d}{p}\right)$ and 0 otherwise. Because $(a_n)_{n\geq 1}$ is 0 whenever n and d are not coprime by (a), we do not need to worry about the behavior of $(b_n)_{n\geq 1}$ when n and d are not coprime.

The term outside the big convolution corresponds to a Dirichlet series with a sequence of coefficients whose n^{th} term is 1 if

$$\left(\tfrac{-4}{n}\right) = \left(\tfrac{-4}{d\operatorname{sgn}(d)}\right)$$

and is 0 otherwise.

Assuming that n satisfies (a)-(c), we see that that $(b_n)_{n\geq 1}$ is contstructed so as to be 1 if and only if (e) is satisfied (because of the first term in (14)) and (d) is satisfied for all but one of the primes dividing d, and to be 0 otherwise. However, we actually have more than this. Since

$$\prod_{p_i\mid d}\left(\tfrac{-\operatorname{sgn}(d)\epsilon_d}{p_i}\right) = 1,$$

we see that knowing $\left(\frac{n}{p_i}\right)$ for $1 \leq i \leq r-1$ tells us $\left(\frac{n}{p_r}\right)$. We are exploiting here that we know that (c) and (d) are compatible. Thus, $a_n = b_n = 1$ if and only if (a)-(e) are satisfied. We have that

$$R_d(x)\big|_{1(4)} = \sum_{n\leq x} a_n b_n.$$

We will access this by applying Theorem 4.8 to

$$\sum_{n\geq 1} a_n b_n n^{-s} = F_d(s) \otimes \left(\sum_{n\geq 1} b_n n^{-s}\right).$$

Expanding out the convolutions of $\sum_n b_n n^{-s}$ in (14) yields a sum of Dirichlet L-series, each associated with a product of Kronecker characters. By Lemma 4.6, convolving $F_d(s)$ with $L(s,\chi)$ for any Dirichlet character χ gives

$$C(s)L(s,\chi)^{1/2}L(s,\chi\chi_d)^{1/2} \tag{15}$$

where $C(s)$ is holomorphic on $\operatorname{Re}(s) > \frac{1}{2}$. (15) will not have a singularity at $s=1$ unless at least one of χ or $\chi\chi_d$ is principal. Because χ_d is primitive and real, $\chi\chi_d$ is principal if and only if χ is an extension by zero of χ_d. This can happen only if the modulus of χ is divisible by m_d. However, none of the characters in (14) are zero at the omitted prime factor. Thus (15) has a singularity only when χ is principal. By Lemma 4.6, the term of interest is

$$\begin{aligned} F_d(s) \otimes \left(\frac{1}{2^{\omega(d)}}\boldsymbol{\chi}_2\right) =& \frac{1}{2^{\omega(d)}} L(s,\boldsymbol{\chi}_2)^{1/2} L(s,\boldsymbol{\chi}_2\chi_d)^{1/2} L(2s,\boldsymbol{\chi}_2)^{-1/2} \\ &\times \prod_{q\mid m_d}(1+\boldsymbol{\chi}_2(q)q^{-s}) \prod_{q:\chi_d(q)=1}(1-\chi^2(q)q^{-2s})^{1/2}. \end{aligned}$$

Observing that

$$L(s,\boldsymbol{\chi}_2)^{1/2} = \zeta(s)^{1/2}(1-2^{-s})^{1/2},$$
$$L(s,\boldsymbol{\chi}_2\chi_d)^{1/2} = L(s,\chi_d)^{1/2}(1-2^{-s})^{1/2},$$
$$L(2s,\boldsymbol{\chi}_2)^{-1/2} = \zeta(2s)^{-1/2}(1-2^{-2s})^{-1/2},$$

$\boldsymbol{\chi}_2(q) = 1$ for all $q|m_d$, and $\chi_d(2) = 1$, we see that

$$F_d(s) \otimes \left(\frac{1}{2^{\omega(d)}}L(s,\boldsymbol{\chi}_2)\right) = \frac{1}{2^{\omega(d)}}(1+2^{-s})^{-1}F_d(s).$$

Now, applying Corollary 4.9 gives

$$R_d(x)\big|_{1(4)} = \sum_{n\leq x} a_n b_n = \frac{\frac{2}{3}(1+o_d'(1))c_d' x}{|d|2^{\omega(d)}\sqrt{\log x}}$$

where the sum is up to x because in this case $m = nd\,\mathrm{sgn}(d) \equiv 1 \pmod 4$.

We can run a similar argument for $R_d(x)|_{3(4)}$. In this case, we can take $\sum_{n\geq 1} b_n n^{-s}$ to be

$$\left(\frac{1}{2}\left(L(s,\boldsymbol{\chi}_2) - \left(\tfrac{-4}{d\,\mathrm{sgn}(d)}\right) L\left(s, \left(\tfrac{-4}{\cdot}\right)\right)\right)\right) \otimes \left(\bigotimes_{i=1}^{r-1} \frac{1}{2}\left(\zeta(s) + \left(\tfrac{-\mathrm{sgn}(d)\epsilon_d}{p_i}\right) L\left(s, \left(\tfrac{\cdot}{p_i}\right)\right)\right)\right),$$

but since the only surviving term corresponds to $L(s,\boldsymbol{\chi}_2)$ the sign change in the first term of the product is irrelevant. The same argument as above yields

$$R_d(x)\big|_{3(4)} = \sum_{n\leq \frac{x}{4}} a_n b_n = \frac{\frac{2}{3}(1+o_d'(1))c_d' x}{4|d|\cdot 2^{\omega(d)}\sqrt{\log x}},$$

where we only consider n up to $\frac{x}{4}$ because there is an additional factor of 4 in $\Delta_{\mathbb{Q}(\sqrt{m})}$ when $m = dn\,\mathrm{sgn}(d) \equiv 3 \pmod 4$.

When computing $R_d(x)\big|_{2(4)}$ we have the added condition

(e) n is even.

We can filter out odd n by convolving with $\zeta(s) - L(s,\chi_2)$, meaning that we can take $\sum_{n\geq 1} b_n n^{-s}$ to be

$$(\zeta(s) - L(s,\boldsymbol{\chi}_2)) \otimes \left(\bigotimes_{i=1}^{r-1} \frac{1}{2}\left(\zeta(s) + \left(\tfrac{-\mathrm{sgn}(d)\epsilon_d}{p_i}\right) L\left(s, \left(\tfrac{\cdot}{p_i}\right)\right)\right)\right),$$

As such, we have

$$F_d(s) \otimes \frac{1}{2^{\omega(d)-1}}\zeta(s) - F_d(s) \otimes L(s,\boldsymbol{\chi}_2).$$

Thus, by Corollary 4.9,

$$R_d(x)\big|_{2(4)} = \frac{\frac{1}{3}(1+o_d'(1))c_d' x}{4|d|\cdot 2^{\omega(d)-1}\sqrt{\log x}}.$$

Adding together the contributions from $1, 2$, and $3 \pmod 4$, we see that

$$R_d(x) = \frac{(1+o_d'(1))c_d' x}{|d|2^{\omega(d)}\sqrt{\log x}}$$

(2) $\boldsymbol{d \equiv \pm 3 \pmod 8}$: Conditions (a)-(d) still apply. In addition, we require that

(e) $m \equiv 1 \pmod 4$.

Note that even though $\boldsymbol{\chi}_{11}(d) \neq 1$, (e) ensures that n is odd and hence (13) still holds, meaning that (a)-(d) are compatible. Additionally, (e) ensures that we need to consider just the case $R_d(x)\big|_{1(4)}$, and the computation is the same as in the $d \equiv \pm 1 \pmod 8$ case, yielding

$$R_d(x) = \frac{\frac{2}{3}(1+o_d'(1))c_d' x}{|d| 2^{\omega(d)}\sqrt{\log x}}.$$

(3) $\boldsymbol{d \equiv \pm 2 \pmod 8}$: As usual, (a)-(d) still apply. We also have the additional condition

(e) $n \equiv d+1 \pmod 8$.

We start with $d \equiv 6 \pmod 8$ as it is simpler. We have by (e) that $\boldsymbol{\chi}_{11}(n) = 1$ in this case and hence (13) holds. In addition,

$$\prod_{i=1}^{r} \left(\frac{\operatorname{sgn} d}{p_i}\right) = 1, \tag{16}$$

because even if $\operatorname{sgn} d = -1$, that $d \equiv 6 \pmod 8$ implies that we have $d' \equiv 3 \pmod 4$ and hence an even number of the primes dividing d' are $3 \pmod 4$ (since $d < 0$). Thus, we have compatibility of (c)-(e).

As before, we now make the stronger claim that we only need to check (c), (e), and (d) at all but one (odd) prime dividing d to ensure that all three are satisfied. Suppose that $\chi_d(n) = 1$, $n \equiv 7 \pmod 8$, and for $1 \leq i \leq r-1$,

$$\left(\frac{n}{p_i}\right) = \left(\frac{\operatorname{sgn} d}{p_i}\right).$$

Then, we see that for such n

$$1 = \chi_d(n) = \boldsymbol{\chi}_{11}(n) \prod_{1 \leq i \leq r} \left(\frac{n}{p_i}\right) = \left(\frac{n}{p_r}\right) \prod_{i=1}^{r-1} \left(\frac{\operatorname{sgn} d}{p_i}\right)$$

and comparing with (16) we have that

$$\left(\frac{n}{p_r}\right) = \left(\frac{\operatorname{sgn} d}{p_r}\right).$$

It is sufficient to use $\sum_n b_n n^{-s}$ to check that $n \equiv 7 \pmod 8$ and the fourth condition for all but the last odd prime dividing d. We already know how to enforce the quadratic residuosity conditions. To force $n \equiv 7 \pmod 8$, consider the function $\mathbf{1}_{7(8)} \colon (\mathbb{Z}/8\mathbb{Z})^\times \to \mathbb{C}$ that is 1 on $7 \pmod 8$ and 0 everywhere else. The Fourier expansion of this function is

$$\mathbf{1}_{7(8)} = \tfrac{1}{4}(\boldsymbol{\chi}_{00} - \boldsymbol{\chi}_{01} - \boldsymbol{\chi}_{10} + \boldsymbol{\chi}_{11}).$$

The initial factor we will add to our expression for $\sum_n b_n n^{-s}$ in this case is thus

$$\tfrac{1}{4}(\zeta(s) - L(s, \boldsymbol{\chi}_{01}) - L(s, \boldsymbol{\chi}_{10}) + L(s, \boldsymbol{\chi}_{11})),$$

where we can use $\zeta(s)$ instead of $L(s, \boldsymbol{\chi}_{00})$ as the coefficients of this factor at even indices are irrelevant. Therefore, we may take $\sum_{n \geq 1} b_n n^{-s}$ to be

$$\tfrac{1}{4}(\zeta(s) - L(s, \boldsymbol{\chi}_{01}) - L(s, \boldsymbol{\chi}_{10}) + L(s, \boldsymbol{\chi}_{11})) \otimes \left(\bigotimes_{i=1}^{r-1} \frac{1}{2} \left(\zeta(s) + \left(\frac{\operatorname{sgn} d}{p_i}\right) L\left(s, \left(\frac{\cdot}{p_i}\right)\right)\right)\right).$$

Following the same logic as before, we see that the only term of $\sum_n b_n n^{-s}$ that yields a term with a singularity at $s = 1$ after convolving with $\sum_n a_n n^{-s}$ is the term corresponding to $\zeta(s)$. Therefore,

$$R_d(x) = \sum_{n \leq \frac{x}{4}} a_n b_n = \frac{(1+o_d'(1))c_d' x}{4|d| 2^{\omega(d)}\sqrt{\log x}},$$

noting in this case that $r := \omega(d) - 1$.

When $d \equiv 2 \pmod 8$ the situation is less simple. By Lemma 4.4 we have

$$1 = \chi_d(n) = \boldsymbol{\chi}_{01}(n) \prod_{1\leq i\leq r} \left(\frac{n}{p_i}\right) = -\prod_{q|n}\prod_{p|d} \left(\frac{q}{p}\right),$$

meaning that (a)-(e) are incompatible when

$$\prod_{i=1}^{r} \left(\frac{-\operatorname{sgn}(d)}{p_i}\right) = 1.$$

This happens when $\operatorname{sgn}(d) < 0$. If we assume $\operatorname{sgn}(d) > 0$ then we have compatibility and get the same answer as we got when $d \equiv 6 \pmod 8$.

In the imaginary case, (a)-(c) are the same but we instead have

(d) $\left(\frac{n}{p}\right) = \left(\frac{\operatorname{sgn}(d)\epsilon_d}{p}\right)$ for every odd $p \mid d$.

The logic when d is odd is identical except that the compatibility between (c) and (d) now plays a role. (d) forces

$$\left(\frac{n}{p}\right) = \left(\frac{\operatorname{sgn}(d)\epsilon_d}{p}\right)$$

for every odd $p \mid d$. There is no way that (c) can also be satisfied if $\operatorname{sgn}(d)\epsilon_d = -1$[9]. When d is even, (c) and (d) are incompatible only when $d > 0$ and $d \equiv 6 \pmod 8$. We also have the restriction from 2.6(v), forbidding $d > 0$ when d is even. □

Remark. In principle, we could have used sequences $(b_n)_{n\geq 1}$ which include all the prime factors of d. This approach yields multiple terms with singularities after convolution because our character expansion of $\sum_n b_n n^{-s}$ has terms which are Dirichlet L-series for characters χ induced by χ_d. Our approach simplifies the computation.

6. A Matching Lower Bound: Proving Theorem C and Theorem A

Consider the upper bound on $R(x)$ (the same logic works for $I(x)$ as well). Using Lemma 5.1 instead of Lemma 4.2 in the proof of Theorem 4.1 tells us that

$$R(x) \leq \sum_{d \text{ good}} R_d(x) \sim \frac{x}{\sqrt{\log x}} \left(\sum_{d \text{ good}} \frac{c'_d c''_d}{|d|} \right). \tag{17}$$

This is a priori only an upper bound because we may be double-counting – if d_1 and d_2 are both good and both divide m then $\mathbb{Q}(\sqrt{m})$ may be double-counted in (17) since it could be that $\frac{m}{d_1}$ contributes to $R_{d_1}(x)$ and $\frac{m}{d_2}$ contributes to $R_{d_2}(x)$. Write $R_{d_1,d_2}(x)$ to denote the set of positive numbers n such that $K = \mathbb{Q}(\sqrt{\operatorname{lcm}(d_1,d_2)n})$ admits an elliptic curve with good reduction everywhere and Δ_K is at most x. Then, by inclusion-exclusion, we have the lower bound

$$R(x) \geq \sum_{d \text{ good}} R_d(x) - \sum_{d,d' \text{ good}} R_{d,d'}(x). \tag{18}$$

The idea is that this second term ends up being $\asymp \frac{x}{\log^{3/4} x}$ and hence is negligible compared to the first term (which is $\asymp \frac{x}{\sqrt{\log x}}$ by Theorem 4.1). As in the proof of Theorem 4.1, there are two parts to this result. We first show that the sum of $\frac{1}{\operatorname{lcm}(d,d')}$ over pairs of good d and d' is constant. Then, we show that the dependence on x of any $R_{d,d'}(x)$ is $\asymp \frac{x}{\log^{3/4} x}$. For the former, we show that the number of pairs (d,d') where d and d' are good, have absolute value at most x, and $\operatorname{lcm}(d,d') \leq x$

[9] As an aside, notice that this is exactly the fifth constraint of Theorem 2.6! This means that the fifth constraint of Theorem 2.6 is redundant for odd d.

is $x^{1-\kappa+o(1)}$ for some $\kappa > 0$. Then, the first part of Lemma 2.1 implies that the sum of reciprocals of least common multiples with multiplicity is some absolute constant.

Theorem C. *A set $S \subseteq \mathbb{N}$ of squarefree numbers is called β-polynomially sparse if there is a constant $\beta \in (0,1)$ such that*

$$\#\{n \leq x \colon n \in S\} \leq x^{1-\beta+o(1)}$$

as x approaches $+\infty$. For any such S, the set

$$\{(n,n') \colon n \in S, n' \in S, \operatorname{lcm}(n,n') \leq x\}.$$

is $\frac{\beta}{2-\beta}$-polynomially sparse. Furthermore, there are sets for which this is tight.

As motivation for Theorem C, notice that the analogous result where least common multiple is replaced by product holds with $\kappa = \beta$. To see this, consider splitting the range $[1,x]$ into intervals $(y,2y]$. For each $a \in (y,2y]$, any $b \in [1,x]$ such that $ab \leq x$ is at most $\frac{x}{y}$. There are at most $\left(\frac{x}{y}\right)^{1-\beta+o(1)}$ such values of b. The number of possible values of $a \in (y,2y]$ is at most $y^{1-\beta+o(1)}$. Therefore, the number of tuples (a,b) where $a \in (y,2y]$ is at most

$$y^{1-\beta+o(1)}\left(\frac{x}{y}\right)^{1-\beta+o(1)} = x^{1-\beta+o(1)}.$$

This is uniform in y and there are at most $\log x + 1$ intervals $(y,2y]$. Therefore, the total number of pairs (a,b) which work is at most $x^{1-\beta+o(1)}(\log x + 1) = x^{1-\beta+o(1)}$. The structure of our proof of Theorem C is similar. The main difficulty is that $\operatorname{lcm}(a,b)$ may be much smaller than ab so it is harder to control the number of b which can be associated to a given a.

We present an improved proof of Theorem C due to Ashwin Sah and Mehtaab Sawhney, and we thank them for allowing us to present it in this paper[10]. We will use the following standard lemma.

Lemma 6.1. *The number of divisors of n is $\exp(O(\log n/\log\log n)) = n^{o(1)}$.*

Proof of Theorem C. We wish to bound the total number of pairs $(a,b) \in S \times S$ with $\operatorname{lcm}(a,b) \leq x$. We consider such pairs with $a \in [y,2y), b \in [z,2z)$, $g := \gcd(a,b) \in [g,2g)$ for some $yz \geq x$ (if $yz \leq x$ then we can just use the product argument above). Note that $g \leq \min(2y,2z)$. We will show that the number of pairs with a, b, and g in these ranges is at most $x^{1-\kappa+o(1)}$. Then, summing the contributions from all such triples of intervals only adds a factor of $O(\log^3 x) = x^{o(1)}$ to the overall bound if we take a dyadic decomposition.

First, observe that

$$x \geq \operatorname{lcm}(a,b) = \frac{ab}{\gcd(a,b)} \geq \frac{yz}{2g}.$$

There are at most $O(y^{1-\beta+o(1)})$ choices of a and at most $O(z^{1-\beta+o(1)})$ choices of b by β-polynomial sparsity of S. Therefore, there are at most $(yz)^{1-\beta+o(1)}$ choices of pairs. Because $yz \leq 2xg$, this is

$$(xg)^{1-\beta+o(1)}. \tag{19}$$

We can bound the number of pairs another way. There are at most $y^{1-\beta+o(1)}$ choices of a. For each such a, there are then $x^{o(1)}$ divisors of a lying in $[g,2g]$ (i.e. choices for $\gcd(a,b)$) by Lemma 6.1. There are $O(\frac{z}{g})$ choices of b divisible by this choice of $\gcd(a,b)$. This gives a bound of $x^{o(1)}y^{1-\beta}z/g$.

We may obtain a symmetric bound by swapping the roles of a, b, giving a bound of

$$x^{o(1)} \cdot \min\left(y^{1-\beta}z/g, yz^{1-\beta}/g\right).$$

[10] The original proof of the result, due to the authors, gave only an upper bound and had a slightly larger exponent.

Taking the geometric mean of the two terms in the minima gives

$$x^{o(1)}(yz)^{1-\beta/2}/g = x^{1-\beta/2+o(1)}/g^{\beta/2}, \tag{20}$$

using again that $yz \le 2xg$.

Combining (19) and (20), we obtain a bound of

$$\min\left((xg)^{1-\beta+o(1)}, x^{1-\beta/2+o(1)}/g^{\beta/2}\right).$$

This is maximized when the two terms are approximately equal, which happens when g becomes $x^{\beta/(2-\beta)+o(1)}$. This yields the bound

$$x^{1-\frac{\beta}{2-\beta}},$$

implying $\beta/(2-\beta)$-polynomial sparsity.

For the matching lower bound, consider the set S constructed as follows. Let $\kappa := \beta/(2-\beta)$. Pick some positive integer x_0 and add to S the multiples of $\lceil x_0^\kappa \rceil$ in the interval $\left[\frac{1}{2}x_0^{(1+\kappa)/2}, x_0^{(1+\kappa)/2}\right)$. Then, we have added at most $x_0^{(1-\kappa)/2}$ values to S, the least common multiple of any pair of such values is at most x_0, and the number of tuples of elements is $x_0^{1-\kappa}$. Continue by choosing x_1 much larger than x_0 and repeating the process for each x_i for all $i \in \mathbb{N}$.

The number of elements of S up to x grows as

$$x^{\frac{1-\kappa}{1+\kappa}} = x^{1-\beta},$$

and the number of least common multiples up to x grows as $x^{1-\kappa+o(1)}$, so we see that we have a lower bound matching our upper bound. □

Applied to the set of good d, which by Theorem B satisfies the conditions of Theorem C for $\beta = 1/3$, we can take $\kappa = 1/5$.

Lemma 6.2.

$$R_{d,d'}(x) \ll \frac{(1+o'_{dd'}(1))c'_{dd'}x}{\operatorname{lcm}(|d|,|d'|)\log^{3/4} x} \quad \textit{and} \quad I_{d,d'}(x) \ll \frac{(1+o'_{dd'}(1))c'_{dd'}x}{\operatorname{lcm}(|d|,|d'|)\log^{3/4} x},$$

where $c'_{dd'} \ll \operatorname{lcm}(|d|,|d'|)^{0.001}$ *and* $o'_{dd}(1)$ *denotes some function of* x *and* d *which goes to* 0 *as* $\frac{x}{\operatorname{lcm}(|d|,|d'|)}$ *goes to infinity.*

Proof. As in the proof of Lemma 4.2, we will use only the first constraint from Theorem 2.6 and order quadratic fields $\mathbb{Q}(\sqrt{m})$ by m rather than by discriminant. Let S (resp. S') be the set of primes q such that $\chi_d(q) = 1$ (resp. $\chi_{d'}(q) = 1$). An upper bound on $R_{d,d'}(x)$ is the number of n at most $\frac{x}{\operatorname{lcm}(|d|,|d'|)}$ which are divisible only by primes in $S \cap S'$[11]. We have that when q is coprime to d and d',

$$\frac{1}{4}(\chi_d(q)+1)(\chi_{d'}(q)+1) = \begin{cases} 1 & q \in S \cap S' \\ 0 & q \notin S \cap S' \end{cases}$$

The expression on the left-hand-side can be written as

$$\frac{1}{4}(1 + \chi_d(q) + \chi_{d'}(q) + \chi_d\chi_{d'}(q)).$$

Let

$$a_n := \begin{cases} 1 & n \text{ is divisible only by primes in } S \cap S' \\ 0 & \text{otherwise.} \end{cases}$$

[11] Note that this condition is necessary but not sufficient, as d and d' must themselves be compatible in the sense that the primes dividing $\frac{d'}{\operatorname{lcm}(|d|,|d'|)}$ must lie in S and vice-versa. However, even this weaker condition is enough.

Note that χ_d and $\chi_{d'}$ are primitive (or primitive up to a local factor, when $d \equiv \pm 3 \pmod 8$) and nonprincipal. We have as in the proof of Lemma 4.2 that

$$F(s) := \sum_{n \geq 1} a_n n^{-s} = C_{d,d'}(s)\big(\zeta(s)L(s,\chi_d)L(s,\chi_{d'})L(s,\chi_d\chi_{d'})\big)^{1/4},$$

where $C_{d,d'}(s)$ is holomorphic on $\mathrm{Re}(s) > \frac{1}{2}$ and $C_{d,d'}(1) \ll \mathrm{lcm}(|d|,|d'|)^{0.001}$. Because the convolution of primitive quadratic characters is principal if and only if they are equal, we see that we can apply Theorem 4.8 with

$$F(s) = \zeta^{1/4}(s)G(s)$$

for

$$G(s) = \big(L(s,\chi_d)L(s,\chi_{d'})L(s,\chi_d\chi_{d'})\big)^{1/4}C_{d,d'}(s).$$

This gives us the desired bound on the sum of a_n up to $\frac{x}{\mathrm{lcm}(|d|,|d'|)}$ after some manipulation, Corollary 4.12, and Proposition 4.10 as before. □

Lemma 6.3.

$$\sum_{d,d' \text{ good}} R_{d,d'}(x) \ll \frac{x}{\log^{3/4} x}$$

Proof. This follows from the same logic as was used in deriving Theorem 4.1 from Lemma 4.2. We have for any $z \leq x$ that

$$\sum_{d,d' \text{ good}} R_{d,d'}(x) \ll x \left(\sum_{d,d' \text{ good}} \frac{(1 + o'_{dd'}(1))c_{dd'}}{\log^{3/4} x} + \sum_{d,d' \text{ good}} \frac{1}{\mathrm{lcm}(|d|,|d'|)} \right).$$

Taking $z := \log^4 x$, we see that the second term in the parenthesis is negligible compared to the first as x goes to infinity by Theorem B, Theorem C and Lemma 2.1(ii). Every $o'_{dd'}(1)$ for $|d| \leq z$ is then upper bounded by some $o(1)$ independent of d and d'. Therefore, as x goes to infinity we have an asymptotic bound

$$\ll \frac{x}{\log^{3/4} x} \sum_{d,d' \text{ good}} \frac{c_{dd'}}{\mathrm{lcm}(|d|,|d'|)} \ll \frac{x}{\log^{3/4} x}$$

as desired. □

Theorem A then follows from Lemma 5.1, (17) and (18), and Theorem C.

7. Computing the Constants: Proving Corollary D and Corollary E

We now turn to the problem of obtaining numerical estimates for c_R and c_I in Theorem A, or equivalently, for series of the form

$$\sum_{d \text{ good}} \frac{c'_d c''_d}{|d| 2^{\omega(d)}}.$$

One natural approach is to first compute this series explicitly for good d for which $|d| \leq D$ and to then bound the size of the tail. This would give us an estimate along with an error bound. Unfortunately, while Theorem B does tell us that the tail has size $\ll_\epsilon D^{-1/3+o(1)}$ as D goes to infinity, our dependence on the *abc*-conjecture means that we cannot control the leading constant. Because each term is positive, we can obtain a lower bound on the sum by ignoring the tail, yielding Corollary D. However, we need an additional hypothesis in order to control the tail and show an upper bound.

Remark (Explicit *abc*-conjectures)*.* One might wonder if we can obtain the desired bounds via an explicit formulation of the *abc*-conjecture. For example, Robert, Stewart, and Tenenbaum [29] conjectured that

$$\max(|a|,|b|,|c|) < k^{1+\epsilon(k)}, \tag{21}$$

where k is the radical of a, b, c in Conjecture 2.2,

$$\varepsilon(k) := \sqrt{\frac{48}{\log k \log\log k}}\left(1 + \frac{3\log\log\log k + 2C_1}{2\log\log k}\right),$$

and $C_1 := 1 + \log 3 - \frac{13}{6}\log 2 + \varepsilon$ for any $\varepsilon > 0$.

Consider (r, d, t) such that $r^3 = dt^2 - 1728$, and let $k := \operatorname{rad}(1728r^3dt^2) = \operatorname{rad}(6rdt)$. Then, the explicit *abc*-conjecture applied to $(r^3, -dt^2, 1728)$ tells us that

$$|r|^{1/2 - 5/2\varepsilon(k)} \le 6^{1+\varepsilon(k)}|d|^{1/2 + 1/2\varepsilon(k)}.$$

This is trivial unless $\varepsilon(k) < \frac{1}{5}$, which does not happen until $k > 10^{141}$. As such, we cannot hope for any sort of good bound on the tail until $k > 10^{141}$. The best lower bound we can presently prove on k is that $k = \operatorname{rad}(6drt) \gg d$. Without a better lower bound, this seems to require that we explicitly compute the contributions to the constant for $d < 10^{141}$. We encountered similar obstacles when attempting to use Baker's explicit *abc*-conjecture [1]; see for example the table in Theorem 1 of [22].

7.1. A conjecture on the frequency of good d.

Recall Granville's conjecture on the twists of hyperelliptic curves (Conjecture 1.3). Intuitively, it suggests that $\operatorname{sqf}(f(x))$ is usually not much smaller than $f(x)$. Here is the precise statement of the conjecture in the setting of elliptic curves.

Conjecture 7.1 ([11])**.** *Let E be an elliptic curve given by the integral model $y^2 = f(x)$, and write f_3 for the leading coefficient of f. Then,*

$$T_E(D) \sim \kappa_f D^{1/3}, \tag{22}$$

where

$$\kappa_f := 2|f_3|^{-1/3}\prod_p\left(1 + \left(1 - \frac{1}{p^{2/3}}\right)\left(\frac{\omega_f(p^2)}{p^{4/3}} + \frac{\omega_f(p^4)}{p^{8/3}} + \frac{\omega_f(p^6)}{p^4} + \dots\right)\right) \tag{23}$$

and $\omega_f(r)$ is the number of roots of f in $\mathbb{Z}/r\mathbb{Z}$.

Granville [10] also showed that the lower bound implicit in (22) holds under the *abc*-conjecture (with the specified constant κ_f).

Lemma 7.2. *If $f(x) = x^3 - 1728$,*

$$11.495 \le \kappa_f \le 13.956$$

Proof. The discriminant of $x^3 - 1728$ is $-80621568 = -2^{12}3^9$. By Hensel's lemma, $\omega_f(p) = \omega_f(p^k)$ for each $k \ge 1$ if p does not divide the discriminant of f. Therefore, the local factor in (23) for $p \ne 2, 3$ is

$$1 + \omega(p)\frac{p^{2/3} - 1}{p^2 - p^{2/3}}.$$

Since $f(x) = (x - 12)(x^2 + 12x + 144)$, 12 is always a simple root of $\bar{f}$ modulo such primes p. The reduction of $x^2 - 12x + 144$ splits if and only if -108 is a quadratic residue, or equivalently -3 is a quadratic residue. Thus, the local factor for $p \ne 2, 3$ is

$$1 + \left(2 + \left(\frac{-3}{p}\right)\right)\frac{p^{2/3} - 1}{p^2 - p^{2/3}}.$$

Over $\mathbb{Z}/2^k\mathbb{Z}$ for $k \leq 6$, $\bar{f}(x) = x^3$ has $2^{k-\lceil \frac{k}{3} \rceil}$ roots, corresponding to multiples of $2^{\lceil \frac{k}{3} \rceil}$. For $k > 6$, 12 is always a root of $\bar{f}$. This root is simple because $f'(12) = 432 \not\equiv 0 \pmod{2^7}$. The polynomial $x^2 + 12x + 144$ has no roots modulo 32, let alone higher powers, as

$$n^2 = 32k - 108 = 4(8k - 27) \equiv 4(8k + 5)$$

and 5 is not a square modulo 8. Thus, the local factor at 2 is

$$1 + \left(1 - 2^{-2/3}\right)\left(2^{-1/3} + 2^{-2/3} + 1 + 2^{-16/3}(1 - 2^{-4/3})^{-1}\right).$$

Over $\mathbb{Z}/3^k\mathbb{Z}$ for $k \leq 3$, $\bar{f}(x) = x^3$ has $3^{k-\lceil \frac{k}{3} \rceil}$ roots. For $k > 3$, the root at 12 is simple, and $x^2 + 12x + 144$ has no roots modulo 81. As such, the local factor at 3 is

$$1 + \left(1 - 3^{-2/3}\right)\left(3^{-1/3} + 3^{-8/3}(1 - 3^{-4/3})^{-1}\right).$$

Multiplying these together for the first $P := 100000$ primes yields 11.49556. The product of the remaining primes is at most

$$\prod_{p>P}\left(1 + \frac{3}{p^{4/3} - 1}\right) \leq \exp\left(3\sum_{n \geq P-1} n^{-4/3}\right) \leq \exp\left(9(P-2)^{-1/3}\right) \leq 1.21398$$

where we've used that $(N-1)^{4/3} \leq N^{4/3} - 1$ for $N \geq 1$. □

In order to get good upper bounds on c_R and c_I in Theorem A, we do not need an asymptotic result, but instead an upper bound on the frequency of good d for which $|d| \leq D$. In (7), the proportion of r which satisfy the given conditions is $\frac{59}{216}$. Motivated by the result of Hooley [13] showing that for cubic polynomials

$$\#\{\mathrm{sqf}(f(1)), \mathrm{sqf}(f(2)), \ldots, \mathrm{sqf}(f(R))\} \sim R,$$

we might expect that the number of good d with absolute value at most D is asymptotically $\frac{59}{216}\kappa_f$. Experimentally, this indeed appears to be the case. Our heuristic upper bound on the limiting value, based on multiplying 13.956 from Lemma 7.2 by $\frac{59}{216}$, is 3.812. We base our bounds in Corollary E on the hypothesis

$$|T_E(D)| \leq 5D^{0.35},$$

accounting for some noise as $|T_E(D)|$ approaches its limiting value. We can check programmatically that this holds for all good d of absolute value at most 10000, and see that it appears to hold quite comfortably. We discuss how we generate the list of good d used for this graph in Section 7.2.

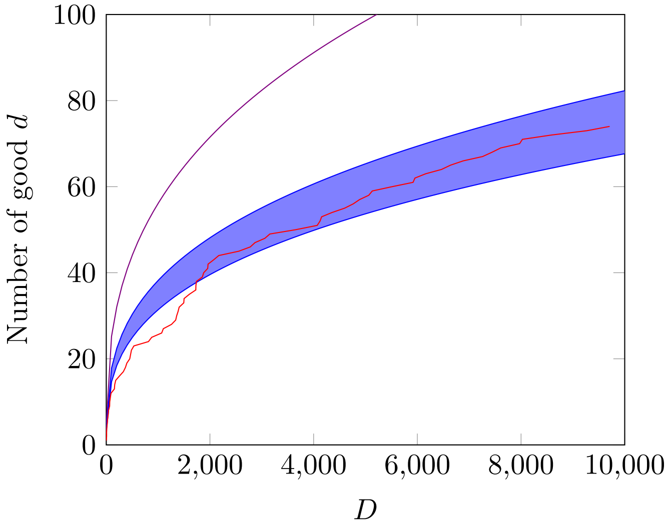

FIGURE 1. The number of good d with absolute value at most D (red), along with a scaled version of the predictions of Granville's conjecture (blue) and our upper bound (violet).

7.2. **An outline of the algorithm.** We briefly outline the steps we use to compute our upper and lower bounds on c_R and c_I. We direct the interested reader to the source code.

7.2.1. *Computing a list of good d.* We compute a list of all good d with $|d| \leq D$ by checking for each squarefree d, $|d| \leq D$, whether $E_d : dy^2 = x^3 - 1728$ has an integral point with $y \neq 0$ and x an element of (7). To compute $E_d(\mathbb{Z})$ we use the algorithm from [16], implemented in Sage [40], which is based on modularity and an elliptic logarithm sieve. It requires the knowledge of a Mordell–Weil basis for E_d. In most of our cases, the latter becomes the bottleneck of the computation of $E_d(\mathbb{Z})$. Note that E_d is isomorphic over $\mathbb{Q}$ to the Mordell curve $y^2 = x^3 - 27d^3$, which in turn is 3-isogenous to $E'_d : y^2 = x^3 + d^3$. Thus it would be enough to compute the Mordell–Weil basis for E'_d, to push it forward to E_d via the 3-isogeny, and to saturate it.

In most cases we use Magma [2] to compute the Mordell–Weil basis for E_d directly. In case the rank of E_d is one, it can be advantageous to find a Mordell–Weil basis with the Heegner point method, e.g. for $d = 131$: In that case, first we estimate the regulators of E_d and E'_d (where the estimate is based on BSD), to see which of the two curves is expected to have a Mordell–Weil generator of smaller Néron–Tate height. For that curve we compute a Heegner point using Pari/GP [39].

When computing lower bounds on c_R and c_I, we bolster this list with additional good d by computing $\mathrm{sqf}(r^3 - 1728)$ for $r \leq 10000000$ satisfying the conditions in (7) and removing repeats.

7.3. **Computing the constant for each d.** For each such d, we compute

$$\frac{c'_d c''_d}{|d| 2^{\omega(d)}}.$$

The values of $c''_{d,R}, c''_{d,I}, |d|$, and $2^{\omega(d)}$ are easy to compute. Recall from Corollary 4.7 that

$$c'_d := \frac{1}{\Gamma(1/2)\zeta(2)^{1/2}} L(1,\chi_d)^{1/2} \prod_{q|m_d} \left(1 + \frac{1}{q}\right)^{-1/2} \prod_{q:\chi_d(q)=1} \left(1 - \frac{1}{q^2}\right)^{1/2}.$$

We compute $L(1, \chi_d)$ using the following theorem.

Theorem 7.3 ([8]). *Let Δ be a fundamental discriminant. Then,*

$$L(1, (\tfrac{\Delta}{\cdot})) = \begin{cases} \frac{\pi}{|\Delta|^{3/2}} \sum_{j=1}^{|\Delta|} j \left(\frac{\Delta}{j}\right) & \Delta < 0 \\ \frac{1}{|\Delta|^{1/2}} \sum_{j=1}^{\Delta} j \log \sin \frac{j\pi}{\Delta} & \Delta > 0 \end{cases}$$

Because $L(s, \chi_d)$ agrees with a Kronecker character up to a constant factor (Lemma 4.4), this allows us to evaluate the L-series at 1.

To bound the product, we observe that for any $Q > 0$,

$$\zeta(2)^{-1/2} \prod_{\substack{q:\chi_d(q)\neq 1 \\ q \leq Q}} \left(1 - \frac{1}{q^2}\right)^{-1/2} \leq \prod_{q:\chi_d(q)=1} \left(1 - \frac{1}{q^2}\right)^{1/2} \leq \prod_{\substack{q:\chi_d(q)\neq 1 \\ q \leq Q}} \left(1 - \frac{1}{q^2}\right)^{1/2},$$

and by taking Q large enough we can obtain a decent approximation to this product.

7.3.1. *Bounding the size of the tail.* We bound the size of the tail by taking

$$\frac{c'_d c''_d}{|d| 2^{\omega(d)}} \leq \frac{L(1, \chi_d)}{2\Gamma(1/2)\zeta(2)^{1/2}|d|}.$$

Lemma 7.4 (Pólya-Vinogradov Inequality [28], Vinogradov 1918). *Let M and N be positive integers. If χ is a primitive character with modulus m,*

$$\left| \sum_{n=M}^{M+N} \chi(n) \right| < m^{1/2} \log m.$$

Corollary 7.5.

$$L(1, \chi_d) \leq \frac{1}{2} \log(4d) + \log\log(4d) + \frac{1}{2\sqrt{d} \log d} + 2 + \gamma$$

This is a standard application of Riemann-Stieljes integrals. We could likely improve upon this by using better bounds on $L(1, \chi)$ [27], but this is already sufficient to show Corollary E, and in particular that $c_R > c_I$ under our hypothesis.

References

[1] Alan Baker. Experiments on the *abc*-conjecture. *Publ. Math. Debrecen*, 65(3-4):253–260, 2004.

[2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] Amanda Clemm and Sarah Trebat-Leder. Elliptic curves with everywhere good reduction. *J. Number Theory*, 161:135–145, 2016.

[4] Salvador Comalada. Courbes elliptiques à bonne réduction d'invariant j fixé. *C. R. Acad. Sci. Paris Sér. I Math.*, 311(11):667–670, 1990.

[5] Salvador Comalada. Elliptic curves with trivial conductor over quadratic fields. *Pacific J. Math.*, 144(2):237–258, 1990.

[6] Salvador Comalada and Enric Nart. Modular invariant and good reduction of elliptic curves. *Math. Ann.*, 293(2):331–342, 1992.

[7] John E. Cremona and Mark P. Lingham. Finding all elliptic curves with good reduction outside a given set of primes. *Experiment. Math.*, 16(3):303–312, 2007.

[8] Harold Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2000. Revised and with a preface by Hugh L. Montgomery.

[9] John Friedlander and Henryk Iwaniec. *Opera de Cribro*, volume 57 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, 2010.

[10] Andrew Granville. *ABC* allows us to count squarefrees. *Internat. Math. Res. Notices*, (19):991–1009, 1998.

[11] Andrew Granville. Rational and integral points on quadratic twists of a given hyperelliptic curve. *Int. Math. Res. Not. IMRN*, (8):Art. ID 027, 24, 2007.

[12] Andrew Granville, Dimitris Koukoulopoulos, and Kaisa Matomäki. When the sieve works. *Duke Math. J.*, 164(10):1935–1969, 2015.

[13] C. Hooley. On the power free values of polynomials. *Mathematika*, 14(1):21–26, 1967.

[14] Hidenori Ishii. The nonexistence of elliptic curves with everywhere good reduction over certain imaginary quadratic fields. *J. Math. Soc. Japan*, 31(2):273–279, 1979.

[15] Takaaki Kagawa. Nonexistence of elliptic curves having everywhere good reduction and cubic discriminant. *Proc. Japan Acad. Ser. A Math. Sci.*, 76(9):141–142, 2000.

[16] Rafael von Känel and Benjamin Matschke. Solving S-unit, Mordell, Thue, Thue–Mahler and generalized Ramanujan–Nagell equations via Shimura–Taniyama conjecture. `https://arxiv.org/abs/1605.06079`, `https://github.com/bmatschke/solving-classical-diophantine-equations/`, 2016.

[17] Masanari Kida. Reduction of elliptic curves over certain real quadratic number fields. *Math. Comp.*, 68(228):1679–1685, 1999.

[18] Masanari Kida. Computing elliptic curves having good reduction everywhere over quadratic fields. II. In *Algebraic number theory and Diophantine analysis (Graz, 1998)*, pages 239–247. de Gruyter, Berlin, 2000.

[19] Masanari Kida. Good reduction of elliptic curves over imaginary quadratic fields. *J. Théor. Nombres Bordeaux*, 13(1):201–209, 2001. 21st Journées Arithmétiques (Rome, 2001).

[20] Masanari Kida. Potential good reduction of elliptic curves. *J. Symbolic Comput.*, 34(3):173–180, 2002.

[21] Masanari Kida and Takaaki Kagawa. Nonexistence of elliptic curves with good reduction everywhere over real quadratic fields. *J. Number Theory*, 66(2):201–210, 1997.

[22] Shanta Laishram and T. N. Shorey. Baker's explicit *abc*-conjecture and applications. *Acta Arith.*, 155(4):419–429, 2012.

[23] Kaisa Matomäki and Xuancheng Shao. When the sieve works II. *J. Reine Angew. Math.*, 763:1–24, 2020.

[24] Benjamin Matschke. Elliptic curve tables. https://github.com/bmatschke/s-unit-equations/tree/master/elliptic-curve-tables, 2020.

[25] Andrew P. Ogg. Abelian curves of 2-power conductor. *Proc. Cambridge Philos. Soc.*, 62:143–148, 1966.

[26] Alekseĭ N. Paršin. Minimal models of curves of genus 2, and homomorphisms of abelian varieties defined over a field of finite characteristic. *Izv. Akad. Nauk SSSR Ser. Mat.*, 36:67–109, 1972.

[27] J. Pintz. Corrigendum: "Elementary methods in the theory of L-functions. VII. Upper bound for $L(1,\chi)$" (Acta Arith. **32** (1977), no. 4, 397–406). *Acta Arith.*, 33(3):293–295, 1977.

[28] Pólya. Über die verteilung der quadratischen reste und nichtreste. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, 1918:21–29, 1918.

[29] Olivier Robert, Cameron L. Stewart, and Gérald Tenenbaum. A refinement of the *abc* conjecture. *Bull. Lond. Math. Soc.*, 46(6):1156–1166, 2014.

[30] G. Robin. Grandes valeurs de la fonction somme des diviseurs et hypothèse de Riemann. *J. Math. Pures Appl. (9)*, 63(2):187–213, 1984.

[31] Jean-Pierre Serre. Divisibilité de certaines fonctions arithmétiques. *Enseign. Math. (2)*, 22(3-4):227–260, 1976.

[32] Bennett Setzer. Elliptic curves over complex quadratic fields. *Pacific J. Math.*, 74(1):235–250, 1978.

[33] Bennett Setzer. Elliptic curves with good reduction everywhere over quadratic fields and having rational j-invariant. *Illinois J. Math.*, 25(2):233–245, 1981.

[34] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[35] Roelof J. Stroeker. Reduction of elliptic curves over imaginary quadratic number fields. *Pacific J. Math.*, 108(2):451–463, 1983.

[36] Nao Takeshi. Elliptic curves with good reduction everywhere over cubic fields. *Int. J. Number Theory*, 11(4):1149–1164, 2015.

[37] Nao Takeshi. Family of elliptic curves with good reduction everywhere over number fields of given degree. *Funct. Approx. Comment. Math.*, 56(1):61–65, 2017.

[38] Gérald Tenenbaum. *Introduction to analytic and probabilistic number theory*, volume 163 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, third edition, 2015. Translated from the 2008 French edition by Patrick D. F. Ion.

[39] The PARI Group, Univ. Bordeaux. *PARI/GP version 2.11.4*, 2020. `https://pari.math.u-bordeaux.fr/`.

[40] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.2)*, 2020. `https://www.sagemath.org`.

[41] Igor R. Šafarevič. Algebraic number fields. In *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*, pages 163–176. Inst. Mittag-Leffler, Djursholm, 1963.

[42] Yu Zhao. Elliptic curves over real quadratic fields with everywhere good reduction and a non-trivial 3-division point. *J. Number Theory*, 133(9):2901–2913, 2013.

Email address: matschke@bu.edu
URL: https://math.bu.edu/people/matschke/

Email address: abhijitm@mit.edu
URL: https://abhijit-mudigonda.github.io/math/