Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Elliptic curves with everywhere good reduction

Amanda Clemm, Sarah Trebat-Leder *,[1]

Department of Mathematics, Emory University, Emory, Atlanta, GA 30322, United States

ARTICLE INFO

Article history:
Received 1 October 2014
Received in revised form 10 July 2015
Accepted 13 July 2015
Available online xxxx
Communicated by Jerome Hoffman, Robert Perlis, Ling Long, Karl Mahlburg, Jorge Morales, Holly Swisher

MSC:
11G05

Keywords:
Elliptic curves
Quadratic fields
Diophantine equations
Everywhere good reduction

ABSTRACT

We consider the question of which quadratic fields have elliptic curves with everywhere good reduction. By revisiting work of Setzer, we expand on congruence conditions that determine the real and imaginary quadratic fields with elliptic curves of everywhere good reduction and rational j-invariant. Using this, we determine the density of such real and imaginary quadratic fields. If $R(X)$ denotes the number of real quadratic fields $K = \mathbb{Q}[\sqrt{m}]$ such that $|\Delta_K| < X$ and for which there exists an elliptic curve E/K with rational j-invariant that has everywhere good reduction, then $R(X) \gg \frac{X}{\sqrt{\log(X)}}$. We also obtain a similar result for imaginary quadratic fields. To obtain these estimates we explicitly construct quadratic fields over which we can construct elliptic curves with everywhere good reduction. The estimates then follow from elementary multiplicative number theory. In addition, we obtain infinite families of real and imaginary quadratic fields such that there are no elliptic curves with everywhere good reduction over these fields.

* Corresponding author.
E-mail addresses: aclemm@emory.edu (A. Clemm), strebat@emory.edu (S. Trebat-Leder).

[1] The second author thanks the National Science Foundation Graduate Research Fellowship Program for its support.

http://dx.doi.org/10.1016/j.jnt.2015.07.001
0022-314X/© 2015 Elsevier Inc. All rights reserved.

1. Introduction

It is a well-known result that over $\mathbb{Q}$ there are no elliptic curves E with everywhere good reduction. However, the same is not true over general number fields. For example, let $K = \mathbb{Q}(\sqrt{29})$ and $a = \frac{5+\sqrt{29}}{2}$. Then the elliptic curve

$$E : y^2 + xy + a^2 y = x^3$$

has unit discriminant, and hence has everywhere good reduction over K.

This leads to the natural question: Over which number fields do there exist elliptic curves with everywhere good reduction? This question has often been approached by studying E/K with everywhere good reduction which satisfy additional properties, such as those which have a K-rational torsion point, admit a global minimal model, or have rational j-invariant. We say that an elliptic curve E/K has $\mathrm{EGR}(K)$ if it has everywhere good reduction over K, and that an elliptic curve E/K has $\mathrm{EGR}_{\mathbb{Q}}(K)$ if it additionally has $\mathbb{Q}$-rational j-invariant. Similarly, we say a quadratic field has EGR if there exists an $\mathrm{EGR}(K)$ elliptic curve and a quadratic field has $\mathrm{EGR}_{\mathbb{Q}}$ if there exists an $\mathrm{EGR}_{\mathbb{Q}}(K)$ elliptic curve.

For many real and imaginary quadratic fields K of small discriminant, explicit examples of elliptic curves E/K with everywhere good reduction can be found in the literature, such as [8] and [6]. There are also many known examples of such fields for which there do not exist any elliptic curves E/K with everywhere good reduction; see [8,11,7] for example.

For example, Kida [8] showed that if K satisfies certain hypotheses, every E/K with EGR has a K-rational point of order two. This condition led to a series of non-existence results for particular real quadratic fields with small discriminant. In [14], Setzer classified elliptic curves with $\mathrm{EGR}_{\mathbb{Q}}$ over real quadratic number fields. Kida extended Setzer's approach by giving a more general method suitable for computing elliptic curves with EGR over certain real quadratic fields with rational or singular j-invariants in [9]. Comalada [1] showed that there exists E/K with EGR, a global minimal model, and a K-rational point of order two if and only if one of his sets of Diophantine equations has a solution. Ishii supplemented this theorem by studying k-rational 2 division points in [6] to demonstrate specific real quadratic fields without EGR elliptic curves. Later Kida and Kagawa in [11] generalized Ishii's result to obtain non-existence results for $\mathbb{Q}(\sqrt{17})$, $\mathbb{Q}(\sqrt{73})$ and $\mathbb{Q}(\sqrt{97})$. Yu Zhao determined criteria for real quadratic fields to have elliptic curves with EGR and a non-trivial 3-division point. In [16], he provides a table for all such fields with discriminant less than 10,000.

For imaginary quadratic fields, Stroeker [15] showed that no E/K with EGR admits a global minimal model. In [13], Setzer showed that there exist elliptic curves with EGR and a K-rational point of order two if and only if $K = \mathbb{Q}(\sqrt{-m})$ with m satisfying certain congruence conditions. Comalada and Nart provided criteria to determine when elliptic curves have EGR in [2]. Kida combined this result with a method of computing

Table 1
Real quadratic fields $\mathbb{Q}(\sqrt{m})$ with and without EGR.

EGR	no EGR
6	2
7	3
14	5
22	10
26	11
29	13
33	15
37	17
38	19
41	21
	23
	30
	31
	34
	35
	39
	42
	43
	46
	47

the Mordell–Weil group in [10] to prove there are no elliptic curves with EGR over the fields $\mathbb{Q}(\sqrt{-35}), \mathbb{Q}(\sqrt{-37}), \mathbb{Q}(\sqrt{-51})$ and $\mathbb{Q}(\sqrt{-91})$. There are no elliptic curves with $\mathrm{EGR}_{\mathbb{Q}}(K)$ for $-37 < m < -1$. However, there are elliptic curves with small discriminant and $\mathrm{EGR}_{\mathbb{Q}}(K)$ for real quadratic fields K.

Table 1 shows what is known for $K = \mathbb{Q}(\sqrt{m})$ with square-free positive integers $m \leq 47$. We stop at 47 because to the best of our knowledge, the $m = 51$ case is still unknown.

A combination of the above results gives many methods to prove that a particular quadratic number field has an EGR elliptic curve. Cremona and Lingham [3] described an algorithm for finding all elliptic curves over any number field K with good reduction outside a given set of primes. However, this procedure relies on finding integral points on certain elliptic curves over K, which can limit its practical implementation. As a consequence of Setzer's result regarding the classification of elliptic curves over both real and imaginary quadratic number fields with rational j-invariant, it is known that there infinitely many quadratic fields which have an EGR elliptic curve. However, there is no conjectured density result for the proportion of quadratic fields over which there exist elliptic curves E with everywhere good reduction.

Let $R(X)$ be the number of real quadratic number fields K with discriminant at most X and an $\mathrm{EGR}_{\mathbb{Q}}(K)$ elliptic curve. By revisiting the results of Setzer, we prove the following.

Theorem 1.1. *With $R(X)$ as above, we have that*

$$R(X) \gg \frac{X}{\sqrt{\log(X)}}.$$

If $I(X)$ is the number of imaginary quadratic number fields K with $|\Delta_K| < X$ and an $\mathrm{EGR}_{\mathbb{Q}}(K)$ elliptic curve, we also obtain the result below.

Theorem 1.2. *With $I(X)$ as above, we have that*

$$I(X) \gg \frac{X}{\sqrt{\log(X)}}.$$

To prove Theorem 1.1, we first show that all real quadratic fields of the form described below in Theorem 1.3 have $\mathrm{EGR}_{\mathbb{Q}}$, and then count these fields.

Theorem 1.3. *Let $m = 2q$, where $q = q_1 \cdots q_n \equiv 3 \pmod 8$ with $q_j \equiv 1, 3 \pmod 8$ distinct primes. Then the real quadratic field $K = \mathbb{Q}(\sqrt{m})$ has $EGR_{\mathbb{Q}}$.*

Remark 1. If m is as described in Theorem 1.3, there exists E/K with $\mathrm{EGR}_{\mathbb{Q}}$ and $j(E) = 20^3$ as shown by Setzer in 2.1.

Similarly, to prove Theorem 1.2, we show all imaginary quadratic fields found below in Theorem 1.4 have $\mathrm{EGR}_{\mathbb{Q}}$.

Theorem 1.4. *Let $m = 37q$, where $q = -q_1 \cdots q_n \equiv 1 \pmod 8$ with q_j distinct primes such that $\left(\frac{q_j}{37}\right) = 1$. Then the imaginary quadratic field $K = \mathbb{Q}(\sqrt{m})$ has $EGR_{\mathbb{Q}}$.*

Remark 2. If m is as described in Theorem 1.4, there exists E/K with $\mathrm{EGR}_{\mathbb{Q}}$ and $j(E) = 16^3$ as shown by Setzer in 2.1.

We can achieve results like Theorems 1.3 and 1.4 for integers other than 2 and 37; these two cases are all is required to prove Theorems 1.1 and 1.2.

To obtain a density result for $m = qD$, where D is fixed and q varies, we define certain 'good' D. We say D is good if it is the square free part of $A^3 - 1728$, where A satisfies certain congruence conditions modulo powers of 2 and 3. Both $D = 2$ and $D = 37$ are examples of 'good' values of D. These congruence conditions will be described explicitly in Section 2. If D is good, then $K = \mathbb{Q}(\sqrt{Dq})$ has $\mathrm{EGR}_{\mathbb{Q}}$ whenever D and q satisfy certain explicit conditions, see Section 2. For any square-free D, define

$$\epsilon_D = \begin{cases} 1 & D \equiv 1 \pmod 4 \\ -1 & \text{otherwise} \end{cases}$$

When $\mathrm{sign}(D) = -\epsilon_D$, we get real quadratic fields $\mathbb{Q}(\sqrt{qD})$, and when $\mathrm{sign}(D) = \epsilon_D$, we get imaginary quadratic fields.

Using this, we show that $R_D(X)$, the number of $q \leq X$ such that $\mathbb{Q}(\sqrt{Dq})$ is a real $\mathrm{EGR}_{\mathbb{Q}}$ quadratic number field, satisfies the following lower bound:

Theorem 1.5. *Let D be good with r distinct prime factors and $R_D(X)$, the number of EGR$_{\mathbb{Q}}$ real quadratic number fields $\mathbb{Q}(\sqrt{Dq})$ with $q \leq X$. Assume that sign$(D) = -\epsilon_D$. Then*

$$R_D(X) \gg \frac{X}{\log^{1-1/2^r} X}.$$

We obtain a similar result to show that $I_D(X)$, the number of EGR$_{\mathbb{Q}}$ imaginary quadratic number fields $\mathbb{Q}(\sqrt{Dq})$ satisfies the following lower bound.

Theorem 1.6. *Let D be good with r distinct prime factors and $I_D(X)$, the number of EGR$_{\mathbb{Q}}$ imaginary quadratic number fields $\mathbb{Q}(\sqrt{Dq})$ with $q \leq X$. Assume that sign$(D) = \epsilon_D$. Then*

$$I_D(X) \gg \frac{X}{\log^{1-1/2^r} X}.$$

Remark 3. While we have only looked at curves with rational j-invariant, Noam Elkies' computations [4] suggest that very few E/K with EGR have $j(E) \notin \mathbb{Q}$ and unit discriminant. Therefore, the theorem below, which to the best of our knowledge has not previously appeared in the literature, suggests that most fields of the form $K = \mathbb{Q}(\sqrt{\pm p})$ for primes $p \equiv 3 \pmod 8$ are not EGR. This is consistent with Elkies' data.

Using this approach we were also able to determine nonexistence of EGR$_{\mathbb{Q}}$ quadratic fields.

Theorem 1.7. *Let $p \equiv 3 \pmod 8$ be prime.*

(1) Let $K = \mathbb{Q}(\sqrt{p})$. Then there are no E/K with EGR$_{\mathbb{Q}}$.
(2) Let $K = \mathbb{Q}(\sqrt{-p})$. Then there are no E/K with EGR$_{\mathbb{Q}}$.

Remark 4. In [7], Kagawa showed that if p is a prime number such that $p \equiv 3(4)$ and $p \neq 3, 11$, then there are no elliptic curves with EGR over $K = \mathbb{Q}(\sqrt{3p})$ whose discriminant is a cube in K. Since all EGR(K) curves have cubic discriminant as shown in Setzer [14], this gives a result similar to Theorem 1.7.

In Section 2, we describe conditions arising from Setzer to define when we have EGR$_{\mathbb{Q}}$ quadratic fields. In Section 3, we use these conditions to find a lower bound based on an example of Serre. In Section 4, we will give examples of EGR$_{\mathbb{Q}}$ real quadratic fields and EGR$_{\mathbb{Q}}$ imaginary quadratic fields.

2. Constructing EGR$_{\mathbb{Q}}$ quadratic fields

In [14], given a rational j-invariant, Setzer determines whether there exist an elliptic curve and number field over which this curve has everywhere good reduction. Following his notation, we make the following definitions. Let $\mathcal{R}$ be the following set:

$$\mathcal{R} = \{A \in \mathbb{Z} : 2|A \Rightarrow 16|A \text{ or } 16|A-4, \text{ and } 3|A \Rightarrow 27|A-12\}.$$

Note that by the Chinese Remainder Theorem, $\mathcal{R}$ is then the union of the following congruence classes:

- $1, 5 \pmod 6$;
- $4, 16, 20, 32 \pmod{48}$;
- $39 \pmod{54}$;
- $228, 336 \pmod{432}$.

We say that D is good if it is in the following set:

$$\{D : Dt^2 = A^3 - 1728, D \text{ square-free}, A \in \mathcal{R}, t \in \mathbb{Z}\}.$$

For example, the good D with $|D| < 100$ are exactly

$$-91, -67, -43, -26, -19, -11, -7, 2, 7, 37, 65, 79.$$

Remark 5. We note that ± 1 are not good, as the elliptic curves $Y^2 = X^3 - 1728$, $-Y^2 = X^3 - 1728$ have no integral points with $Y \neq 0$.

By Setzer [14], the only candidates for elliptic curves E with EGR$_{\mathbb{Q}}(K)$ over a quadratic field K have $j(E) = A^3$ with $A \in \mathcal{R}$.

Theorem 2.1. *(See [14].) Let $K = \mathbb{Q}(\sqrt{m})$ be a quadratic field with m square-free. Then there exists an elliptic curve E/K with EGR$_{\mathbb{Q}}$ if and only if the following conditions are satisfied for some good $D \mid \Delta_K$.*

(1) $\epsilon_D D$ is a rational norm from K.
(2) If $D \equiv \pm 3 \pmod 8$, then $m \equiv 1 \pmod 4$.
(3) If D is even then $m \equiv 4 + D \pmod{16}$.

To prove the theorem, Setzer shows that given a pair (m, D) satisfying the conditions of the theorem, there exists $u \in K^\times$ such that

$$E_{u,A} : y^2 = x^3 - 3A(A^3 - 1728)u^2 x - 2(A^3 - 1728)^2 u^3$$

has j-invariant A^3 and EGR$_{\mathbb{Q}}$ over K.

Remark 6. We correct a mistake in condition (2) of this theorem as written in [14].

We note that if $u \equiv v \pmod{4\mathcal{O}_K}$ and $m \equiv 2, 3 \pmod 4$, then we must have that $N(u) \equiv N(v) \pmod 8$. However, if $m \equiv 1 \pmod 4$, we only know that $N(u) \equiv N(v) \pmod 4$. Moreover, we can pick $w \in 4\mathcal{O}_K$ such that $N(u+w) \equiv N(u)+4 \pmod 8$.

Condition (2) as written in Setzer's paper states that if $D \equiv \pm 3 \pmod 8$, then $m \equiv 5 \pmod 8$. $D \equiv \pm 3 \pmod 8$ implies that a certain element $u \in \mathcal{O}_K$ has $N(u) \equiv 5 \pmod 8$. But for the curve to have good reduction at primes dividing 2, it is necessary that u is congruent to a square modulo $4\mathcal{O}_K$. For $m \equiv 2, 3 \pmod 4$ this is not possible, as no squares can have norm equivalent to 5 modulo 8. However, if $m \equiv 1 \pmod 4$, the condition that $N(u) \equiv 5 \pmod 8$ is not an obstacle, as u is congruent modulo $4\mathcal{O}_K$ to elements of norm 1 modulo 8. Setzer mistakenly assumes that this can only happen when $m \equiv 5 \pmod 8$.

In proving that fields do and do not have elliptic curves with $\text{EGR}_{\mathbb{Q}}$, the following equivalent version of Setzer's theorem will be useful.

Theorem 2.2. *Fix D good, and $m = qD$ square-free. $K = \mathbb{Q}(\sqrt{m})$ has $EGR_{\mathbb{Q}}$ if and only if the following conditions are satisfied:*

(a) $(-\epsilon_D q/p_i) = 1$ *for all odd primes p_i dividing D;*
(b) $(\epsilon_D D/q_j) = 1$ *for all odd primes q_j dividing q;*
(c) $m > 0$ *if* $\epsilon_D D < 0$;
(d) If $D \equiv \pm 3 \pmod 8$ *then* $q \equiv D \pmod 4$;
(e) If D is even then $q \equiv D + 1 \pmod 8$.

Proof. We need to show that the conditions in Theorem 2.1 are equivalent to those in Theorem 2.2.

Assume that $K = \mathbb{Q}(\sqrt{m})$ where m is square-free.

Clearly if $m = qD$, D divides Δ_K. We need to show that if $D \mid \Delta_K$ then $D \mid m$. This is trivial for $m \equiv 1 \pmod 4$, as then $\Delta_K = m$. If $m \equiv 3 \pmod 4$, then D cannot be even because of condition (3) of Theorem 2.1, so $D \mid m$. If $m \equiv 2 \pmod 4$, then D must be square-free, so $D \mid m$.

Now, $\epsilon_D D$ is a rational norm from K if and only if there exists a rational solution to $\epsilon_D D = a^2 - b^2 Dq$. Since $D \mid a$, the above is equivalent to the existence of a rational solution to $\epsilon_D = D(a')^2 - b^2 q$, which is equivalent to the existence of a nontrivial integer solution to $\epsilon_D x^2 - Dy^2 + qz^2 = 0$. By Legendre's Theorem [5], this equation has a nontrivial integral solution if and only if the following hold:

(i) $\epsilon_D, -D$, and q do not all have the same sign, which is equivalent to condition (c).
(ii) $\epsilon_D D$ is a square modulo $|q|$, which is equivalent to condition (b).

(iii) $-\epsilon_D q$ is a square modulo $|D|$, which is equivalent to condition (a).
(iv) $-Dq$ is a square modulo $|\epsilon_D|$, which is always the case.

Lastly, conditions (d) and (e) are directly equivalent to (2) and (3). □

To prove Theorem 1.1, the lower bound for $R_D(X)$ and Theorem 1.2, the lower bound for $I_D(X)$, we require Theorem 1.3 (which considers the case $D = 2$) and Theorem 1.4 (which considers the case $D = 37$). Below, we prove both those theorems using the result above.

Proof of Theorem 1.3. Let $A = 20 \in \mathcal{R}$. This shows that $D = 2$ is good. For $m = 2q$ with $q = q_1 \cdots q_n \equiv 3 \pmod 8$ and $q_j \equiv 1, 3 \pmod 8$ distinct primes, all of the conditions in Theorem 2.2 are satisfied, and so $K = \mathbb{Q}(\sqrt{m})$ has $\mathrm{EGR}_{\mathbb{Q}}$. □

Proof of Theorem 1.4. Let $A = 16 \in \mathcal{R}$. This that shows that $D = 37$ is good. For $m = 37q$ with $q = -q_1 \cdots q_n \equiv 1 \pmod 8$ and q_j distinct primes such that $\left(\frac{q_j}{37}\right) = 1$, all of the conditions in Theorem 2.2 are satisfied, and so $K = \mathbb{Q}(\sqrt{m})$ has $\mathrm{EGR}_{\mathbb{Q}}$. □

We also can use Theorem 2.2 to prove nonexistence results about $\mathrm{EGR}_{\mathbb{Q}}$ quadratic fields.

Proof of Theorem 1.7. Let $p \equiv 3 \pmod 8$ be prime.

To show that there are no $E/\mathbb{Q}(\sqrt{p})$ with $\mathrm{EGR}_{\mathbb{Q}}$, we must show that neither of the pairs $(D, q) = (p, 1), (-p, -1)$ satisfy the conditions of Theorem 2.2. We note that since $p = D \equiv \pm 3 \pmod 8$, condition (d) implies that $q \equiv 5D \equiv \pm 1 \pmod 8$, which is a contradiction.

Similarly, to show that there are no $\mathrm{EGR}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{-p})$, we have to show that neither of the pairs $(D, q) = (p, -1), (-p, 1)$ satisfy the conditions of the theorem. We note that in both cases, condition (a) implies that $\left(\frac{-1}{p}\right) = 1$, which is a contradiction. □

3. Finding lower bounds

To prove the lower bounds, we use an example of Serre [12] as a reference. Let $K/\mathbb{Q}$ be a Galois extension and $C \subset \mathrm{Gal}(K/\mathbb{Q})$ be a conjugacy class. Let $\pi(K/\mathbb{Q}, C)$ denote the set of primes p that are unramified in $K/\mathbb{Q}$ with Frobenius conjugacy class C.

Definition 1. We call a set of primes a Chebotarev set if there are finitely many finite Galois extensions $K_i/\mathbb{Q}$ and conjugacy classes $C_i \subset \mathrm{Gal}(K_i/\mathbb{Q})$ such that up to finite sets, $P = \cup_i \pi(K_i/\mathbb{Q}, C_i)$.

Definition 2. We define a set $E \subset \mathbb{N}_{>0}$ to be multiplicative if for all pairs n_1, n_2 relatively prime, we have that $n_1 n_2 \in E$ if and only if $n_1 \in E$ or $n_2 \in E$.

Given a multiplicative set E, let $P(E)$ be the set of primes p in E. Let $\bar{E} := \mathbb{N}_{>0} - E$, and $\bar{E}(X) := \{m \in \bar{E}, m \leq X\}$.

Theorem 3.1. *(See [12].) Suppose that E is multiplicative and $P(E)$ is a Chebotarev set with density $0 < \alpha < 1$. Then*

$$\bar{E}(X) \sim cX/\log^{\alpha} X$$

for some $c > 0$.

We will use the theorem above to prove Theorem 1.5 and Theorem 1.6. As shown in Section 2, the special cases with $D = 2, 37$ will then imply Theorems 1.1 and 1.2.

Proof of Theorem 1.5 and Theorem 1.6. Let D be good. Let D' be the odd part of D, and $\delta = \epsilon_D \epsilon_{D'} D/D'$. Note that if D is odd, then $\delta = 1$.

Also define

$$\bar{E}_D := \{q_1^{a_1} \cdots q_n^{a_n} : q_j \text{ is prime, } a_j \geq 0, \left(\frac{q_j}{p}\right) = 1 \text{ for all odd primes } p \mid D, \left(\frac{\delta}{q_j}\right) = 1\}.$$

The compliment $E_D = \mathbb{N} - \bar{E}_D$ is then multiplicative and $P(E_D)$ has Chebotarev density $\alpha = 1 - 1/2^r$, where r is the number of prime factors of D. Therefore, by Theorem 3.1, we have

$$\bar{E}_D(X) \sim cX/\log^{\alpha} X.$$

Now, we have to relate $\bar{E}_D(X)$ to $R_D(X)$ and $I_D(X)$. We do this by showing that if $\pm q \in \bar{E}(X)$ is squarefree and satisfies congruence conditions coming from (d) and (e) of Theorem 2.2, then $m = qD$ has $\mathrm{EGR}_{\mathbb{Q}}$.

Let C_D be the set of $q \in \mathbb{Z}$ that satisfy the congruence conditions (d) and (e) of Theorem 2.2, so that

$$C_D = \begin{cases} \{q \in \mathbb{Z} : q \equiv D \pmod 4\} & \text{if } D \equiv \pm 3 \pmod 8 \\ \{q \in \mathbb{Z} : q \equiv D + 1 \pmod 8\} & \text{if } D \equiv 0 \pmod 2 \\ \{q \in \mathbb{Z}\} & \text{otherwise} \end{cases}$$

We define

$$R_D^E(X) := \{Dq : \mathrm{sgn}(D)q \in \bar{E}_D(X/D), q \text{ squarefree}, \ q \in C_D\}$$
$$I_D^E(X) := \{Dq : -\mathrm{sgn}(D)q \in \bar{E}_D(X/D), q \text{ squarefree}, \ q \in C_D\}$$

Lemma 3.2. *For good D, $R_D^E(X) \subset R_D(X)$ if $\epsilon_D = -sgn(D)$ and $I_D^E(X) \subset I_D(X)$ if $\epsilon_D = sgn(D)$.*

Proof. We need to check (a) and (b) of Theorem 2.2. They follow from the properties of the Jacobi symbol. Let D be good. If either $\epsilon_D = -\mathrm{sgn}(D)$ with $0 < qD$ or $\epsilon_D = \mathrm{sgn}(D)$ with $0 > qD$, we have that $0 < -\epsilon_D q = \prod q_j$, so

$$\left(\frac{-\epsilon_D q}{p}\right) = \prod \left(\frac{q_j}{p}\right) = 1.$$

Note that then we always have that $\epsilon_{D'} D' \equiv 1 \pmod 4$ and $\epsilon_D D = \delta D' \epsilon_{D'}$. So

$$\left(\frac{\epsilon_D D}{q_j}\right) = \left(\frac{\delta}{q_j}\right)\left(\frac{\epsilon_{D'} D'}{q_j}\right) = \left(\frac{q_j}{|\epsilon_{D'} D'|}\right) = \prod_{p|D \text{ odd}} \left(\frac{q_j}{p}\right) = 1 \qquad \square$$

Since a positive proportion of $\pm q \in \overline{E}_D(X/D)$ satisfies the extra conditions of being squarefree and in C_D, we have that

$$R_D^E(X), I_D^E(X) \gg \frac{X}{\log^\alpha X},$$

and hence the same is true of the bigger sets $R_D(X), I_D(X)$. $\square$

Proof of Theorem 1.1. The theorem follows immediately from Theorem 1.5 and Theorem 1.3. Theorem 1.3 shows $D = 2$ is good with $r = 1$ distinct factors and the real quadratic field $K = \mathbb{Q}(\sqrt{qD})$ has $\mathrm{EGR}_\mathbb{Q}$. If $R(X)$ is the number of these fields, Theorem 1.5 shows

$$R(X) \gg \frac{X}{\sqrt{\log(X)}}. \qquad \square$$

Proof of Theorem 1.2. The theorem follows immediately from Theorem 1.6 and Theorem 1.4. Theorem 1.4 shows $D = 37$ is good with $r = 1$ distinct factors and the imaginary quadratic field $K = \mathbb{Q}(\sqrt{qD})$ has $\mathrm{EGR}_\mathbb{Q}$. If $I(X)$ is the number of these fields, Theorem 1.6 shows

$$I(X) \gg \frac{X}{\sqrt{\log(X)}}. \qquad \square$$

4. Examples

In this section, we explain how to find elliptic curves with $\mathrm{EGR}_\mathbb{Q}$ when the conditions of Theorem 2.2 are satisfied, and give examples of elliptic curves with $\mathrm{EGR}_\mathbb{Q}$. The results in this section are based on Setzer's construction in 2.1.

We start with a quadratic field $K = \mathbb{Q}(\sqrt{m})$ and a factorization $m = Dq$ with D good which satisfies the conditions of Theorem 2.2. We want to find u such that

$$E_{u,A} : y^2 = x^3 - 3A(A^3 - 1728)u^2 x - 2(A^3 - 1728)^2 u^3$$

has $\mathrm{EGR}_{\mathbb{Q}}(K)$. Let $\alpha \in K$ have norm $\epsilon_D D$, and pick n odd such that $\beta := n\alpha = a + b\sqrt{m} \in \mathcal{O}_K$. Let $A \in \mathcal{R}$ be such that D is the square-free part of $A^3 - 1728$. Define d_1, d_2 such that $3^2(A^3 - 1728) = Dd_1^2 d_2^4$ with d_1 square-free. If $m \equiv 1, 2 \pmod 4$, then one of $u = \pm\beta d_1$ works. If $m \equiv 3 \pmod 4$, then either $u = \pm\beta d_1$ both work or $u = \pm\beta d_1\rho$ both work, where $\rho = \frac{1}{2}(m+1) + \sqrt{m}$.

The table below has some examples.

A	D	d_1	q	α	u
20	2	42	3	$2+\sqrt{6}$	$-d_1\alpha = -84 - 42\sqrt{6}$
-15	-7	1	-11	$35 + 4\sqrt{77}$	$-d_1\alpha = -35 - 4\sqrt{77}$
-32	-11	42	-15	$77 + 6\sqrt{165}$	$d_1\alpha = 3234 + 252\sqrt{165}$
-32	-11	42	-3	$11 + 2\sqrt{33}$	$-d_1\alpha = -462 - 84\sqrt{33}$
39	79	1	5	$79 + 4\sqrt{395}$	$\pm d_1\alpha\rho = \pm(17\,222 + 871\sqrt{395})$
16	37	6	-7	$37 + 6\sqrt{-259}$	$\pm d_1\alpha = \pm(222 + 36\sqrt{-259})$

References

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

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

[3] J.E. Cremona, M.P. Lingham, Finding all elliptic curves with good reduction outside a given set of primes, Exp. Math. 16 (3) (2007) 303–312.

[4] Noam Elkies, Elliptic curves of unit discriminant over real quadratic number fields, Online, accessed April-2014.

[5] Kenneth Ireland, Michael Rosen, A Classical Introduction to Modern Number Theory, second edition, Grad. Texts in Math., vol. 84, Springer-Verlag, New York, 1990.

[6] Hidenori Ishii, The nonexistence of elliptic curves with everywhere good reduction over certain quadratic fields, Jpn. J. Math. (N. S.) 12 (1) (1986) 45–52.

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

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

[9] Masanari Kida, Computing elliptic curves having good reduction everywhere over quadratic fields. II, in: Algebraic Number Theory and Diophantine Analysis, Graz, 1998, de Gruyter, Berlin, 2000, pp. 239–247.

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

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

[12] Jean-Pierre Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (4) (1972) 259–331.

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

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

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

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

Please cite this article in press as: A. Clemm, S. Trebat-Leder, Elliptic curves with everywhere good reduction, J. Number Theory (2015), http://dx.doi.org/10.1016/j.jnt.2015.07.001