ON THE NUMBER OF ELLIPTIC CURVES WITH CM OVER LARGE ALGEBRAIC FIELDS

by

Gerhard Frey

Institute for Experimental Mathematics, Essen University
Ellernstrasse 29, D-45326 Germany
e-mail: frey@exp-math.uni-essen.de

and

Moshe Jarden

School of Mathematics, Tel Aviv University
Ramat Aviv, Tel Aviv 69978, Israel
e-mail: jarden@post.tau.ac.il

MR Classification: 12E30
Directory: \Jarden\Diary\CM
19 July, 2005

* Research supported by the Minkowski Center for Geometry at Tel Aviv University, established by the Minerva Foundation.

** This note was partially written while the second author was a guest of the IWR Research Group Algorithmic Algebra of Heidelberg University.
Introduction

The goal of this note is to report on a new phenomena in the theory of large fields.

As usual, we denote the absolute Galois group of \( \mathbb{Q} \) by \( \operatorname{Gal}(\mathbb{Q}) \) and equip each of the cartesian powers \( \operatorname{Gal}(\mathbb{Q})^e \) by the normalized Haar measure \( \mu \). Let \( \bar{\mathbb{Q}} \) be the algebraic closure of \( \mathbb{Q} \). For each \( \sigma = (\sigma_1, \ldots, \sigma_e) \) let \( \bar{\mathbb{Q}}(\sigma) \) be the fixed field in \( \bar{\mathbb{Q}} \) of \( \sigma_1, \ldots, \sigma_e \). The behavior of the fields \( \bar{\mathbb{Q}}(\sigma) \) becomes regular if we remove sets of measure zero. This is exemplified by the following fundamental result:

**Theorem A** ([FrJ, Thms. 18.5.6 and 18.6.1]): The following statements hold for almost all \( \sigma \in \operatorname{Gal}(\mathbb{Q})^e \):

(a) The absolute Galois group of \( \bar{\mathbb{Q}}(\sigma) \) is isomorphic to the free profinite group \( \hat{F}_e \) on \( e \) generators.

(b) The field \( \bar{\mathbb{Q}}(\sigma) \) is PAC, that is, each absolutely irreducible variety \( V \) defined over \( \bar{\mathbb{Q}}(\sigma) \) has a \( \bar{\mathbb{Q}}(\sigma) \)-rational point.

Likewise, the following holds for Abelian varieties:

**Theorem B** ([FyJ]): Let \( A \) be an abelian variety over \( \mathbb{Q} \). Then for almost all \( \sigma \in \operatorname{Gal}(\mathbb{Q})^e \) the rank of \( A(\bar{\mathbb{Q}}(\sigma)) \) is infinite.

Note that the fields \( \bar{\mathbb{Q}}(\sigma) \) become smaller as \( e \) increases. Thus, it is expected that in general less arithmetical objects will be defined over \( \bar{\mathbb{Q}}(\sigma) \) as \( e \) increases. Here are two typical examples:

**Theorem C** ([JaJ, Main Theorem(a)]): Let \( A \) be an Abelian variety and \( l \) a prime number. Then for each \( e \geq 1 \) and for almost all \( \sigma \in \operatorname{Gal}(K)^e \) the set \( \bigcup_{i=1}^{\infty} A_l(\bar{\mathbb{Q}}(\sigma)) \) is finite (while \( \bigcup_{i=1}^{\infty} A_l(\bar{\mathbb{Q}}) \) is infinite, which is the case if \( e = 0 \)).

Here \( A_n(L) = \{ p \in A(L) \mid np = 0 \} \) for each positive integer \( n \) and each field extension \( L \) of \( K \).

**Theorem D**: [Jar, Thms. 8.1 and 8.2] The following holds for almost all \( \sigma \in \operatorname{Gal}(\mathbb{Q})^e \):

(a) If \( e = 1 \), then \( \bar{\mathbb{Q}}(\sigma) \) contains infinitely many roots of unity.

(b) If \( e \geq 2 \), then \( \bar{\mathbb{Q}}(\sigma) \) contains only finitely many roots of unity.

1
Theorem E: Let $E$ be an elliptic curve over $\mathbb{Q}$. Then the following holds for almost all $\sigma \in \text{Gal}(\mathbb{Q})^e$:

(a) If $e = 1$, then $E_{\text{tor}}(\bar{\mathbb{Q}}(\sigma))$ is infinite.

(b) If $e \geq 2$, then $E_{\text{tor}}(\bar{\mathbb{Q}}(\sigma))$ is finite.

The arithmetical reason that lies behind the distinction between the cases $e = 1$ and $e \geq 2$ in Theorems D and E is that the series $\sum \frac{1}{l^e}$, with $l$ ranges over all prime numbers, diverges for $e = 1$ and converges for $e \geq 2$.

In general, we call a nonnegative integer $e_0$ a cut for the large fields over $\mathbb{Q}$ if there exists an infinite set $P$ of arithmetical or geometrical objects defined over $\bar{\mathbb{Q}}$ such that for almost all $\sigma \in \text{Gal}(K)^e$ infinitely many objects of $P$ are defined over $\bar{\mathbb{Q}}(\sigma)$ if $e < e_0$ and only finitely many objects of $P$ are defined over $\bar{\mathbb{Q}}(\sigma)$ if $e \geq e_0$.

Theorem C implies that 1 is a cut for the large fields over $\mathbb{Q}$, while Theorems D and E imply that 2 is a cut for the large fields over $\mathbb{Q}$.

For a long time 1 and 2 were the only known cuts for large fields over $\mathbb{Q}$. The goal of the present note is to prove that also 3 and 4 are cuts for large fields over $\mathbb{Q}$. The relevant properties of fields were hidden in the theory of elliptic curves with complex multiplication:

Theorem F: The following holds for almost all $\sigma \in \text{Gal}(\mathbb{Q})^e$:

(a) If $e \leq 2$, then there are infinitely many elliptic curves $E$ (up to $\mathbb{C}$-isomorphism) with CM over $\bar{\mathbb{Q}}(\sigma)$ such that $\text{End}(E) \subseteq \bar{\mathbb{Q}}(\sigma)$.

(b) If $e \geq 3$, then there are only finitely many elliptic curves $E$ (up to $\mathbb{C}$-isomorphism) with CM over $\bar{\mathbb{Q}}(\sigma)$ such that $\text{End}(E) \subseteq \bar{\mathbb{Q}}(\sigma)$.

Theorem G: The following holds for almost all $\sigma \in \text{Gal}(\mathbb{Q})^e$:

(a) If $e \leq 3$, then there are infinitely many elliptic curves $E$ (up to $\mathbb{C}$-isomorphism) with CM over $\bar{\mathbb{Q}}(\sigma)$.

(b) If $e \geq 4$, then there are only finitely many elliptic curves $E$ (up to $\mathbb{C}$-isomorphism) with CM over $\bar{\mathbb{Q}}(\sigma)$.

The proofs of Theorems F and G use the standard properties of the $j$-function of elliptic curves with CM as in [Shi] and [Lan] and information about the growth of the
class number of imaginary quadratic fields:

**Theorem H:** For each prime number $p$ let $h(p)$ be the class number of $\mathbb{Q}(\sqrt{-p})$. Then

$$\sum_{p \equiv 3 \pmod{4}} \frac{1}{h(p)^2} = \infty,$$

where $p$ ranges on all prime numbers which are congruent to 3 modulo 4.

The authors are indebted to Ram Murty for kindly supplying the proof of Theorem H.

Finally, we rephrase Theorem F for a family of large fields which are considerably smaller than the fields $\tilde{\mathbb{Q}}(\sigma)$. For each $\sigma \in \text{Gal}(\mathbb{Q})^c$ we denote the maximal Galois extension of $\mathbb{Q}$ which is contained in $\tilde{\mathbb{Q}}(\sigma)$ by $\tilde{\mathbb{Q}}[\sigma]$. Then the following holds:

**Theorem I:** The following holds for almost all $\sigma \in \text{Gal}(\mathbb{Q})^c$:

(a) If $e \leq 2$, then there are infinitely many elliptic curves $E$ (up to $\mathbb{C}$-isomorphism) with CM over $\tilde{\mathbb{Q}}[\sigma]$.

(b) If $e \geq 3$, then there are only finitely many elliptic curves $E$ (up to $\mathbb{C}$-isomorphism) with CM over $\tilde{\mathbb{Q}}[\sigma]$. 

3
1. On the growth of the class number of imaginary quadratic fields

For each prime number \( p \) let \( h(p) \) be the class number of \( K_p = \mathbb{Q}(\sqrt{-p}) \). By a theorem of Siegel, \( \log h(p) \sim \log \sqrt{p} \) \cite[p. 96]{Lan}. Thus, there exists \( \varepsilon(p) \) which tends to 0 as \( p \to \infty \) such that \( \log h(p) = (1 + \varepsilon(p)) \log \sqrt{p} \). It follows that

\[
\sum_p \frac{1}{h(p)^2} = \sum \frac{1}{p^{1+\varepsilon(p)}}.
\]

One knows that \( \sum \frac{1}{p} \) diverges. Unfortunately, without any additional information about \( \varepsilon(p) \) one cannot draw from (1) that its left hand side diverges. Still, the sum does diverge, as we prove below:

**Proposition 1.1 (Murty):** With the notation above,

\[
\sum_{p \equiv 3 \mod 4} \frac{1}{h(p)^2} = \infty,
\]

**Proof:** Lemma 1.2 below reduces (2) to the proof of the existence of a constant \( c > 0 \) such that

\[
\sum_{p \equiv 3 \mod 4} \frac{h(p)}{p} \sim \frac{c \sqrt{x}}{\log x}.
\]

In order to prove (3) suppose \( p \equiv 3 \mod 4 \) is a prime number and let \( \chi_p \) be the quadratic character of \( K_p \). Thus, \( \chi_p(n) = (-1)^{n+1} \left( \frac{n}{p} \right) \) if \( p \nmid n \) \cite[Chap. 3, §8.2]{BoS}. Let \( l \) be a prime number satisfying \( l \nmid 2p \). Then \( l \) decomposes in \( K_p \) into two distinct primes if \( \chi_p(l) = 1 \) and \( l \) remains prime in \( K_p \) if \( \chi_p(l) = -1 \) \cite[Chap. 3, §8.2, Thm. 2]{BoS}. Let \( L(s, \chi_p) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \) be the corresponding \( L \)-series. By the Dirichlet class number formula \( \text{BoS, Chap. 5, §4.1} \), \( h(p) \) is a multiple of \( \sqrt{p}L(1, \chi_p) \) by a constant. Hence, (3) is equivalent to the existence of \( c > 0 \) such that

\[
\sum_{p \equiv 3 \mod 4} \frac{L(1, \chi_p)}{\sqrt{p}} \sim \frac{c \sqrt{x}}{\log x}.
\]

Statement (4) is essentially proved in \cite[pp. 91–93]{FoM}. \( \blacksquare \)

The rest of this section proves the equivalence of (2) and (3).
For each set \( P \) of prime numbers let \( \pi(P, x) \) be the number of \( p \in P \) with \( p \leq x \).

In particular, if \( P \) is the set of all prime numbers, then \( \pi(P, x) = \pi(x) \). If \( P \) is the set of all prime numbers \( p \equiv a \mod n \), we write \( \pi_{a,n}(x) \) for \( \pi(P, x) \). By the prime number theorem for arithmetical progressions [LaO, Thms. 1.3 and 1.4 applied to the case of \( L = \mathbb{Q}(\zeta_n) \)],

\[
\pi(x) = \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right) \quad \text{and} \quad \pi_{a,n}(x) = \frac{1}{\varphi(n)} \cdot \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right),
\]

where \( \varphi(n) \) is Euler’s totient function.

**Lemma 1.2:** For each prime number \( p \) let \( h(p) \) be a positive real number. Suppose that there exists \( c > 0 \) such that

\[
\sum_{\substack{p \leq x \mod 4 \leq x \atop p \equiv 3 \mod 4}} h(p) \frac{\sqrt{p}}{p} \sim c \frac{\sqrt{x}}{\log x}.
\]

Then (2) is true.

**Proof:** Apply summation by parts:

\[
\sum_{\substack{p \leq x \mod 4 \leq x \atop p \equiv 3 \mod 4}} \frac{h(p)}{\sqrt{p}} = \sum_{\substack{p \leq x \mod 4 \leq x \atop p \equiv 3 \mod 4}} \frac{h(p)}{p} \cdot \sqrt{p}
\]

\[
= \sum_{\substack{p \leq x \mod 4 \leq x \atop p \equiv 3 \mod 4}} \frac{h(p)}{p} \cdot \sqrt{p} - \frac{1}{2} \int_2^x \sum_{\substack{p \leq t \mod 4 \leq t \atop p \equiv 3 \mod 4}} \frac{h(p)}{p} \cdot \frac{1}{\sqrt{t}} \, dt
\]

\[
\sim c \frac{\sqrt{x}}{\log x} \cdot \sqrt{x} - \frac{c}{2} \int_2^x \frac{\sqrt{t}}{\log t} \cdot \frac{1}{\sqrt{t}} \, dt \quad \text{by (6)}
\]

\[
= c \frac{x}{\log x} - \frac{c}{2} \int_2^x \frac{dt}{\log t} \sim \frac{c}{2} \frac{x}{\log x}.
\]

The latter approximation is a consequence of the formula \( \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x} \) [Gol, pp. 254–255, Remark (2)]. Hence, by (5) there exists \( x_0 \) such that

\[
c \pi_{3,4}(x) \geq \frac{1}{2} \sum_{\substack{p \leq x \mod 4 \leq x \atop p \equiv 3 \mod 4}} \frac{h(p)}{\sqrt{p}}
\]

and \( \pi_{3,4}(x) \geq \frac{1}{3} \pi(x) \) for all \( x \geq x_0 \). Let \( P = \{ p \equiv 3 \mod 4 \mid h(p) > 6c\sqrt{p} \} \) and let \( P' = \{ p \equiv 3 \mod 4 \mid h(p) \leq 6c\sqrt{p} \} \). Then, for all \( x \geq x_0 \)

\[
\pi_{3,4}(x) \geq \frac{1}{2c} \sum_{\substack{p \leq x \mod 4 \leq x \atop p \equiv 3 \mod 4}} \frac{h(p)}{\sqrt{p}} \geq \frac{1}{2c} \sum_{\substack{p \leq x \mod 4 \leq x \atop p \in P}} \frac{h(p)}{\sqrt{p}} \geq 3\pi(P, x).
\]
It follows from $\pi_{3,4}(x) = \pi(P, x) + \pi(P', x)$ that $\pi(P', x) \geq \frac{2}{3} \pi_{3,4}(x) \geq \frac{2}{5} \pi(x)$ for all $x \geq x_0$. It follows from Lemma 1.3 below that

$$\sum_{p \equiv 3 \mod 4} \frac{1}{h(p)^2} \geq \sum_{p \in P'} \frac{1}{h(p)^2} \geq \frac{1}{36c^2} \sum_{p \in P'} \frac{1}{p} = \infty,$$

as contended. ■

**Lemma 1.3:** Let $Q$ be a set of prime numbers, $0 < b \leq 1$, and $x_0 > 0$ such that $\pi(Q, x) \geq b \pi(x)$ for all $x \geq x_0$. Then $\sum_{p \in Q} \frac{1}{p} = \infty$.

**Proof:** We reduce the statement to the well known fact that $\sum \frac{1}{p} = \infty$ [LeV, p. 100, Thm. 6-13]. To this end make $b$ smaller and add all prime numbers $p \leq x_0$ to $Q$ if necessary, in order to assume that $x_0 = 1$. Then write the set of all prime numbers as an ascending sequence, $p_1 < p_2 < p_3 \cdots$ and define

$$\chi(n) = \begin{cases} 1 & p_n \in Q \\ 0 & p_n \notin Q \end{cases}$$

Then $s(n) = \sum_{i=1}^{n} \chi(i) = \pi(Q, p_n) \geq b \pi(p_n) = bn$. Therefore, with $s(0) = 0$, we have

$$\sum_{p_i \in Q} \frac{1}{p_i} = \sum_{i=1}^{n} \frac{\chi(i)}{p_i} = \sum_{i=1}^{n} \frac{s(i) - s(i-1)}{p_i} = \sum_{i=1}^{n} \frac{s(i)}{p_i} - \sum_{i=1}^{n} \frac{s(i-1)}{p_i} = \frac{bn}{p_n} + b \sum_{i=1}^{n-1} i \left( \frac{1}{p_i} - \frac{1}{p_{i+1}} \right) = b \sum_{i=1}^{n} \frac{i}{p_i} - b \sum_{i=1}^{n-1} \frac{i}{p_{i+1}} = b \sum_{i=1}^{n} \frac{1}{p_i} \rightarrow \infty \quad \text{as } n \rightarrow \infty$$

as contended. ■
2. On the number of elliptic curves with CM over large algebraic fields

Consider a positive integer $e$ and choose $\sigma$ in $\text{Gal}(\mathbb{Q})^e$ at random. We would like to know whether there are infinitely many elliptic curves $E$ (up to $C$-isomorphism) with CM which are defined over $\mathbb{Q}(\sigma)$. We would also like to know whether there are infinitely many elliptic curves $E$ (up to $C$-isomorphism) which are defined over $\mathbb{Q}(\sigma)$ and such that all $C$-endomorphisms of $E$ are defined over $\mathbb{Q}(\sigma)$. Since $\mathbb{Q}(\sigma)$ becomes smaller as $e$ increases, we expect to find for each of those questions an $e_0$ such that the answer to the question is affirmative if and only if $e \leq e_0$. Indeed, we prove that $e_0 = 3$ for the former question and $e_0 = 2$ for the latter.

These results reflect the distribution of the modular $j$-function at singular values, that is complex values which correspond to elliptic curves with CM. To be more precise consider an imaginary quadratic field $K$, an order $O$ of $K$, and a proper $O$-ideal $a$. Then $a$ is a 2-dimensional lattice which is $O$-invertible [Lan, p. 91]. Let $z_1, z_2$ be a basis of $a$ and put $z = z_1/z_2$. Then $j(a) = j(z)$ is the absolute invariant of an elliptic curve $E$ with the analytic presentation $C/a$ and such that $\text{End}(E) \cong O$. Moreover, $E$ can be chosen to be defined by a Weierstrass equation over $\mathbb{Q}(j(a))$. The basic properties of $j(a)$ are intimately connected to class field theory:

**Proposition 2.1** ([Shi, p. 123, Thm. 5.7]): Let $K$ be an imaginary quadratic field, $O$ an order of $K$, and $a$ a proper $O$-ideal. Then:

(a) $K(j(a))/K$ is a Galois extension and $\text{Gal}(K(j(a))/K)$ is isomorphic to the group of all classes of proper $O$-ideals through the correspondence $\sigma \mapsto b$ such that $j(a^\sigma) = j(b^{-1}a)$.

(b) $[K(j(a)) : K] = [\mathbb{Q}(j(a)) : \mathbb{Q}]$.

(c) If $a_1, \ldots, a_n$ are representatives of the classes of proper $O$-ideals, then the values $j(a_1), \ldots, j(a_n)$ form a complete set of conjugates of $j(a)$ over $\mathbb{Q}$, and over $K$.

(d) If $O$ is the ring of integers of $K$ (hence, $a$ is a fractional ideal of $O$ in $K$), then $K(j(a))$ is the maximal unramified abelian extension of $K$, and for each fractional ideal $b$ of $K$ we have $j(a^\sigma) = j(b^{-1}a)$ where $\sigma = \left(\frac{K(j(a))/b}{b}\right)$ is the Artin symbol.

**Corollary 2.2**: Fix an embedding of $\mathbb{Q}$ in $\mathbb{C}$. Then, with the notation of Proposition
2.1, we have:
(a) \( K(j(a)) \) is the Galois closure of \( \mathbb{Q}(j(a)) \) over \( \mathbb{Q} \).
(b) \([K(j(a)) : \mathbb{Q}(j(a))]=2\).
(c) \( K(j(a))/K \) is an abelian extension.
(d) If \( \tau \) is a conjugate of the restriction to \( K(j(a)) \) of the complex conjugation, then \( \tau^{-1}\alpha\tau=\alpha^{-1} \) for each \( \alpha \in \text{Gal}(K(j(a))/K) \).

Proof: Statement (d) follows from [Lan, p. 134, Remark 2]. Statement (c) is a consequence of Proposition 2.1(a). Statements (a) and (b) follow from Proposition 2.1(b,c) and from (d).

Denote the set of all squarefree positive integers by \( D \). For each \( d \in D \) let \( K_d=\mathbb{Q}(\sqrt{-d}) \). Denote the ring of integers and the class number of \( K_d \), respectively, by \( \mathcal{O}_d \) and \( h(d) \). Choose a nonzero ideal \( \mathfrak{a}_d \) of \( \mathcal{O}_d \) and let \( L_d=K_d(j(\mathfrak{a}_d)) \). By Proposition 2.1(a), \( h(d)=[L_d : K_d] \). Choose also an elliptic curve \( E^{(d)} \) with \( j(\mathfrak{a}_d) \) as its absolute invariant which is defined over \( \mathbb{Q}(j(\mathfrak{a}_d)) \) [Lan, p. 300, Thm. 2].

Lemma 2.3: Let \( \Lambda \) be the set of all prime \( l \equiv 3 \mod 4 \). Then, the fields \( L_l \), with \( l \in \Lambda \), are linearly disjoint over \( \mathbb{Q} \).

Proof: Consider a finite set \( \Lambda_0 \) of \( \Lambda \) and an element \( l' \in \Lambda \setminus \Lambda_0 \). Let \( L=\prod_{l \in \Lambda_0} L_l \). By Corollary 2.2(a), each \( L_l \) is Galois over \( \mathbb{Q} \). Hence, it suffices to prove that \( L \cap L_{l'}=\mathbb{Q} \). Since, by a theorem of Minkowski, each proper extension of \( \mathbb{Q} \) is ramified [Jan, p. 57, Cor. 11.11] it suffices to prove that no prime number \( p \) is ramified in \( L \cap L_{l'} \).

Indeed, for each \( l \in \Lambda \) we have \( -l \equiv 1 \mod 4 \). Hence, the discriminant of \( K_l/\mathbb{Q} \) is \(-l \) [BoS, §2.7, p. 132, Thm. 1], so the only prime number which ramifies in \( K_l \) is \( l \). Since \( L_l/K_l \) is unramified (Proposition 2.1(d)), the only prime number which ramifies in \( L_l \) is \( l \). In particular, \( l' \) is unramified in each \( L_l \) with \( l \in \Lambda_0 \). Hence, \( l' \) is unramified in \( L \), so \( l' \) is unramified in \( L \cap L_{l'} \). If \( p \neq l' \), then \( p \) is unramified in \( L_{l'} \), so \( p \) is also unramified in \( L \cap L_{l'} \). Consequently, \( L \cap L_{l'}=\mathbb{Q} \), as asserted.

The orders of \( K_d \) have the form \( O_{d,c}=\mathbb{Z}+c\mathcal{O}_d \), where \( c \) ranges over all positive integers. For each \( d \in D \) and \( c \in \mathbb{N} \) choose a proper \( \mathcal{O}_{d,c} \)-ideal \( \mathfrak{a}_{d,c} \) and let \( L_{d,c}=\mathbb{Q}(\sqrt{-d}) \).
$K_d(j(a_{d,c}))$. By Proposition 2.1(c), $h(d,c) = [L_{d,c} : K_d]$ is the class number of $O_{d,c}$. It is related to $h(d)$ by the following formula [Lan, p. 95]:

$$h(d,c) = h(d) - \frac{\psi(d,c)}{(O_d^\times : O_{d,c}^\times)},$$

where

$$\psi(d,c) = c \prod_{p|c} \left( 1 - \frac{K_d}{p} \frac{1}{p} \right),$$

and $(\frac{K_d}{p})$ is 1 if $p$ decomposes in $K_d$, $-1$ if $p$ remains irreducible in $K_d$, and 0 if $p$ ramifies in $K_d$.

**Lemma 2.4:** Let $L$ be a finite Galois extension of $\mathbb{Q}$. Then there are only finitely many elliptic curves $E$ with CM (up to $\mathbb{C}$-isomorphism) which are defined over $L$ and satisfy $\text{End}(E) \subseteq L$.

**Proof:** Let $E$ be an elliptic curve over $L$ with CM such that $\text{End}(E) \subseteq L$. Then $\text{End}(E) \otimes \mathbb{Q} = K_d$ for some $d \in D$ [Shi, p. 103, Prop. 4.5]. Moreover, $\text{End}(E)$ is an order of $O_d$ and there is a unique $c \in \mathbb{N}$ with $\text{End}(E) = O_{d,c}$ [Shi, p. 105, Prop. 4.1]. In addition, $E \cong \mathbb{C}/a$ for some proper $O_{d,c}$-ideal $a$ [Shi, p. 104, Prop. 4.8]. In particular $j(a)$ is the absolute invariant of $E$, so $K_d(j(a)) \subseteq L$. By the comments preceding the lemma, $[K_d(j(a)) : \mathbb{Q}] = 2h(d,c)$ and $h(d,c)$ tends to infinity if $d$ or $c$ tend to infinity. Indeed, by the estimates quoted in the proof of the next lemma, $\log h(d) \sim \log d^{1/2}$ and $\psi(d,c) \geq \frac{ac}{\log \log c}$ for some $a > 0$. Thus, there are only finitely many possibilities for $(d,c)$. For each pair $(d,c) \in D \times \mathbb{N}$ there are only finitely many possibilities (up to $\mathbb{C}$-isomorphism) for $E$. They correspond to the number $h(d,c)$ of classes of proper $O_{d,c}$-ideals [Shi, p. 105, Prop. 4.10]. Consequently, there are only finitely many $\mathbb{C}$-isomorphism classes of elliptic curves $E$ with CM such that $j(E) \in L$ and $\text{End}(E) \subseteq L$.

**Lemma 2.5:** Let $D$ be the set of all squarefree positive integers. Then

$$\sum_{d \in D} \sum_{c=1}^{\infty} \frac{1}{h(d,c)^2} < \infty.$$
Proof: By (1), it suffices to prove that

$$
\sum_{d \in D} \frac{1}{h(d)^3} \sum_{c=1}^{\infty} \frac{\left( O_d^x : O_{d,c}^x \right)^3}{\psi(d,c)^3} < \infty.
$$

There are at most 6 units in $O_d$ [BoS, §2.7.3]. Hence, the numerator in the inner sum of the right hand side of (4) is bounded. Next consider the Euler totient function: $\varphi(c) = c \prod_{p \mid c} \left( 1 - \frac{1}{p} \right)$. It has an estimate from below: $\varphi(c) > \frac{ac}{\log \log c}$ for some positive constant $a$ [Lev, p. 114, Thm. 6-26]. For each $p$, $1 - \left( \frac{K}{p} \right) / p \geq 1 - \frac{1}{p}$. Hence, $\psi(d,c) \geq \varphi(c)$, so

$$
\sum_{c=1}^{\infty} \frac{1}{\psi(d,c)^3} \leq \sum_{c=1}^{\infty} \frac{1}{\varphi(c)^3} \leq \frac{1}{a^3} \sum_{c=1}^{\infty} \frac{(\log \log c)^3}{c^3} < \infty.
$$

Finally, by a theorem of Siegel, $\log h(d) \sim \log d^{1/2}$ [Lan, p. 96]. This means that for each $d \in D$ there exists $\varepsilon(d) > 0$ such that $h(d) = d^{\varepsilon(d)/2}$ and $\varepsilon(d) \to 1$ as $d \to \infty$. In particular, $\varepsilon(d) > \frac{3}{4}$ for all $d$ sufficiently large. Hence, $\frac{3-\varepsilon(d)}{2} > \frac{9}{8}$ for almost all $d$ sufficiently large, so there exists $b > 0$ such that

$$
\sum_{d \in D} \frac{1}{h(d)^3} = \sum_{d \in D} \frac{1}{d^{3\varepsilon(d)/2}} \leq \sum_{d=1}^{\infty} \frac{b}{d^{9/8}} < \infty.
$$

We conclude from (5) and (6) that (4) holds.

The main tool from probability theory we use is the Borel-Cantelli Lemma. We formulate its Galois theoretic version as appears in [FrJ, Theorem 18.5.3]:

**Lemma 2.6:** Let $L_1, L_2, L_3, \ldots$ be finite separable extensions of a field $K$. For each $i \geq 1$ let $\tilde{A}_i$ be a set of left cosets of $\text{Gal}(L_i)^e$ in $\text{Gal}(K)^e$ and

$$
A_i = \{ \sigma \in \text{Gal}(K)^e \mid \sigma \text{Gal}(L_i)^e \in \tilde{A}_i \}.
$$

Let $A$ be the set of all $\sigma \in \text{Gal}(K)^e$ which belong to infinitely many $A_i$’s.

(a) If $\sum_{i=1}^{\infty} \frac{|A_i|}{|L_i:K|^e} < \infty$, then $\mu(A) = 0$.

(b) Suppose $L_1, L_2, L_3, \ldots$ are linearly disjoint over $K$ and $\sum_{i=1}^{\infty} \frac{|A_i|}{|L_i:K|^e} = \infty$, then $\mu(A) = 1$. 

10
Theorem 2.7: The following holds for almost all $\sigma \in \text{Gal}(\mathbb{Q})^e$:

(a) If $e \leq 2$, then there are infinitely many elliptic curves $E$ (up to $\mathbb{C}$-isomorphism) with CM over $\hat{\mathbb{Q}}(\sigma)$ such that $\text{End}(E) \subseteq \hat{\mathbb{Q}}(\sigma)$.

(b) If $e \geq 3$, then there are only finitely many elliptic curves $E$ (up to $\mathbb{C}$-isomorphism) with CM over $\hat{\mathbb{Q}}(\sigma)$ such that $\text{End}(E) \subseteq \hat{\mathbb{Q}}(\sigma)$.

Proof of (a): Let $\Lambda$ be the set of all prime numbers $l \equiv 3 \mod 4$. For each $l$ we have $[L_l : K_l] = h(l)$ and $[L_l : \mathbb{Q}_l] = 2h(l)$. In addition, $E^{(l)}$ is defined over $\mathbb{Q}(j(a_l))$ and $\text{End}(E^{(l)}) = O_l$. Hence, if $\sigma \in \text{Gal}(L_l)$, then $E^{(l)}$ is defined over $\hat{\mathbb{Q}}(\sigma)$ and $\text{End}(E^{(l)}) \subseteq \hat{\mathbb{Q}}(\sigma)$. By Proposition 1.1,

$$\sum_{l \in \Lambda} \frac{1}{[L_l : \mathbb{Q}]^e} = \frac{1}{2^e} \sum_{l \in \Lambda} \frac{1}{h(l)^e} \geq \frac{1}{2^e} \sum_{l \in \Lambda} \frac{1}{h(l)^2} = \infty.$$  

By Lemma 2.3, the fields $L_l$, $l \in \Lambda$, are linearly disjoint. In particular $j(a_l) \neq j(a_{l'})$, so $E^{(l)} \neq E^{(l)}$ if $l \neq l'$. It follows from Borel-Cantelli [FrJ, Lemma 18.5.3(b)] that for almost all $\sigma \in \text{Gal}(\mathbb{Q})^e$ there are infinitely many primes $l$ such that $E^{(l)}$ is defined over $\hat{\mathbb{Q}}(\sigma)$ and $\text{End}(E^{(l)}) \subseteq \hat{\mathbb{Q}}(\sigma)$, as desired.

Proof of (b): Let $\sigma \in \text{Gal}(\mathbb{Q})^e$. If an elliptic curve $E$ with CM is defined over $\hat{\mathbb{Q}}(\sigma)$ and $\text{End}(E) \subseteq \hat{\mathbb{Q}}(\sigma)$, then there exist $d \in D$ and a positive integer $c$ such that $L_{d,c} \subseteq \hat{\mathbb{Q}}(\sigma)$. By Lemma 2.4, for each $d$ and $c$ there are only finitely many $E$'s (up to a $\mathbb{C}$-isomorphism) which are defined together with their endomorphisms over $L_{d,c}$. Thus, if there are infinitely many elliptic curves with CM which are defined together with their endomorphisms over $L_{d,c}$, then $\sigma$ belongs to infinitely many sets $\text{Gal}(L_{d,c})^e$. Since $[L_{d,c} : \mathbb{Q}] = 2h(d,c)$, Lemma 2.5 implies that $\sum_{d \in D} \sum_{c=1}^{\infty} \frac{1}{[L_{d,c} : \mathbb{Q}]^e} = \sum_{d \in D} \sum_{c=1}^{\infty} \frac{1}{h(d,c)^e} < \infty$. Hence, by Borel-Cantelli [FrJ, Lemma 18.5.3.(a)], the measure of those $\sigma$'s is 0.

If an elliptic curve $E$ with CM is defined over a field $K$ and if $\text{End}(E) \subseteq K$, then, by Proposition 2.1, all conjugates of $j_E$ are in $K(j_E)$. Therefore, for $\sigma \in \text{Gal}(\mathbb{Q})^e$, if we drop the condition that the endomorphisms of the elliptic curves are defined over $\hat{\mathbb{Q}}(\sigma)$, then the probability that there are infinitely many elliptic curves with CM over $\hat{\mathbb{Q}}(\sigma)$ increases. This is reflected in the following result:
Theorem 2.8: The following holds for almost all $\sigma \in \text{Gal}(\mathbb{Q})^e$:

(a) If $e \leq 3$, then there are infinitely many elliptic curves $E$ (up to isomorphism) with CM over $\bar{\mathbb{Q}}(\sigma)$.

(b) If $e \geq 4$, then there are only finitely many elliptic curves $E$ (up to isomorphism) with CM over $\bar{\mathbb{Q}}(\sigma)$.

Proof of (a): As in the proof of Theorem 2.7 let $\Lambda$ be the set of primes $l \equiv 3 \mod 4$. Consider $l \in \Lambda$ and let $K_l$, $O_l$, $L_l$, $a_l$, $E(l)$, and $h(l)$ be as above. Let $\tau$ be a generator of $\text{Gal}(L_l/\mathbb{Q}(j(a_l)))$. If $\alpha \in \text{Gal}(L_l/K_l)$, then $\tau^\alpha$ generates $\text{Gal}(L_l/\mathbb{Q}(j(a_l))^\alpha)$ and $(E(l))^\alpha$ is an elliptic curve with CM which is defined over $\mathbb{Q}(j(a_l))^\alpha$. Thus, if $\sigma \in \text{Gal}(\mathbb{Q})^e$ and $\text{res}_{L_l} \sigma \in (\tau^\alpha)^e$, then $(E(l))^\alpha$ is defined over $\bar{\mathbb{Q}}(\sigma)$.

Claim: $\#\{\tau^\alpha \mid \alpha \in \text{Gal}(L_l/K_l)\} = h(l)$.

Indeed, embed $L_l$ in $\mathbb{C}$ and let $\rho$ be the restriction of the complex conjugation to $L_l$. Since $K_l$ is an imaginary quadratic field, $\text{res}_{K_l} \rho \neq 1$, so $\rho^2 = 1$ and $\rho \neq 1$. Since $l \equiv 3 \mod 4$, $h(l)$ is odd [BoS, p. 346, Thm. 4]. Thus, $\rho \in \text{Gal}(L_l/\mathbb{Q}) \setminus \text{Gal}(L_l/K_l)$. Now assume $\rho^\alpha = \rho$ for some $\alpha \in \text{Gal}(L_l/K_l)$. By Corollary 2.2(d), $\rho \alpha \rho = \alpha^{-1}$, hence $1 = \rho^2 = \alpha^{-1} \rho \alpha = \alpha^{-2}$, which implies $\alpha = 1$ (because $h(l)$ is odd). It follows that the map $\alpha \mapsto \rho^\alpha$ from $\text{Gal}(L_l/K_l)$ into $\text{Gal}(L_l/\mathbb{Q}) \setminus \text{Gal}(L_l/K_l)$ is injective. Since both sets have the same cardinality, the map is bijective. In particular, $\tau$ is conjugate to $\rho$ by an element of $\text{Gal}(L_l/K_l)$. Consequently, $\#\{\tau^\alpha \mid \alpha \in \text{Gal}(L_l/K_l)\} = \#\{\rho^\alpha \mid \alpha \in \text{Gal}(L_l/K_l)\} = [L_l : K_l] = h(l)$.

Let $\bar{A}_l = \bigcup_{\alpha \in \text{Gal}(L_l/K_l)} \{1, \tau^\alpha\}^e$. Each of the sets $\{1, \tau^\alpha\}^e$ has $2^e$ elements and the intersection of every two of them contains only one element (by the Claim). Thus, $|\bar{A}_l| = h(l) \cdot 2^e - (h(l) - 1)$. Let $A_l = \{\sigma \in \bar{\mathbb{Q}} \mid \text{res}_{L_l} \sigma \in \bar{A}_l\}$. Then, $\mu(A_l) = \frac{h(l) \cdot 2^e - (h(l) - 1)}{(2h(l))^e}$. Since $e \leq 3$, Proposition 1.1 implies that

$$\sum_{l \in \Lambda} \mu(A_l) = \sum_{l \in \Lambda} \frac{h(l) \cdot 2^e - (h(l) - 1)}{(2h(l))^e} \geq \frac{2^e - 1}{2^e} \sum_{l \in \Lambda} \frac{1}{h(l)^2} = \infty.$$

By Lemma 2.3, the fields $L_l$, $l \in \Lambda$ are linearly disjoint. It follows from Borel-Cantelli that for almost all $\sigma \in \text{Gal}(\mathbb{Q})^e$ there are infinitely many elliptic curves with CM which are defined over $\bar{\mathbb{Q}}(\sigma)$. 

12
Proof of (b): Let $d$ range over $D$ and let $c$ range over all positive integers. For each $d$ and $c$ let
\[ A(d, c) = \bigcup_{\alpha \in \text{Gal}(L_{d,c}/K_d)} \text{Gal}(\mathbb{Q}(j(a_{d,c})^\alpha))^{e}. \]
By Proposition 2.1(b),
\[ \mu(A(d, c)) \leq [L_{d,c} : K_d] \left( \frac{1}{[\mathbb{Q}(j(a_{d,c})) : \mathbb{Q}]} \right)^e = \frac{1}{h(d,c)^{e-1}}. \]
If for $\sigma \in \text{Gal}(\mathbb{Q})^e$ there are infinitely many elliptic curves with CM which are defined over $\tilde{\mathbb{Q}}(\sigma)$, then $\sigma$ belongs to infinitely many of the sets $A(d, c)$ (as argued in the proof of Lemma 2.4). Since $e \geq 4$, we have by Lemma 2.5 that
\[ \mu\left( \bigcup_{d,c} A(d, c) \right) \leq \sum_{d,c} \frac{1}{h(d,c)^{e-1}} \leq \sum_{d,c} \frac{1}{h(d,c)^3} < \infty. \]
We conclude from Borel-Cantelli that almost no $\sigma \in \text{Gal}(\mathbb{Q})^e$ belongs to infinitely many sets $A(d, c)$. Thus, for almost all $\sigma \in \text{Gal}(\mathbb{Q})^e$, there are only finitely many elliptic curves with CM (up to a $\mathbb{C}$-isomorphism) which are defined over $\tilde{\mathbb{Q}}(\sigma)$. 

**Corollary 2.9:** The following holds for almost all $\sigma \in \text{Gal}(\mathbb{Q})^e$:

(a) If $e \leq 2$, then there are infinitely many elliptic curves $E$ (up to $\mathbb{C}$-isomorphism) with CM over $\tilde{\mathbb{Q}}[\sigma]$.

(b) If $e \geq 3$, then there are only finitely many elliptic curves $E$ (up to $\mathbb{C}$-isomorphism) with CM over $\tilde{\mathbb{Q}}[\sigma]$.

**Proof:** First suppose $e \leq 2$. By Theorem 2.7(a), for almost all $\sigma \in \text{Gal}(\mathbb{Q})^e$ there are infinitely many elliptic curves $E$ with CM over $\tilde{\mathbb{Q}}(\sigma)$ such that $\text{End}(E) \subseteq \tilde{\mathbb{Q}}(\sigma)$. For all such $\sigma$ and $E$ let $K_E$ be the quotient field of $\text{End}(E)$. Then $K_E(j_E)$ is a Galois extension of $\mathbb{Q}$ which is contained in $\tilde{\mathbb{Q}}(\sigma)$. Hence, $K_E(j_E) \subseteq \tilde{\mathbb{Q}}[\sigma]$. It follows that an isomorphic copy of $E$ (over $\mathbb{C}$) is defined over $\tilde{\mathbb{Q}}[\sigma]$.

Now suppose $e \geq 3$. For each $\sigma \in \text{Gal}(\mathbb{Q})^e$ let $\mathcal{E}(\sigma)$ be the set of all elliptic curves $E$ (up to $\mathbb{C}$-isomorphism) which are defined over $\tilde{\mathbb{Q}}(\sigma)$ such that $\text{End}(E) \subseteq \tilde{\mathbb{Q}}(\sigma)$. Let $S$ be the set of all $\sigma \in \text{Gal}(\mathbb{Q})^e$ such that $\mathcal{E}(\sigma)$ is a finite set. By Theorem 2.7(b), $\mu(S) = 1$. 

13
Consider $\sigma \in S$ and let $E$ be an elliptic curve with CM over $\mathbb{Q}[\sigma]$. Then $j_E \in \mathbb{Q}[\sigma]$. Hence, the Galois closure of $\mathbb{Q}(j_E)/\mathbb{Q}$ is contained in $\mathbb{Q}[\sigma]$. By Corollary 2.2(a), the latter contains $\text{End}(E)$. Hence, $E \in \mathcal{E}(\sigma)$. Consequently, there are only finitely many elliptic curves (up to $\mathbb{C}$-isomorphism with CM over $\mathbb{Q}[\sigma]$). □
References


9 February, 2007