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 $\mathrm{Gal}(\mathbb{Q})$ and equip each of the cartesian powers $\mathrm{Gal}(\mathbb{Q})^e$ by the normalized Haar measure μ. Let $\tilde{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$. For each $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e)$ let $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ be the fixed field in $\tilde{\mathbb{Q}}$ of $\sigma_1, \ldots, \sigma_e$. The behavior of the fields $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ 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 $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$:*

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

(b) *The field $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ is PAC, that is, each absolutely irreducible variety V defined over $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ has a $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$-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 $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$ the rank of $A(\tilde{\mathbb{Q}}(\boldsymbol{\sigma}))$ is infinite.*

Note that the fields $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ become smaller as e increases. Thus, it is expected that in general less arithmetical objects will be defined over $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ 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 $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ the set $\bigcup_{i=1}^{\infty} A_{l^i}(\tilde{\mathbb{Q}}(\boldsymbol{\sigma}))$ is finite (while $\bigcup_{i=1}^{\infty} A_{l^i}(\tilde{\mathbb{Q}})$ is infinite, which is the case if $e = 0$).*

Here $A_n(L) = \{\mathbf{p} \in A(L) \mid n\mathbf{p} = 0\}$ 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 $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$:*

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

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

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

(a) *If $e = 1$, then $E_{\mathrm{tor}}(\tilde{\mathbb{Q}}(\boldsymbol{\sigma}))$ is infinite.*

(b) *If $e \geq 2$, then $E_{\mathrm{tor}}(\tilde{\mathbb{Q}}(\boldsymbol{\sigma}))$ 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 $\tilde{\mathbb{Q}}$ such that for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ infinitely many objects of P are defined over $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ if $e < e_0$ and only finitely many objects of P are defined over $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ 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 $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$:*

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

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

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

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

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

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 $\sum \frac{1}{h(p)^2} = \infty$, 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 $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$. For each $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$ we denote the maximal Galois extension of $\mathbb{Q}$ which is contained in $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ by $\tilde{\mathbb{Q}}[\boldsymbol{\sigma}]$. Then the following holds:

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

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

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

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, $\log h(p) \sim \log \sqrt{p}$ [Lan, p. 96]. 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

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

One knows that $\sum \frac{1}{p}$ diverges. Unfortunately, without any additional information about $\varepsilon(p)$ one can not 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,*

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

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

$$\sum_{\substack{p \le x \\ p \equiv 3 \mod 4}} \frac{h(p)}{p} \sim \frac{c\sqrt{x}}{\log x}. \tag{3}$$

In order to prove (3) suppose $p \equiv 3 \mod 4$ is a prime number and let χ_p be the quadratic character of K_p. Thus, $\chi_p(n) = (-1)^{\frac{n-1}{2}} \left(\frac{n}{p}\right)$ if $p \nmid n$ [BoS, Chap. 3, §8.2]. 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 $\chi_p(l) = -1$ [BoS, Chap. 3, §8.2, Thm. 2]. 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 [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

$$\sum_{\substack{p \le x \\ p \equiv 3 \mod 4}} \frac{L(1, \chi_p)}{\sqrt{p}} \sim \frac{c\sqrt{x}}{\log x} \tag{4}$$

Statement (4) is essentially proved in [FoM, pp. 91–93]. ∎

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 $p\le x$. 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 $L=\mathbb{Q}(\zeta_n)$],

$$\pi(x)=\frac{x}{\log x}+O\Big(\frac{x}{\log^2 x}\Big) \quad \text{and} \quad \pi_{a,n}(x)=\frac{1}{\varphi(n)}\cdot\frac{x}{\log x}+O\Big(\frac{x}{\log^2 x}\Big)\ , \tag{5}$$

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*

$$\sum_{\substack{p\le x\\ p\equiv 3 \mod 4}}\frac{h(p)}{p}\sim\frac{c\sqrt{x}}{\log x} \tag{6}$$

Then (2) is true.

Proof: Apply summation by parts:

$$\begin{aligned}
\sum_{\substack{p\le x\\ p\equiv 3 \mod 4}}\frac{h(p)}{\sqrt{p}} &= \sum_{\substack{p\le x\\ p\equiv 3 \mod 4}}\frac{h(p)}{p}\cdot\sqrt{p}\\
&= \sum_{\substack{p\le x\\ p\equiv 3 \mod 4}}\frac{h(p)}{p}\cdot\sqrt{x}-\frac{1}{2}\int_2^x \sum_{\substack{p\le t\\ p\equiv 3 \mod 4}}\frac{h(p)}{p}\cdot\frac{1}{\sqrt{t}}dt\\
&\sim c\frac{\sqrt{x}}{\log x}\cdot\sqrt{x}-\frac{c}{2}\int_2^x\frac{\sqrt{t}}{\log t}\cdot\frac{1}{\sqrt{t}}dt \qquad \text{by (6)}\\
&= c\frac{x}{\log x}-\frac{c}{2}\int_2^x\frac{dt}{\log t}\sim\frac{c}{2}\frac{x}{\log x}.
\end{aligned}$$

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

$$c\pi_{3,4}(x)\ge\frac{1}{2}\sum_{\substack{p\le x\\ p\equiv 3 \mod 4}}\frac{h(p)}{\sqrt{p}}$$

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

$$\pi_{3,4}(x)\ge\frac{1}{2c}\sum_{\substack{p\le x\\ p\equiv 3 \mod 4}}\frac{h(p)}{\sqrt{p}}\ge\frac{1}{2c}\sum_{\substack{p\le x\\ p\in P}}\frac{h(p)}{\sqrt{p}}\ge 3\pi(P,x).$$

It follows from $\pi_{3,4}(x) = \pi(P, x) + \pi(P', x)$ that $\pi(P', x) \geq \frac{2}{3}\pi_{3,4}(x) \geq \frac{2}{9}\pi(x)$ 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

$$\begin{aligned}
\sum_{\substack{i=1 \\ p_i \in Q}}^{n} \frac{1}{p_i} &= \sum_{i=1}^{n} \frac{\chi(i)}{p_i} = \sum_{i=1}^{n} \frac{s(i) - s(i-1)}{p_i} = \sum_{i=1}^{n} \frac{s(i)}{p_i} - \sum_{i=1}^{n} \frac{s(i-1)}{p_i} \\
&= \sum_{i=1}^{n} \frac{s(i)}{p_i} - \sum_{i=1}^{n-1} \frac{s(i)}{p_{i+1}} = \frac{s(n)}{p_n} + \sum_{i=1}^{n-1} s(i)\Big(\frac{1}{p_i} - \frac{1}{p_{i+1}}\Big) \\
&\geq \frac{bn}{p_n} + b\sum_{i=1}^{n-1} i\Big(\frac{1}{p_i} - \frac{1}{p_{i+1}}\Big) = \frac{bn}{p_n} + b\sum_{i=1}^{n-1} \frac{i}{p_i} - b\sum_{i=1}^{n-1} \frac{i}{p_{i+1}} \\
&= b\sum_{i=1}^{n} \frac{i}{p_i} - b\sum_{i=1}^{n} \frac{i-1}{p_i} = b\sum_{i=1}^{n} \frac{1}{p_i} \to \infty \qquad \text{as } n \to \infty
\end{aligned}$$

as contended. ∎

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

Consider a positive integer e and choose $\boldsymbol{\sigma}$ in $\mathrm{Gal}(\mathbb{Q})^e$ at random. We would like to know whether there are infinitely many elliptic curves E (up to $\mathbb{C}$-isomorphism) with CM which are defined over $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$. We would also like to know whether there are infinitely many elliptic curves E (up to $\mathbb{C}$-isomorphism) which are defined over $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ and such that all $\mathbb{C}$-endomorphisms of E are defined over $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$. Since $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ 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 $e \le e_0$. 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 $\mathfrak{a}$. Then $\mathfrak{a}$ is a 2-dimensional lattice which is O-invertible [Lan, p. 91]. Let z_1, z_2 be a basis of $\mathfrak{a}$ and put $z = z_1/z_2$. Then $j(\mathfrak{a}) = j(z)$ is the absolute invariant of an elliptic curve E with the analytic presentation $\mathbb{C}/\mathfrak{a}$ and such that $\mathrm{End}(E) \cong O$. Moreover, E can be chosen to be defined by a Weierstrass equation over $\mathbb{Q}(j(\mathfrak{a}))$. The basic properties of $j(\mathfrak{a})$ 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 $\mathfrak{a}$ a proper O-ideal. Then:*

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

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

(c) *If $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are representatives of the classes of proper O-ideals, then the values $j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_n)$ form a complete set of conjugates of $j(\mathfrak{a})$ over $\mathbb{Q}$, and over K.*

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

Corollary 2.2: *Fix an embedding of $\tilde{\mathbb{Q}}$ in $\mathbb{C}$. Then, with the notation of Proposition*

2.1, we have:

(a) $K(j(\mathfrak{a}))$ *is the Galois closure of* $\mathbb{Q}(j(\mathfrak{a}))$ *over* $\mathbb{Q}$.

(b) $[K(j(\mathfrak{a})) : \mathbb{Q}(j(\mathfrak{a}))] = 2$.

(c) $K(j(\mathfrak{a}))/K$ *is an abelian extension.*

(d) *If* τ *is a conjugate of the restriction to* $K(j(\mathfrak{a}))$ *of the complex conjugation, then* $\tau^{-1}\alpha\tau = \alpha^{-1}$ *for each* $\alpha \in \mathrm{Gal}(K(j(\mathfrak{a}))/K)$.

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 O_d and $h(d)$. Choose a nonzero ideal $\mathfrak{a}_d$ of 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* Λ *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 Λ_0 of Λ and an element $l' \in \Lambda \smallsetminus \Lambda_0$. 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 $O_{d,c} = \mathbb{Z} + cO_d$, where c ranges over all positive integers. For each $d \in D$ and $c \in \mathbb{N}$ choose a proper $O_{d,c}$-ideal $\mathfrak{a}_{d,c}$ and let $L_{d,c} =$

$K_d(j(\mathfrak{a}_{d,c}))$. 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]:

$$h(d,c) = h(d)\frac{\psi(d,c)}{(O_d^\times : O_{d,c}^\times)}, \tag{1}$$

where

$$\psi(d,c) = c\prod_{p|c}\left(1 - \left(\frac{K_d}{p}\right)\frac{1}{p}\right), \tag{2}$$

and $\left(\frac{K_d}{p}\right)$ 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* $\mathrm{End}(E) \subseteq L$.

Proof: Let E be an elliptic curve over L with CM such that $\mathrm{End}(E) \subseteq L$. Then $\mathrm{End}(E) \otimes \mathbb{Q} = K_d$ for some $d \in D$ [Shi, p. 103, Prop. 4.5]. Moreover, $\mathrm{End}(E)$ is an order of O_d and there is a unique $c \in \mathbb{N}$ with $\mathrm{End}(E) = O_{d,c}$ [Shi, p. 105, Prop. 4.1]. In addition, $E \cong \mathbb{C}/\mathfrak{a}$ for some proper $O_{d,c}$-ideal $\mathfrak{a}$ [Shi, p. 104, Prop. 4.8]. In particular $j(\mathfrak{a})$ is the absolute invariant of E, so $K_d(j(\mathfrak{a})) \subseteq L$. By the comments preceding the lemma, $[K_d(j(\mathfrak{a})) : \mathbb{Q}] = 2h(d,c)$ 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, $\log h(d) \sim \log d^{\frac{1}{2}}$ 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 $\mathrm{End}(E) \subseteq L$. ∎

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

$$\sum_{d\in D}\sum_{c=1}^{\infty}\frac{1}{h(d,c)^3} < \infty. \tag{3}$$

Proof: By (1), it suffices to prove that

$$\sum_{d\in D}\frac{1}{h(d)^3}\sum_{c=1}^{\infty}\frac{(O_d^\times : O_{d,c}^\times)^3}{\psi(d,c)^3}<\infty. \tag{4}$$

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: $\varphi(c)=c\prod_{p|c}\left(1-\frac{1}{p}\right)$. 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, $1-\left(\frac{K_d}{p}\right)\frac{1}{p}\geq 1-\frac{1}{p}$. Hence, $\psi(d,c)\geq\varphi(c)$, so

$$\sum_{c=1}^{\infty}\frac{1}{\psi(d,c)^3}\leq\sum_{c=1}^{\infty}\frac{1}{\varphi(c)^3}\leq\frac{1}{a^3}\sum_{c=1}^{\infty}\frac{(\log\log c)^3}{c^3}<\infty. \tag{5}$$

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, $\frac{3\cdot\varepsilon(d)}{2}>\frac{9}{8}$ for almost all d sufficiently large, so there exists $b>0$ such that

$$\sum_{d\in D}\frac{1}{h(d)^3}=\sum_{d\in D}\frac{1}{d^{3\cdot\varepsilon(d)/2}}\leq\sum_{d=1}^{\infty}\frac{b}{d^{9/8}}<\infty. \tag{6}$$

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 $\bar{A}_i$ be a set of left cosets of $\mathrm{Gal}(L_i)^e$ in $\mathrm{Gal}(K)^e$ and*

$$A_i=\{\boldsymbol{\sigma}\in\mathrm{Gal}(K)^e \mid \boldsymbol{\sigma}\mathrm{Gal}(L_i)^e\in\bar{A}_i\}.$$

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

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

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

THEOREM 2.7: *The following holds for almost all* $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$*:*

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

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

Proof of (a): Let Λ 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 $\mathbb{Q}(j(\mathfrak{a}_l))$ and $\mathrm{End}(E^{(l)}) = O_l$. Hence, if $\boldsymbol{\sigma} \in \mathrm{Gal}(L_l)$, then $E^{(l)}$ is defined over $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ and $\mathrm{End}(E^{(l)}) \subseteq \tilde{\mathbb{Q}}(\boldsymbol{\sigma})$. By Proposition 1.1,

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

By Lemma 2.3, the fields L_l, $l \in \Lambda$, are linearly disjoint. In particular $j(\mathfrak{a}_l) \neq j(\mathfrak{a}_{l'})$, so $E^{(l)} \not\cong E^{(l)}$ if $l \neq l'$. It follows from Borel-Cantelli [FrJ, Lemma 18.5.3(b)] that for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$ there are infinitely many primes l such that $E^{(l)}$ is defined over $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ and $\mathrm{End}(E^{(l)}) \subseteq \tilde{\mathbb{Q}}(\boldsymbol{\sigma})$, as desired.

Proof of (b): Let $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$. If an elliptic curve E with CM is defined over $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ and $\mathrm{End}(E) \subseteq \tilde{\mathbb{Q}}(\boldsymbol{\sigma})$, then there exist $d \in D$ and a positive integer c such that $L_{d,c} \subseteq \tilde{\mathbb{Q}}(\boldsymbol{\sigma})$. 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 $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$, then $\boldsymbol{\sigma}$ belongs to infinitely many sets $\mathrm{Gal}(L_{d,c})^e$. Since $[L_{d,c} : \mathbb{Q}] = 2h(d,c)$, Lemma 2.5 implies that $\sum_{d\in D}\sum_{c=1}^{\infty} \frac{1}{[L_{d,c}:\mathbb{Q}]^e} \leq \sum_{d\in D}\sum_{e=1}^{\infty} \frac{1}{h(d,c)^3} < \infty$. Hence, by Borel-Cantelli [FrJ, Lemma 18.5.3.(a)], the measure of those $\boldsymbol{\sigma}$'s is 0. ∎

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

THEOREM 2.8: *The following holds for almost all* $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$*:*

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

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

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

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

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

Let $\bar{A}_l = \bigcup_{\alpha \in \mathrm{Gal}(L_l/K_l)}\{1, \tau^\alpha\}^e$. 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 $A_l = \{\boldsymbol{\sigma} \in \mathrm{Gal}(\tilde{\mathbb{Q}})^e \mid \mathrm{res}_{L_l}\boldsymbol{\sigma} \in \bar{A}_l\}$. Then, $\mu(A_l) = \frac{h(l)\cdot 2^e - (h(l)-1)}{(2h(l))^e}$. Since $e \le 3$, Proposition 1.1 implies that

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

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

Proof of (b): Let d range over D and let c range over all positive integers. For each d and c let

$$A(d,c) = \bigcup_{\alpha \in \mathrm{Gal}(L_{d,c}/K_d)} \mathrm{Gal}(\mathbb{Q}(j(\mathfrak{a}_{d,c})^\alpha))^e.$$

By Proposition 2.1(b),

$$\mu(A(d,c)) \le [L_{d,c} : K_d] \biggl(\frac{1}{[\mathbb{Q}(j(\mathfrak{a}_{d,c})) : \mathbb{Q}]} \biggr)^e = \frac{1}{h(d,c)^{e-1}}\,.$$

If for $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$ there are infinitely many elliptic curves with CM which are defined over $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$, then $\boldsymbol{\sigma}$ belongs to infinitely many of the sets $A(d,c)$ (as argued in the proof of Lemma 2.4). Since $e \ge 4$, we have by Lemma 2.5 that

$$\mu\bigl(\bigcup_{d,c} A(d,c)\bigr) \le \sum_{d,c} \frac{1}{h(d,c)^{e-1}} \le \sum_{d,c} \frac{1}{h(d,c)^3} < \infty.$$

We conclude from Borel-Cantelli that almost no $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$ belongs to infinitely many sets $A(d,c)$. Thus, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$, there are only finitely many elliptic curves with CM (up to a $\mathbb{C}$-isomorphism) which are defined over $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$. ∎

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

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

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

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

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

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

References

[BoS] Z. I. Borevich and I. R. Shafarevich, *Number Theory,* Academic Press, New York, 1966.

[FoM] E. Fouvry and M. R. Murty, *On the distribution of supersingular primes,* Canadian Journal of Mathematics **48** (1996), 81–104.

[FrJ] M. D. Fried and M. Jarden, *Field Arithmetic, 2nd Edition, revised and enlarged by Moshe Jarden,* Springer, 2005.

[FyJ] G. Frey and M. Jarden, *Approximation theory and the rank of abelian varieties over large algebraic fields,* Proceedings of the London Mathematical Society **28** (1974), 112–128.

[Gol] L. J. Goldstein, *Analytic Number Theory,* Prentice-Hall, Englewood Cliffs, 1971.

[JaJ] M. Jacobson and M. Jarden, *Finiteness theorems for torsion of abelian varieties over large algebraic fields,* Acta Arithmetica **98** (2001), 15–31.

[Jan] G.J. Janusz, *Algebraic Number Fields,* Academic Press, New York, 1973.

[Jar] M. Jarden, *Roots of unity over large algebraic fields,* Mathematische Annalen **213** (1975), 109–127.

[Lan] S. Lang, *Elliptic Functions,* Addison-Wesley, Reading, 1973.

[LaO] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem,* in Algebraic Number Fields, Proceedings of a symposium organised by the London Mathematical Society and held in Durham University 1975, edited by A. Fröhlich, Academic Press 1997, pp. 409–464.

[LeV] W. J. LeVeque, *Topic in Number Theory I,* Addison-Wesley, Reading, 1958.

[Shi] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions,* Iwanami Shoten Publishers and Princeton University Press, 1971.

9 February, 2007