



ANNALES

DE

L'INSTITUT FOURIER

Gerhard FREY & Moshe JARDEN

On the number of elliptic curves with CM cover large algebraic fields

Tome 55, n° 7 (2005), p. 2361-2374.

http://aif.cedram.org/item?id=AIF_2005__55_7_2361_0

© Association des Annales de l'institut Fourier, 2005, tous droits réservés.

L'accès aux articles de la revue « Annales de l'institut Fourier » (<http://aif.cedram.org/>), implique l'accord avec les conditions générales d'utilisation (<http://aif.cedram.org/legal/>). Toute reproduction en tout ou partie cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

*Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
<http://www.cedram.org/>*

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

by Gerhard FREY & Moshe JARDEN (**)

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

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

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

(*) 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.

Keywords: Elliptic curves with CM, large algebraic fields, absolute Galois group, Haar measure, class number.

Math. classification: 12E30.

Likewise, the following holds for Abelian varieties:

THEOREM B ([FyJ]). — *Let A be an abelian variety over \mathbb{Q} . Then for almost all $\sigma \in \text{Gal}(\mathbb{Q})^e$ the rank of $A(\tilde{\mathbb{Q}}(\sigma))$ is infinite.*

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

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

- (a) *If $e = 1$, then $\tilde{\mathbb{Q}}(\sigma)$ contains infinitely many roots of unity.*
- (b) *If $e \geq 2$, then $\tilde{\mathbb{Q}}(\sigma)$ 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 $\sigma \in \text{Gal}(\mathbb{Q})^e$:*

- (a) *If $e = 1$, then $E_{\text{tor}}(\tilde{\mathbb{Q}}(\sigma))$ is infinite.*
- (b) *If $e \geq 2$, then $E_{\text{tor}}(\tilde{\mathbb{Q}}(\sigma))$ 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 $\tilde{\mathbb{Q}}$ such that for almost all $\sigma \in \text{Gal}(K)^e$ infinitely many objects of P are defined over $\tilde{\mathbb{Q}}(\sigma)$ if $e < e_0$ and only finitely many objects of P are defined over $\tilde{\mathbb{Q}}(\sigma)$ 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 $\tilde{\mathbb{Q}}(\sigma)$ such that $\text{End}(E) \subseteq \tilde{\mathbb{Q}}(\sigma)$.*

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

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 $\tilde{\mathbb{Q}}(\sigma)$.*

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

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 $\sum \frac{1}{h(p)^2} = \infty$, 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 $\sigma \in \text{Gal}(\mathbb{Q})^e$ 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 $\sigma \in \text{Gal}(\mathbb{Q})^e$:*

(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 $\tilde{\mathbb{Q}}[\sigma]$.*

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 $\epsilon(p)$ which tends to 0 as $p \rightarrow \infty$ such that $\log h(p) = (1 + \epsilon(p)) \log \sqrt{p}$. It follows that

$$(1) \quad \sum_p \frac{1}{h(p)^2} = \sum_p \frac{1}{p^{1+\epsilon(p)}}.$$

One knows that $\sum_p \frac{1}{p}$ diverges. Unfortunately, without any additional information about $\epsilon(p)$ 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,*

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

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

$$(3) \quad \sum_{\substack{p \leq x \\ p \equiv 3 \pmod{4}}} \frac{h(p)}{p} \sim \frac{c\sqrt{x}}{\log x}.$$

In order to prove (3) suppose $p \equiv 3 \pmod{4}$ 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

$$(4) \quad \sum_{\substack{p \leq x \\ p \equiv 3 \pmod{4}}} \frac{L(1, \chi_p)}{\sqrt{p}} \sim \frac{c\sqrt{x}}{\log x}$$

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 $p \leq x$. 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 $p \equiv a \pmod n$, 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 $L = \mathbb{Q}(\zeta_n)$,

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

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

$$(6) \quad \sum_{\substack{p \leq x \\ p \equiv 3 \pmod 4}} \frac{h(p)}{p} \sim \frac{c\sqrt{x}}{\log x}.$$

Then (2) is true.

Proof. — Apply summation by parts:

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

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

$$c\pi_{3,4}(x) \geq \frac{1}{2} \sum_{\substack{p \leq x \\ p \equiv 3 \pmod 4}} \frac{h(p)}{\sqrt{p}}$$

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

$$\pi_{3,4}(x) \geq \frac{1}{2c} \sum_{\substack{p \leq x \\ p \equiv 3 \pmod 4}} \frac{h(p)}{\sqrt{p}} \geq \frac{1}{2c} \sum_{\substack{p \leq x \\ p \in P'}} \frac{h(p)}{\sqrt{p}} \geq 3\pi(P, x).$$

It follows from $\pi_{3,4}(x) = \pi(P, x) + \pi(P', x)$ that $\pi(P', x) \geq \frac{2}{3}\pi_{3,4}(x) \geq \frac{2}{9}\pi(x)$ for all $x \geq x_0$. It follows from Lemma 1.3 below that

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

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, $p_1 < p_2 < p_3 < \dots$ 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

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

as contended. □

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

Consider a positive integer e and choose σ in $\text{Gal}(\mathbb{Q})^e$ 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 $\tilde{\mathbb{Q}}(\sigma)$. We would also like to know whether there are infinitely many elliptic curves E (up to \mathbb{C} -isomorphism) which are defined over $\tilde{\mathbb{Q}}(\sigma)$ and such that all \mathbb{C} -endomorphisms of E are defined over $\tilde{\mathbb{Q}}(\sigma)$. Since $\tilde{\mathbb{Q}}(\sigma)$ 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 \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 $\text{End}(E) \cong O$. 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 $\text{Gal}(K(j(\mathfrak{a}))/K)$ 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 $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ are representatives of the classes of proper O -ideals, then the values $j(\mathfrak{a}_1), \dots, j(\mathfrak{a}_n)$ 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 $\alpha \in \text{Gal}(K(j(\mathfrak{a}))/K)$.

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). \square

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 $l \equiv 3 \pmod{4}$. 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 $l' \in \Lambda \setminus \Lambda_0$. 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 $-l \equiv 1 \pmod{4}$. 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. \square

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:

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

where

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

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 $\text{End}(E) \subseteq L$.*

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, $E \cong \mathbb{C}/\mathfrak{a}$ 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 $\text{End}(E) \subseteq L$. □

LEMMA 2.5. — *Let D be the set of all squarefree positive integers. Then*

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

Proof. — By (1), it suffices to prove that

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

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

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

Finally, by a theorem of Siegel, $\log h(d) \sim \log d^{\frac{1}{2}}$ [Lan], p. 96. This means that for each $d \in D$ there exists $\epsilon(d) > 0$ such that $h(d) = d^{\epsilon(d)/2}$

and $\epsilon(d) \rightarrow 1$ as $d \rightarrow \infty$. In particular, $\epsilon(d) > \frac{3}{4}$ for all d sufficiently large. Hence, $\frac{3-\epsilon(d)}{2} > \frac{9}{8}$ for almost all d sufficiently large, so there exists $b > 0$ such that

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

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, \dots be finite separable extensions of a field K . For each $i \geq 1$ let \bar{A}_i be a set of left cosets of $\text{Gal}(L_i)^e$ in $\text{Gal}(K)^e$ and*

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

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

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

(b) Suppose L_1, L_2, L_3, \dots 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 $\sigma \in \text{Gal}(\mathbb{Q})^e$:*

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

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

Proof of (a). — Let Λ be the set of all prime numbers $l \equiv 3 \pmod 4$. 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 $\text{End}(E^{(l)}) = O_l$. Hence, if $\sigma \in \text{Gal}(L_l)$, then $E^{(l)}$ is defined over $\tilde{\mathbb{Q}}(\sigma)$ and $\text{End}(E^{(l)}) \subseteq \tilde{\mathbb{Q}}(\sigma)$. By Proposition 1.1,

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

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 $\sigma \in \text{Gal}(\mathbb{Q})^e$ there are infinitely many

primes l such that $E^{(l)}$ is defined over $\tilde{\mathbb{Q}}(\sigma)$ and $\text{End}(E^{(l)}) \subseteq \tilde{\mathbb{Q}}(\sigma)$, as desired.

Proof of (b). — Let $\sigma \in \text{Gal}(\mathbb{Q})^e$. If an elliptic curve E with CM is defined over $\tilde{\mathbb{Q}}(\sigma)$ and $\text{End}(E) \subseteq \tilde{\mathbb{Q}}(\sigma)$, then there exist $d \in D$ and a positive integer c such that $L_{d,c} \subseteq \tilde{\mathbb{Q}}(\sigma)$. 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 $\tilde{\mathbb{Q}}(\sigma)$, then σ 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 $\sum_{d \in D} \sum_{c=1}^{\infty} \frac{1}{[L_{d,c} : \mathbb{Q}]^e} \leq \sum_{d \in D} \sum_{e=1}^{\infty} \frac{1}{h(d,c)^3} < \infty$. Hence, by Borel-Cantelli [Fr.J], Lemma 18.5.3.(a), the measure of those σ 's is 0. \square

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 $\tilde{\mathbb{Q}}(\sigma)$, then the probability that there are infinitely many elliptic curves with CM over $\tilde{\mathbb{Q}}(\sigma)$ 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 $\tilde{\mathbb{Q}}(\sigma)$.*

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

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

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

Indeed, embed L_l in \mathbb{C} and let ρ 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 $l \equiv 3 \pmod{4}$, $h(l)$ 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 $1 = \rho^2 = \alpha^{-1}\rho\alpha\rho = \alpha^{-2}$, 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, τ is conjugate to ρ 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 $A_l = \{\sigma \in \text{Gal}(\tilde{\mathbb{Q}})^e \mid \text{res}_{L_l} \sigma \in \bar{A}_l\}$. 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 $\tilde{\mathbb{Q}}(\sigma)$.

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

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

By Proposition 2.1(b),

$$\mu(A(d, c)) \leq [L_{d,c} : K_d] \left(\frac{1}{[\mathbb{Q}(j(\mathbf{a}_{d,c})) : \mathbb{Q}]} \right)^e = \frac{1}{h(d, c)^{e-1}}.$$

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 σ 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 σ 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), $\mu(S) = 1$.

Consider $\sigma \in S$ and let E be an elliptic curve with CM over $\tilde{\mathbb{Q}}[\sigma]$. Then $j_E \in \tilde{\mathbb{Q}}[\sigma]$. Hence, the Galois closure of $\mathbb{Q}(j_E)/\mathbb{Q}$ is contained in $\tilde{\mathbb{Q}}[\sigma]$. 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 $\tilde{\mathbb{Q}}[\sigma]$). □

BIBLIOGRAPHY

- [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), 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.

Manuscrit reçu le ,
Accepté le .

Moshe JARDEN,
Tel Aviv University
School of Mathematical Sciences
Ramat Aviv
Tel Aviv 69978 (Israël)
jarden@post.tau.ac.il

Gerhard FREY,
Essen University
Institute for Experimental Mathematics
Ellernstrasse 29
45326 Essen (Allemagne)
frey@exp-math.uni-essen.de