C. R. Acad. Sci. Paris, t. 325, Série I, p. 813-818, 1997
Théorie des nombres/*Number Theory*

Elliptic curves with no exceptional primes

William DUKE

Department of Mathematics, Rutgers University,
New Brunswick, NJ 08903 USA.
E-mail : duke@math.rutgers.edu

Abstract. Let E be an elliptic curve over $\mathbf{Q}$. A prime N is said to be *exceptional* for E if the mod N Galois representation of E is not surjective, *i.e.* if the Galois group of the N-th division field of E is not equal to $\mathbf{GL}(2, N)$. We show that, in terms of heights, almost all curves have no exceptional prime.

Courbes elliptiques sur $\mathbf{Q}$ *sans nombres premiers exceptionnels*

Résumé. *Soit E une courbe elliptique sur $\mathbf{Q}$ et soit N un nombre premier. On dit que N est* exceptionnel *pour E si le groupe de Galois des points de N-division de E est distinct de $\mathbf{GL}(2, N)$. Nous montrons que, si l'on range les courbes elliptiques par hauteur croissante, presque toutes les courbes n'ont aucun nombre premier exceptionnel.*

Version française abrégée

Soit E une courbe elliptique sur $\mathbf{Q}$ et soit N un nombre premier. Le groupe $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ opère sur les points de N-division de E, et l'on obtient ainsi un homomorphisme

$$\varphi_N : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, N).$$

Disons que N est *exceptionnel* pour E si φ_N n'est pas surjectif. D'après Serre (*voir* [13]), une courbe sans multiplication complexe n'a qu'un nombre fini de N exceptionnels.

La courbe E a un modèle unique de la forme :

$$y^2 = x^3 + rx + s,$$

avec $r, s \in \mathbf{Z}$, et pgcd (r^3, s^2) non divisible par une 12 ème puissance > 1. La hauteur « naïve » de E est $\mathrm{H}(E) = \max(|r|^3, |s|^2)$. Si $X > 0$, notons $\mathcal{C}(X)$ l'ensemble des E (à isomorphisme près) avec $\mathrm{H}(E) \leq X^6$, et notons $\mathcal{E}(X)$ le sous-ensemble de $\mathcal{C}(X)$ formé des courbes qui ont au moins un nombre premier exceptionnel. Le théorème suivant exprime que « presqu'aucune » courbe n'a de nombre premier exceptionnel :

THÉORÈME 1. – $\lim_{X\to\infty} \frac{|\mathcal{E}(X)|}{|\mathcal{C}(X)|} = 0.$

Note présentée par Jean-Pierre SERRE.

De façon plus précise, on montre que $|\mathcal{E}(X)|/|\mathcal{C}(X)| \ll X^{-1}\log^B X$, où B est une constante absolue. (La démonstration utilise le théorème de Siegel-Walfisz : elle n'est pas « effective ».)

La démonstration dépend d'une variante du théorème de Chebotarev. Soit Δ_E le discriminant minimal de E et soit $a_E(p)$ la trace de Frobenius pour la réduction de E modulo p, $p \nmid \Delta_E$. Pour $d \in \mathbf{Z}/N\mathbf{Z}$, $d \neq 0$, et $t \in \mathbf{Z}/N\mathbf{Z}$, soient

$$\pi_E(X; N, d, t) = |\{p \leq X; p \nmid \Delta_E, p \equiv d \pmod N \quad \text{et} \quad a_E(p) \equiv t \pmod N\}|,$$

et $\pi(X; N, d) = |\{p \leq X; p \equiv d \pmod N\}|$. Posons :

$$\delta = \frac{N + \chi(N)}{N^2 - 1}, \quad \text{où } \chi(N) = \left(\frac{(t^2 - 4d)}{N}\right).$$

THÉORÈME 2. – *Il existe une constante absolue C tel que, pour tout $X \geq 1$, tout nombre premier N et tous d, $t \in \mathbf{Z}/N\mathbf{Z}$, $d \neq 0$, on ait :*

$$\frac{1}{|\mathcal{C}(X)|} \sum_{E \in \mathcal{C}(X)} (\pi_E(X; N, d, t) - \delta\pi(X; N, d))^2 \leq CX.$$

Le théorème 2 se déduit d'une inégalité du grand crible deux-dimensionnel et de résultats classiques de Deuring et Hurwitz. Le théorème 1 est une conséquence du théorème 2 et d'une borne pour le plus grand nombre premier exceptionnel en termes de la hauteur d'une courbe elliptique donnée par Masser et Wüstholz.

Let E be an elliptic curve defined over $\mathbf{Q}$. For a prime N the Galois group $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ acts on the N-torsion points of E giving rise to the mod N representation associated to E:

$$\phi_N : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, N).$$

Say that N is *exceptional* for E if ϕ_N is not surjective. Equivalently, N is exceptional for E if the Galois group G_N of the N-th division field of E, which is the Galois extension of $\mathbf{Q}$ obtained by adjoining to $\mathbf{Q}$ the coordinates of the N-torsion points of E, is isomorphic to a proper subgroup of $\mathbf{GL}(2, N)$. If E has CM then every odd N is exceptional. On the other hand, a fundamental result of Serre (*see* [13]) says that an E without CM has only finitely many exceptional N. Mazur showed in [12] that a semistable E has no exceptional $N \geq 11$ and that, in general, if E has an exceptional $N > 19$ not equal to 37, 43, 67, or 163, then G_N is contained in the normalizer of a Cartan subgroup of $\mathbf{GL}(2, N)$.

In practice, one observes that most E have no exceptional primes and one could try to estimate the density of such curves. However, unless one restricts to semistable curves, it does not appear to be known whether or not there is a bound past which no prime can be exceptional for any non-CM curve. The main point of this paper is to show that it is possible to obtain in general some quantitative information, in spite of this difficulty. It will be shown that almost all elliptic curves have no exceptional primes when the curves are counted by their height.

The curve E has a unique model of the form

$$y^2 = x^3 + rx + s \tag{1}$$

with integral r and s such that $\gcd(r^3, s^2)$ is twelfth-power free. The "naive" height of E will be defined by:

$$\mathrm{H}(E) = \max(|r|^3, |s|^2).$$

It is closely related to the modular height of Faltings (*see* [16]) but it is easier to work with in this setting. Let $\mathcal{C}(X)$ be the set of all (isomorphism classes of) curves E with $\mathrm{H}(E) \leq X^6$. As shown in [2],

$$|\mathcal{C}(X)| = C_1 X^5 + O(X^3) \tag{2}$$

with $C_1 = 4/\zeta(10)$. Let $\mathcal{E}(X)$ be the set of curves in $\mathcal{C}(X)$ with at least one exceptional prime. Our main result is the following.

THEOREM 1.

$$\lim_{X\to\infty} \frac{|\mathcal{E}(X)|}{|\mathcal{C}(X)|} = 0.$$

In fact, we will prove that for some absolute constant B,

$$|\mathcal{E}(X)| \ll X^4 \log^B X$$

but, since the Siegel-Walfisz theorem is used, the implied constant in $\ll$ is non-effective. It is easy to check that the number of CM curves in $\mathcal{E}(X)$ is $2X^3 + O(X^2)$, the main term coming from the curves

$$y^2 = x^3 + s.$$

It may be shown that the number of curves in $\mathcal{E}(X)$ with rational 2-torsion is $C_2 X^3 + O(X^2)$, where C_2 is a certain explicit positive constant. Thus certainly

$$|\mathcal{E}(X)| \gg X^3.$$

It does not seem unreasonable to conjecture that for some $C > 0$, we have

$$|\mathcal{E}(X)| \sim CX^3.$$

The proof of Theorem 1 employs a uniform mean-square estimate of the remainder term in a form of the Chebotarev theorem for the N-th division field of E. Let Δ_E be the minimal discriminant of E and for $p \nmid \Delta_E$, let $a_E(p)$ be the trace of the Frobenius for the reduction of E modulo p. The discriminant of (1) is given by:

$$\Delta_{r,s} = -16(4r^3 + 27s^2).$$

Then $\Delta_{r,s} = e^{12}\Delta_E$ for some $e \mid 6$, and for $p \nmid 3\Delta_{r,s}$, we have $a_E(p) = a_{r,s}(p)$, where

$$a_{r,s}(p) = -\sum_{x \,(\mathrm{mod}\, p)} \left(\frac{x^3 + rx + s}{p}\right).$$

For $d \in \mathbf{Z}/N\mathbf{Z}$ with $d \neq 0$ and $t \in \mathbf{Z}/N\mathbf{Z}$, define

$$\pi_E(X; N, d, t) = |\{p \leq X; p \nmid \Delta_E, p \equiv d \,(\mathrm{mod}\, N) \text{ and } a_E(p) \equiv t \,(\mathrm{mod}\, N)\}|.$$

It is readily verified that

$$|\{g \in \mathbf{GL}(2, N); \det(g) = d \text{ and } \mathrm{tr}(g) = t\}| = N(N + \chi(N)),$$

where

$$\chi(N) = \left(\frac{t^2 - 4d}{N}\right)$$

is the Kronecker symbol. Set

$$\delta = \delta_{N,d,t} = \frac{N + \chi(N)}{N^2 - 1}. \tag{4}$$

As a consequence of the Chebotarov theorem (*see* [1], [3], and [14]), we have that if N is a fixed nonexceptional prime for E, then, as $X \to \infty$,

$$\pi_E(X; N, d, t) \sim \delta\pi(X; N, d),$$

where $\pi(X; N, d) = |\{p \leq X; p \equiv d \pmod N\}|$. We estimate the remainder term in this asymptotic in the mean-square over all curves of $\mathcal{C}(X)$.

THEOREM 2. – *There exists an absolute constant C such that for all $X \geq 1$, N prime, and d, $t \in \mathbf{Z}/N\mathbf{Z}$ with $d \neq 0$, we have*

$$\frac{1}{|\mathcal{C}(X)|} \sum_{E \in \mathcal{C}(X)} (\pi_E(X; N, d, t) - \delta\pi(X; N, d))^2 \leq CX.$$

Proof. – The proof of Theorem 2 relies on a version of the large sieve inequality in two dimensions. Generally, for each prime p, let $\Omega(p) \subset (\mathbf{Z}/p\mathbf{Z})^n$ be an arbitrary set of vector residue classes. For $m \in \mathbf{Z}^n$ define

$$P(X; m) = |\{p \leq X; m \pmod p \in \Omega(p)\}| \tag{5}$$

and

$$P(X) = \sum_{p \leq X} |\Omega(p)| p^{-n}. \tag{6}$$

Let $\mathcal{B}$ be a box in $\mathbb{R}^n$ whose sides are parallel to the coordinate planes which has minimum width $\mathrm{W}(\mathcal{B})$ and volume $\mathrm{V}(\mathcal{B})$. The following is a straightforward extension of Lemma A of [8] using Theorem 1 of [10].

LEMMA 1. – *If $\mathrm{W}(\mathcal{B}) \geq X^2$, then*

$$\sum_{m \in \mathcal{B} \cap \mathbf{Z}^n} (P(X; m) - P(X))^2 \underset{n}{\ll} \mathrm{V}(\mathcal{B}) P(X),$$

where the implied constant depends only on n.

We apply Lemma 1 with $n = 2$ and take $\Omega(p)$ to be empty unless $p > 3$ and $p \equiv d \pmod N$, in which case we define, using (3),

$$\Omega(p) = \{(r, s) \in (\mathbf{Z}/p\mathbf{Z})^2;\ 4r^3 + 27s^2 \neq 0 \quad \text{and} \quad a_{r,s}(p) \equiv t \pmod N\}. \tag{7}$$

The following two Lemmas allow us to estimate $|\Omega(p)|$. Recall the *Hurwitz class number* $\mathrm{H}(n)$, which is defined for any integer n by $\mathrm{H}(n) = 0$ if $n < 0$ or $n \equiv 1, 2 \pmod 4$, $\mathrm{H}(0) = -1/12$, and otherwise $\mathrm{H}(n)$ is the class number of (not necessarily primitive) quadratic forms $ax^2 + bxy + cy^2$ with discriminant $b^2 - 4ac = -n$ except that a form proportional to $x^2 + y^2$ is counted with multiplicity $1/2$ and one proportional to $x^2 + xy + y^2$ with multiplicity $1/3$. We need the following beautiful outcome of the paper [6] of Deuring (*see* [4]).

LEMMA 2. – *For $p > 3$ and $a \in \mathbf{Z}$, we have that*

$$|\{(r, s) \in (\mathbf{Z}/p\mathbf{Z})^2;\ 4r^3 + 27s^2 \neq 0 \quad \textit{and} \quad a_{r,s}(p) = a\}| = \frac{1}{2}(p-1)\mathrm{H}(4p - a^2).$$

The next Lemma is a consequence of an 1885 paper of Hurwitz, [9], taken together with the Ramanujan bound for the Hecke eigenvalues of weight 2 cusp form (*see* [7]). Today it is a standard application of the trace formula for Hecke operators for subgroups of $\Gamma(N)$.

LEMMA 3. – *For* $p \equiv d \pmod N$ *and* δ *defined in* (3),

$$\sum_{a \equiv t \pmod N} \mathrm{H}(4p - a^2) = 2\delta p + O(N p^{1/2})$$

with an absolute constant.

Proof of Theorem 2. – For $p > 3$ and $p \equiv d \pmod N$ we have $|\Omega(p)| = \delta p^2 + O(N p^{3/2})$ by (7), Lemma 2, and Lemma 3, so it follows from (6) that

$$P(X) = \delta \pi(X; N, d) + O(X^{1/2}). \tag{8}$$

From (1) and (5) with $E \in \mathcal{C}(X)$, we have that

$$P(X; (r, s)) = \pi_E(X; N, d, t) + O(\log X). \tag{9}$$

Taking

$$\mathcal{B} = \{(r, s) \in \mathbf{R}^2; |r| \leq X^2, |s| \leq X^3\},$$

for which $\mathrm{V}(\mathcal{B}) = 4X^5$ and $\mathrm{W}(\mathcal{B}) = 2X^2$, we get Theorem 2 from Lemma 1 using (8), (9), and (2).

Proof of Theorem 1. – Let $\mathcal{E}_N(X)$ denote the set of $E \in \mathcal{C}(X)$ for which N is exceptional. Our proof of Theorem 1 requires that we estimate individually $|\mathcal{E}_2(X)|$ and $|\mathcal{E}_3(X)|$. Well-known conditions on the discriminant in these cases (*see* p. 304 of [13]) and standard lattice point counting arguments lead to the asymptotic formula

$$|\mathcal{E}_2(X)| = C_2 X^3 + O(X^2 \log^5 X)$$

and to the inequality

$$|\mathcal{E}_3(X)| \ll X^3 \log^5 X.$$

Here $C_2 = (4\varepsilon_+^{-1} + 4\varepsilon_- + 6\log(\varepsilon_+ \varepsilon_-))/(3\zeta(6)) = 3.93471\ldots$ with ε_+ and ε_- being the fundamental units for the cubic fields defined by $x^3 \pm x - 1$.

For $N > 3$ we apply Theorem 2 to estimate $|\mathcal{E}_N(X)|$. To do this we employ the following Lemma (*see* Corollaire on p. 284 of [13] or Lemma 4 of [15]).

LEMMA 4. – *Suppose that* $N > 3$ *is prime and that* $G \subset \mathbf{GL}(2, N)$ *is a subgroup. If for each* d, $t \in \mathbf{Z}/N\mathbf{Z}$, $d \neq 0$, *there is a* $g \in G$ *with* $\mathrm{tr}(g) = t$ *and* $\det(g) = d$, *then* $G = \mathbf{GL}(2, N)$.

This result allows us to use Theorem 2 to pick out curves for which a given $N > 3$ is exceptional.

LEMMA 5. – *For* $N > 3$ *we have*

$$|\mathcal{E}_N(X)| \ll X^6 \pi(X; N, d)^{-2},$$

with an absolute implied constant.

Proof. – By Lemma 4, if $G_N \neq \mathbf{GL}(2, N)$ for E, then for some d, $t \in \mathbf{Z}/N\mathbf{Z}$, $d \neq 0$, we must have $\pi_E(X; N, d, t) = 0$ for all $X > 0$. By Theorem 2 we conclude that

$$|\mathcal{E}_N(X)| \ll X|\mathcal{C}(X)|\pi(X; N, d)^{-2},$$

and the lemma follows from (2).

To prove Theorem 1 we apply the explicit bound for the largest possible exceptional N given by Masser and Wüstholz in [11]:

$$N \ll \log^A \mathrm{H}(E)$$

with abolute constants. Thus if $E \in \mathcal{E}_N(X)$, then $N \ll \log^A X$. In this range, by the Siegel-Walfisz theorem (*see* p. 133 of [5]), we have that

$$\pi(X; N, d) \gg N^{-1} \pi(X)$$

with, since Siegel's theorem is used, a non-effective constant. Thus from Lemmas 4, 5, and 7 we conclude that for some absolute $B > 0$,

$$|\mathcal{E}(X)| \ll X^4 \log^B X,$$

but where the implied constant is non-effective. Theorem 1 follows.

Acknowledgements. I thank C. David for stimulating discussions and J.-P. Serre for helpful comments on an earlier version of this paper.

Note remise et acceptée le 5 septembre 1997.

References

[1] **Artin E., 1923.** Über eine neue Art von L-Reithen, *Hamb. Abh.*, 89-108, Collected Papers, pp. 105-124.
[2] **Brumer A., 1992.** The average rank of elliptic curves I, *Invent. Math.*, 109, pp. 445-472.
[3] **Tshebotareff N., 1926.** Die Bestimmungder Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen substitutionsklasse gehören, *Math. Ann.*, 95, pp. 191-228.
[4] **Cox D. A., 1989.** *Primes of the form* $x^2 + ny^2$, Wiley.
[5] **Davenport H., 1980.** *Multiplicative Number Theory*, 2nd ed., Springer.
[6] **Deuring M., 1941.** Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, *Hamb. Abh.*, pp. 197-272.
[7] **Eichler M., 1954.** Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruentzzeta Funktion, *Arch. der Math.*, 5, pp. 355-366.
[8] **Gallagher P. X., 1972.** The large sieve and probabilistic Galois theory, in *Analytic number theory*, Proc. Symp. Pure Math., Vol. XXIV, pp. 91-101.
[9] **Hurwitz A., 1885.** Über die Klassenzahlrelationen und Modularkorrespondenzen primzahliger Stufe, in *Werke Bd.*, II, pp. 51-67.
[10] **Huxley M., 1968.** The large sieve inequality for algebraic number fields, *Mathematika*, 15, pp. 178-187.
[11] **Masser D. W. and Wüstholz G., 1993.** Galois properties of division fields of elliptic curves, *Bull. London Math. Soc.*, 25, No. 3, pp. 247-254.
[12] **Mazur B., 1978.** Rational isogenies of prime degree, *Invent. Math.*, 44, pp. 129-162.
[13] **Serre J.-P., 1972.** Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.*, 15, pp. 123-201 (= Collected Papers III, pp. 1-73).
[14] **Serre J.-P., 1981.** Quelques applications du théorème de densité de Chebotarev, *Pub. IHES*, 54, pp. 123-201 (= Collected Papers III, pp. 563-641).
[15] **Shimura G., 1966.** A reciprocity law in non-solvable extensions, *J. Crelle*, 221, pp. 209-220.
[16] **Silverman J., 1986.** Heights and elliptic curves, in: **Cornell G. and Silverman Eds.**, *Arithmetic Geometry*, Springer, pp. 253-265.