Available online at www.sciencedirect.com
SCIENCE DIRECT
C. R. Acad. Sci. Paris, Ser. I 337 (2003) 689–692
COMPTES RENDUS MATHEMATIQUE

Number Theory/Algebraic Geometry

Almost all reductions modulo p of an elliptic curve have a large exponent

William Duke [1]

UCLA Mathematics Department, Box 951555, Los Angeles, CA 90095-1555, USA

Received 20 June 2003; accepted 7 October 2003

Presented by Jean-Pierre Serre

Abstract

Let E be an elliptic curve defined over $\mathbb{Q}$. Suppose that $f(x)$ is any positive function tending to infinity with x. It is shown (under GRH) that for almost all p, the group of $\mathbb{F}_p$-points of the reduction of E mod p contains a cyclic group of order at least $p/f(p)$. ***To cite this article: W. Duke, C. R. Acad. Sci. Paris, Ser. I 337 (2003).***

Résumé

Presque toutes les réductions mod p d'une courbe elliptique sur $\mathbb{Q}$ ont un groupe de points qui est presque cyclique. Soit E une courbe elliptique sur $\mathbb{Q}$. Soit $f(x)$ une fonction réelle positive tendant vers l'infini. Nous montrons (sous GRH) que, pour presque tout p, le groupe des $\mathbb{F}_p$-points de la réduction de E mod p contient un groupe cyclique d'ordre au moins $p/f(p)$. ***Pour citer cet article : W. Duke, C. R. Acad. Sci. Paris, Ser. I 337 (2003).***

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$. For a prime p of good reduction for E the reduction of E modulo p is an elliptic curve E_p defined over the finite field $\mathbb{F}_p$ with p elements. The finite abelian group $E_p(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points of E_p has size

$$\#E_p(\mathbb{F}_p) = p + 1 - a_p, \tag{1}$$

where $|a_p| < 2\sqrt{p}$, and structure

$$E_p(\mathbb{F}_p) \simeq (\mathbb{Z}/d_p\mathbb{Z}) \oplus (\mathbb{Z}/e_p\mathbb{Z}), \tag{2}$$

for uniquely determined positive integers d_p, e_p with $d_p|e_p$. Here e_p is the size of the maximal cyclic subgroup of $E_p(\mathbb{F}_p)$, called the exponent of E_p.

E-mail address: duke@math.ucla.edu (W. Duke).
[1] Research partially supported by the NSF.

1631-073X/$ – see front matter
doi:10.1016/j.crma.2003.10.006

Schoof [3] initiated the study of e_p as a function of p. It is immediate from (1) and (2) that $\sqrt{p} \ll e_p \ll p$. If E has no complex multiplication (CM) he showed by an elegant argument that

$$e_p \gg \frac{\log p}{\log\log p}\sqrt{p}.$$

He also observed that this is likely to be false if E has CM. For example, for a prime of the form $p = (4n)^2 + 1$ the CM curve E given by $y^2 = x^3 - x$ has $e_p = d_p = 4n = \sqrt{p-1}$. It is conjectured that there are infinitely many such p, but of course these anomalous primes may only occur rarely.

In this Note I will show that e_p is much larger for *almost all* p. Recall that a statement holds for almost all primes if the number of exceptional primes $p \leqslant x$ for which it does not hold is $o(\pi(x))$ as $x \to \infty$. As usual, $\pi(x)$ is the number of all primes $\leqslant x$. To obtain the optimal result in the non-CM case we assume the generalized Riemann hypothesis (GRH) for Dedekind zeta functions.

Theorem 1.1. *Let E be an elliptic curve defined over $\mathbb{Q}$. If E does not have CM assume GRH. Let $f(x)$ be any positive function on $[2,\infty)$ that tends to infinity with x. Then the exponent e_p of E_p satisfies $e_p > p/f(p)$ for almost all p.*

This result is optimal in the sense that it is not true for bounded f (see the statement below (10)). Unconditionally we are able to show that

$$e_p > p^{3/4}/\log p \tag{3}$$

for almost all p (see the discussion above (9)).

For the proof of Theorem 1.1 we exploit the obvious fact that for any sequence of positive integers d_p the number of primes $p \leqslant x$ with $d_p > y$ is bounded from above by $\sum_{n>y} \pi_n(x)$, where

$$\pi_n(x) = \#\{p \leqslant x\colon\ d_p \equiv 0 \pmod{n}\}. \tag{4}$$

For d_p defined in (2), the function $\pi_n(x)$ counts split primes in the n-th division field of E and we are reduced to estimating the number of such primes from above in various ranges of n. For large enough n this is done using known properties of the Frobenius automorphism for a division field. For CM curves we also handle small n unconditionally using the Brun–Titchmarsh theorem in the associated quadratic field. To treat small n for non-CM curves we apply a strong version of the Chebotarev theorem that is conditional on GRH.

2. Reduction

From now on assume that p denotes a prime >3 of good reduction for a fixed elliptic curve E defined over $\mathbb{Q}$. In order to prove Theorem 1.1 it is sufficient to show that as $x \to \infty$ we have $\#\{p \leqslant x\colon\ d_p > f(p)/3\} = \mathrm{o}(\pi(x))$, where d_p is defined in (2). For this it is enough to prove that as $x \to \infty$

$$\#\{x/\log x \leqslant p \leqslant x\colon\ d_p > g(x)\} = \mathrm{o}(x/\log x),$$

where $g(x) = \frac{1}{3}\inf\{f(y)\colon\ x/\log x \leqslant y \leqslant x\}$. Clearly $g(x) \to \infty$ as $x \to \infty$. Set for $x \geqslant 3$

$$S(x) = \sum_{g(x) < n \leqslant 2\sqrt{x}} \pi_n(x), \tag{5}$$

where $\pi_n(x)$ is defined in (4). Obviously $\#\{x/\log x \leqslant p \leqslant x\colon\ d_p > g(x)\} \leqslant S(x)$ and so it is sufficient to prove that $S(x) = \mathrm{o}(x/\log x)$ as $x \to \infty$.

Let $E[n]$ denote the group of n-division points of E and $L_n := \mathbb{Q}(E[n])$ be the n-th division field of E. Then $L_n/\mathbb{Q}$ is a finite Galois extension whose Galois group G_n is a subgroup of $\mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. It is clear that p splits completely in L_n exactly when $d_p \equiv 0 \pmod n$. The ring of endomorphisms $\mathrm{End}_{\mathbb{F}_p}(E_p)$ of E_p over $\mathbb{F}_p$ is an order in the imaginary quadratic field $\mathbb{Q}((a_p^2 - 4p)^{1/2})$ of discriminant Δ_p. Define $b_p \in \mathbb{Z}^+$ by

$$4p = a_p^2 - \Delta_p b_p^2 \tag{6}$$

and consider the (integral) matrix

$$\sigma_p = \begin{pmatrix} (a_p + b_p\delta_p)/2 & b_p \\ b_p(\Delta_p - \delta_p)/4 & (a_p - b_p\delta_p)/2 \end{pmatrix}, \tag{7}$$

where δ_p is 0 or 1 according to whether $\Delta_p \equiv 0$ or $1 \pmod 4$. Then, as shown in [1], for an integer n such that $p \nmid n$, the matrix σ_p reduced modulo n represents the class of the Frobenius over p for L_n. In particular, if p splits in L_n then $b_p \equiv 0 \pmod n$ and $a_p \equiv 2 \pmod n$. We then have immediately from (6) that for $n \leqslant 2\sqrt{x}$

$$\pi_n(x) \ll x^{3/2} n^{-3}. \tag{8}$$

In fact, this estimate may be improved a little by applying the Brun–Titchmarsh theorem, but we will not need this improvement here.

Let $h(x) = \frac{1}{4}(x \log^3 x)^{1/4}$. Summing (8) over the range $h(x) \leqslant n \leqslant 2\sqrt{x}$ shows that, with the possible exception of at most $\mathrm{O}(x \log^{-3/2} x)$ values of p, the set $E_p(\mathbb{F}_p)$ contains points of order at least $p^{3/4}/\log p$, thus justifying the second statement after Theorem 1.1 above.[2] Toward the proof of Theorem 1.1, we also derive for $S(x)$ from (5) that

$$S(x) = \sum_{g(x) < n < h(x)} \pi_n(x) + \mathrm{O}\big(x \log^{-3/2} x\big). \tag{9}$$

This leads us to the problem of estimating $\pi_n(x)$ for smaller values of n, where we must distinguish between the CM and non-CM cases.

3. CM

We now complete the proof of Theorem 1.1 in the CM case.

Suppose that E has CM by an order $\mathcal{O}$ of discriminant $\Delta = m^2\Delta_K$ in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{\Delta_K})$ of discriminant Δ_K. If p is supersingular, so $a_p = 0$, then either $d_p = 1$ or $d_p = 2$. Otherwise we have that $\Delta_p = \Delta$ and from (6)

$$4p = a_p^2 - \Delta b_p^2 = a_p^2 - \Delta_K (m b_p)^2.$$

It follows easily from (7) and the discussion following it (or from the classical theory of complex multiplication) that for $n > 2$

$$\pi_n(x) \leqslant \#\{p \leqslant x\colon\ p = N(\rho) \text{ for some } \rho \in \mathcal{O}_K \text{ with } \rho \equiv 1 \pmod n\}.$$

The Brun–Titchmarsh theorem is readily generalized to the *fixed* number field K and its ray class group mod n, which has size

$$\#(\mathcal{O}_K/n\mathcal{O}_K)^\times = n^2 \prod_{p|n} \big(1 - p^{-1}\big)\big(1 - \chi_K(p)p^{-1}\big) \geqslant \phi(n)^2,$$

[2] After seeing a previous version of this Note, I. Shparlinski pointed out to me that an immediate extension of the proof of (8) yields the estimate $\#\{p \leqslant x\colon$ there exists a curve over $\mathbb{F}_p$ with $d_p \equiv 0 \pmod n\} \ll x^{3/2} n^{-3}$. This shows that, for almost all p, the group of $\mathbb{F}_p$-points of *every* elliptic curve defined over $\mathbb{F}_p$ contains points of order at least $p^{3/4}/\log p$.

where χ_K is the quadratic character of K and ϕ is the Euler function. This is carried out in [2] and gives, in particular when $n < h(x) = \frac{1}{4}(x\log^3 x)^{1/4}$, that

$$\pi_n(x) \ll \frac{x}{\phi(n)^2 \log x}.$$

This finishes the proof of Theorem 1.1 in the CM case since, according to (9),

$$\sum_{g(x)<n<h(x)} \pi_n(x) \ll g(x)^{-1+\varepsilon}(x/\log x) = \mathrm{o}(x/\log x)$$

for any $\varepsilon > 0$, as $x \to \infty$.

4. Non-CM

In the non-CM case we must at this point apply the (conditional) Chebotarev theorem in order to bound $\pi_n(x)$ in the range $g(x) < n < h(x)$. The ordinary Chebotarev theorem applied to the Galois extension $L_n/\mathbb{Q}$ implies that

$$\pi_n(x) \sim \frac{1}{|G_n|}\pi(x) \tag{10}$$

as $x \to \infty$. This is certainly enough to conclude that for any fixed $n \in \mathbb{Z}^+$ we have $e_p \leqslant (2/n)p$ for a positive proportion of p, justifying the first statement after Theorem 1.1 above.

To obtain a strong uniform estimate we assume GRH for the Dedekind zeta functions for L_n. Assuming this, we have the following useful conditional version (see (20_R) p. 134 of [5]):

$$\pi_n(x) = \frac{1}{|G_n|}\pi(x) + \mathrm{O}\big(x^{1/2}\log(xnN)\big),$$

where the implied constant is absolute and N is the conductor of E. It follows that to finish the proof of Theorem 1.1 it is sufficient to show that

$$\sum_{g(x)<n<h(x)} |G_n|^{-1} = \mathrm{o}(1)$$

as $x \to \infty$. This is deduced immediately from Serre's result [4] that in the non-CM case the index of G_n in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is bounded in n and the well known formula

$$\#\,\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) = n^4 \prod_{\substack{\ell|n \\ \ell \text{ prime}}} \big(1-\ell^{-1}\big)\big(1-\ell^{-2}\big).$$

Acknowledgements

I thank Igor Shparlinski for his inquiry leading me to write this Note. I also thank J.-P. Serre for suggesting several improvements of an earlier version.

References

[1] W. Duke, Á Tóth, The splitting of primes in division fields of elliptic curves, Experiment. Math. 11 (2003) 555–565.
[2] J. Hinz, M. Lodemann, On Siegel zeros of Hecke–Landau zeta-functions, Monatsh. Math. 118 (1994) 231–248.
[3] R. Schoof, The exponents of the groups of points on the reductions of an elliptic curve, in: Arithmetic Algebraic Geometry (Texel, 1989), in: Progr. Math., Vol. 89, Birkhäuser, Boston, MA, 1991, pp. 325–335.
[4] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (1972) 259–331, also in: Collected Papers, Vol. III, Springer-Verlag, 1985.
[5] J.-P. Serre, Quelques applications du théorème de densité de Chebotarev, Publ. Math. I. H. E. S. 54 (1981) 123–201, also in: Collected Papers, Vol. III, Springer-Verlag, 1985.