REVISTA DE LA
UNIÓN MATEMÁTICA ARGENTINA
Volumen 50, Número 1, 2009, Páginas 69–74

# EXPONENTS OF MODULAR REDUCTIONS OF FAMILIES OF ELLIPTIC CURVES

IGOR E. SHPARLINSKI

Abstract. For some natural families of elliptic curves we show that "on average" the exponent of the point group of their reductions modulo a prime $p$ grows as $p^{1+o(1)}$.

## 1. Introduction

For integers $a$ and $b$ such that $4a^3 + 27b^2 \neq 0$, we denote by $\mathbf{E}_{a,b}$ the elliptic curve defined by the *affine Weierstraß equation*:

$$\mathbf{E}_{a,b} \ : \ Y^2 = X^3 + aX + b.$$

For a basic background on elliptic curves, we refer to [11].

For a prime $p > 3$, we denote by $\mathbb{F}_p$ the finite field of $p$ elements, which we identify with the set of integers $\{0, \pm 1, \ldots, \pm(p-1)/2\}$.

When $p \nmid 4a^3 + 27b^2$, the set $\mathbf{E}_{a,b}(\mathbb{F}_p)$, consisting of the $\mathbb{F}_p$-rational points of $\mathbf{E}_{a,b}$ together with a point at infinity $\mathcal{O}$, forms an *abelian group* under an appropriate composition rule called *addition*, and the number of elements in the group $\mathbf{E}_{a,b}(\mathbb{F}_p)$ satisfies the *Hasse bound*:

$$|\#\mathbf{E}_{a,b}(\mathbb{F}_p) - p - 1| \leqslant 2\sqrt{p} \tag{1}$$

(see, for example, [11, Chapter V, Theorem 1.1]).

It is well-known that $\mathbf{E}_{a,b}(\mathbb{F}_p)$ is of rank at most two, that is, $\mathbf{E}_{a,b}(\mathbb{F}_p)$ is isomorphic to

$$\mathbf{E}_{a,b}(\mathbb{F}_p) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \tag{2}$$

for unique integers $m$ and $n$ with $m \mid n$ and $\#\mathbf{E}_{a,b}(\mathbb{F}_p) = mn$. The number $n$ is called the *exponent* of $\mathbf{E}_{a,b}(\mathbb{F}_p)$ which we denote by $\ell_{a,b}(p)$. In other words, $\ell_{a,b}(p)$ is the smallest positive $\ell$ such that $\ell P = \mathcal{O}$ for all points $P \in \mathbf{E}_{a,b}(\mathbb{F}_p)$.

We also put $\ell_{a,b}(p) = 0$ if $p \mid 4a^3 + 27b^2$.

Thus we see that (1) and (2) imply the following trivial bound

$$\ell_{a,b}(p) \geqslant (\mathbf{E}_{a,b}(\mathbb{F}_p))^{1/2} \geqslant p^{1/2} - 1. \tag{3}$$

The exponent of elliptic curves has been studied in a number of works, see [4, 7, 8, 9, 10], with a variety of results, each of them indicating that in a "typical case"

2000 *Mathematics Subject Classification.* 11B57, 11G07, 14H52.
*Key words and phrases.* elliptic curves, group exponent, Farey fractions.

the exponent tends to be substantially larger than the bound (3) (and its analogue for curves over arbitrary finite fields) guarantees.

W. Duke [4], among other results, has proved that, assuming the Generalised Riemann Hypothesis, for every fixed integer $a$ and $b$ with $4a^3 + 27b^2 \neq 0$, and arbitrary small $\varepsilon > 0$, the bound

$$\ell_{a,b}(p) \geqslant p^{1-\varepsilon} \tag{4}$$

holds for all but $o(T/\log T)$ of primes $p \leqslant T$.

It is also shown in [10] that (4) holds for all but $o(p^2)$ pairs $(a,b) \in \mathbb{F}_p \times \mathbb{F}_p$.

Here we use a combination of the results and ideas of [1, 10] to prove unconditionally that (4) is satisfied for almost all pairs $(a,b)$ with $|a| \leqslant A$, $|b| \leqslant B$ for $A$ and $B$ relatively small compared to $p$.

**Theorem 1.** *For any fixed $\varepsilon > 0$ and all integers $A$, $B$ satisfying the inequalities*

$$AB^{1/2} \geqslant p^{1+\varepsilon} \qquad \text{and} \qquad B \geqslant p^{1/4+\varepsilon}$$

*or*

$$A^{1/2}B \geqslant p^{1+\varepsilon} \qquad \text{and} \qquad A \geqslant p^{1/4+\varepsilon}$$

*the bound*

$$\ell_{a,b}(p) \geqslant p^{1-\varepsilon}$$

*holds for all but $o(AB)$ pairs $(a,b)$ with $|a| \leqslant A$, $|b| \leqslant B$*

In particular, Theorem 1 is nontrivial if

$$\max\{A,B\} \geqslant p^{7/8+\varepsilon} \qquad \text{and} \qquad \min\{A,B\} \geqslant p^{1/4+\varepsilon}$$

or

$$AB \geqslant p^{4/3+\varepsilon}.$$

We also show that averaging over $p$ gives some additional saving.

**Theorem 2.** *For any fixed $\varepsilon > 0$ and all integers $A$, $B$ and $T$ satisfying the inequalities*

$$T^{\varepsilon} \leqslant A, B \leqslant T^{1-\varepsilon} \qquad \text{and} \qquad AB \geqslant T^{1+\varepsilon}\sqrt{\min\{A,B\}}\,.$$

*the bound (4) holds for all but $o(ABT/\log T)$ triples $(a,b,p)$ with $|a| \leqslant A$, $|b| \leqslant B$, $p \leqslant T$.*

We note that the condition $A, B \leqslant T^{1-\varepsilon}$ from [1], where it is used to simplify the error term, is not neccessary. One can easily extend Theorem 2 for $A$ and $B$ beyond this range, however since (as in [1]) small values of $A$ and $B$ are of main interest we have not done this.

We remark that in [5] some of the results of [4] have been extended to hyperelliptic curves. It would also be interesting to obtain analogues of our result for natural families of hyperelliptic curves.

We also consider the set of Farey fractions

$$\mathcal{F}(W) = \{u/v \ : \ \gcd(u,v) = 1, \ 1 \leqslant u, v \leqslant W\}.$$

In particular

$$\#\mathcal{F}(W) = \left(\frac{6}{\pi^2} + o(1)\right) W^2.$$

For $t = u/v$ with $\gcd(v, p) = 1$ and two polynomial $A(X), B(X) \in \mathbb{Z}[X]$, the reduction $\mathbf{E}_{A(t),B(t)}(\mathbb{F}_p)$ is correctly defined. Various questions concerning the behaviour of the curves $\mathbf{E}_{A(t),B(t)}(\mathbb{F}_p)$ on average over $p \leqslant T$ and $t \in \mathcal{F}(W)$ have been studied in [2]. Here we continue to study this family of curves. Certainly the most interesting case is when $W$ is small compared to $T$.

**Theorem 3.** *Assume that the discriminant*

$$\Delta_{A,B}(t) = -16(4A(t)^3 + 27B(t)^2)$$

*is nonzero and the $j$-invariant*

$$j_{A,B}(t) = -\frac{6912A(t)^3}{4A(t)^3 + 27B(t)^2}$$

*is nonconstant. Then for any fixed $\varepsilon > 0$ and all integers $W$ and $T$ with*

$$W \geqslant T^{1/2+\varepsilon}$$

*the bound*

$$\ell_{A(t),B(t)}(p) \geqslant p^{1-\varepsilon}$$

*holds for all but $o(WT/\log T)$ pairs $(t, p)$ with $t \in \mathcal{F}(W)$, $p \leqslant T$.*

## 2. Preparations

The following result follows immediately from the more precise statement of [10, Theorem 3.1].

**Lemma 4.** *For any $\varepsilon > 0$, the number of triples $(a, b) \in \mathbb{F}_p \times \mathbb{F}_p$ with*

$$\ell_{a,b}(p) < p^{1-\varepsilon}$$

*is at most $o\left(p^2\right)$.*

Let $d_p = \gcd(p - 1, 6)$ and put

$$\sigma_p(H) = \max_{\substack{\chi^{d_p}=\chi_0 \\ \chi\neq\chi_0}} \left\{1, \left|\sum_{n=1}^{H} \chi(n)\right|\right\},$$

where the maximum is taken over all non-principal multiplicative characters $\chi$ modulo $p$ such that $\chi^{d_p}$ is the principal character $\chi_0$.

Similarly, we define $e_p = \gcd(p - 1, 4)$ and put

$$\rho_p(H) = \max_{\substack{\chi^{e_p}=\chi_0 \\ \chi\neq\chi_0}} \left\{1, \left|\sum_{n=1}^{H} \chi(n)\right|\right\},$$

where the maximum is taken over all non-principal multiplicative characters $\chi$ modulo $p$ such that $\chi^{e_p}$ is the principal character $\chi_0$. For an arbitrary subset

$\mathcal{S} \subseteq \mathbb{F}_p \times \mathbb{F}_p$, we denote by $N_p(\mathcal{S}, A, B)$ the number of pairs such that $(a,b) \in \mathcal{S}$ with $|a| \leqslant A$ and $|b| \leqslant B$. We also denote

$$\mathcal{E}(A, B; p) = \min \left\{ A\,\sigma_p(B) + B^{1/2}p,\ B\,\rho_p(A) + A^{1/2}p \right\}.$$

The following estimate is given in [1].

**Lemma 5.** *For all primes $p > 3$, integers $1 \leqslant A, B \leqslant (p-1)/2$, and subsets $\mathcal{S} \subseteq \mathbb{F}_p \times \mathbb{F}_p$ such that whenever $(r,s) \in \mathcal{S}$ the isomorphism $\mathbf{E}_{a,b}(\mathbb{F}_p) \cong \mathbf{E}_{r,s}(\mathbb{F}_p)$ implies $(a,b) \in \mathcal{S}$, the following bound holds:*

$$\left| N_p(\mathcal{S}, A, B) - \frac{4AB}{p^2} \# \mathcal{S} \right| \ll \mathcal{E}(A, B; p).$$

Moreover, it is shown in [1] that $\mathcal{E}(A, B; p)$ is small "on average" over $p$.

**Lemma 6.** *The following bound holds:*

$$\sum_{p \leqslant T} \mathcal{E}(A, B; p) \ll ABT^{1/2+o(1)} + AB^{7/8}T + B^{1/2}T^2$$

For a prime $p$ and an integer $t$ with $1 \leqslant t < p$ we denote by $R_{T,p}(t)$ the number of fractions $u/v \in \mathcal{F}(T)$ with $\gcd(v,p) = 1$ and $u/v \equiv t \pmod p$.

It is shown in [3] that $R_{T,p}(t)$ is close to its expected value $\#\mathcal{F}(T)/p$ on average over $t = 1, \ldots, p-1$. More precisely, we have:

**Lemma 7.** *We have,*

$$\sum_{t=0}^{p-1} \left| R_{W,p}(t) - \frac{6}{\pi^2} \cdot \frac{W^2}{p} \right| = O\left( W^2 p^{-1} + W p^{1/2+o(1)} \right).$$

## 3. Proof of Theorem 1

Let $\mathcal{S}_p(\varepsilon)$ be the set of pairs $(a,b) \in \mathbb{F}_p \times \mathbb{F}_p$ for which $\ell_{a,b}(p) \leqslant p^{1-\varepsilon}$. Then it is enough to show that

$$N_p\left(\mathcal{S}_p(\varepsilon), A, B\right) = o(AB).$$

Since by Lemma 4 we have $\#\mathcal{S}_p(\varepsilon) = o(p^2)$, invoking Lemma 5 we see that it is enough to check that $\mathcal{E}(A, B; p) = o(AB)$.

Assume that $B \geqslant p^{1/4+\varepsilon}$ then by the Burgess bound, see [6, Theorems 12.5 and 12.6], we have $\sigma_p(B) = o(B)$. Also, if $AB^{1/2} \geqslant p^{1+\varepsilon}$ then have $B^{1/2}p = o(AB)$.

Similarly, if $A \geqslant p^{1/4+\varepsilon}$ then $\rho_p(B) = o(B)$, and if $A^{1/2}B \geqslant p^{1+\varepsilon}$ then have $A^{1/2}p = o(AB)$.

## 4. Proof of Theorem 2

As before, let $\mathcal{S}_p(\varepsilon)$ be the set of pairs $(a,b) \in \mathbb{F}_p \times \mathbb{F}_p$ for which $\ell_{a,b}(p) \leqslant p^{1-\varepsilon}$. Then it is enough to show that

$$\sum_{p \leqslant T} N_p\left(\mathcal{S}_p(\varepsilon), A, B\right) = o(ABT/\log T). \tag{5}$$

Let us assume that $A \geqslant B$ since the case $A < B$ is similar.

Using the trivial bound $N_p(\mathcal{S}_p(\varepsilon), A, B) \leqslant AB$ for primes $p \leqslant 2A+1$, we deduce

$$\sum_{p\leqslant T} N_p\left(\mathcal{S}_p(\varepsilon), A, B\right) = \sum_{2A+1<p\leqslant T} N_p(\mathcal{S}_p(\varepsilon), A, B) + O(A^2B). \tag{6}$$

Noticing that for $p > 2A+1$ the set $\mathcal{S}_p(\varepsilon)$ satisfies the conditions of Lemma 5, we obtain

$$\begin{aligned}\sum_{2A+1<p\leqslant x} & N_p(\mathcal{S}_p(\varepsilon), A, B) \\ &= 4AB \sum_{2A+1<p\leqslant T} \frac{\#\mathcal{S}_p(\varepsilon)}{p^2} + O\left(\sum_{2A+1<p\leqslant T} \mathcal{E}(A, B; p)\right).\end{aligned} \tag{7}$$

By Lemma 4 we have

$$\sum_{2A+1<p\leqslant T} \frac{\#\mathcal{S}_p(\varepsilon)}{p^2} = o(T/\log T). \tag{8}$$

Substituting (7) and (8) in (6), we obtain

$$\begin{aligned}\sum_{p\leqslant T} & N_p\left(\mathcal{S}_p(\varepsilon), A, B\right) \\ &= o(ABT/\log T) + O\left(\sum_{2A+1<p\leqslant T} \mathcal{E}(A, B; p) + A^2B\right).\end{aligned}$$

We now easily verify that under the conditions of the theorem, Lemma 6 implies the desired bound (5).

## 5. Proof of Theorem 3

As before, we use $\mathcal{S}_p(\varepsilon)$ to denote the set of pairs $(a, b) \in \mathbb{F}_p \times \mathbb{F}_p$ for which $\ell_{a,b}(p) \leqslant p^{1-\varepsilon}$.

Let $\mathcal{T}_{A,B,p}(\varepsilon)$ be the set of $t \in \mathbb{F}_p$ such that

$$\left(A(t)\lambda^4, B(t)\lambda^6\right) \in \mathcal{S}_p(\varepsilon).$$

for some $\lambda \in \mathbb{F}_p^*$.

Obviously, for any $t \in \mathbb{F}_p$ and $\lambda \in \mathbb{F}_p^*$ we have

$$\ell_{A(t),B(t)}(p) = \ell_{A(t)\lambda^4,B(t)\lambda^6}(p)$$

(since the corresponding curves are isomorphic, see [11, Section III.1]).

We also note that the system of equations

$$A(t)\lambda^4 = a, \qquad B(t)\lambda^6 = b$$

leads to the equation

$$b^2A(t)^3 = a^3B(t)^2$$

which has $O(1)$ solutions (by the condition on the $j$-invariant $j_{A,B}(t)$).

Therefore

$$\#\mathcal{T}_{A,B,p}(\varepsilon) \ll \frac{\#\mathcal{S}_p(\varepsilon)}{p}.$$

Using Lemma 7, we obtain

$$\sum_{t \in \mathcal{T}_{A,B,p}} R_{W,p}(t) \ll \frac{W^2 \# \mathcal{T}_{A,B,p}(\varepsilon)}{p} + W^2 p^{-1} + W p^{1/2+o(1)} = o(W^2)$$

which concludes the proof.

## References

[1] W. D. Banks and I. E. Shparlinski, ‘Sato–Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height’, *Israel J. Math.*, (to appear).

[2] A. Cojocaru and C. Hall, ‘Uniform results for Serre’s theorem for elliptic curves’, *Internat. Math. Res. Notices*, **2005** (2005), 3065–3080.

[3] A. Cojocaru and I. E. Shparlinski, ‘Distribution of Farey fractions in residue classes and Lang–Trotter conjectures on average’, *Proc. Amer. Math. Soc.*, **136** (2008), 1977–1986.

[4] W. Duke, ‘Almost all reductions modulo $p$ of an elliptic curve have a large exponent’, *Comptes Rendus Mathematique*, **337** (2003), 689–692.

[5] K. Ford and I. E. Shparlinski, ‘On finite fields with Jacobians of small exponent’, *Preprint*, 2006 (available from `http://arxiv.org/abs/math.NT/0607474`).

[6] H. Iwaniec and E. Kowalski, *On curves over finite fields with Jacobians of small exponent.* Intern. J. Number Theory, **4**, 2008, 819-826.

[7] F. Luca, J. McKee and I. E. Shparlinski, ‘Small exponent point groups on elliptic curves’, *J. Théorie des Nombres Bordeaux*, **18** (2006), 471–476.

[8] F. Luca and I. E. Shparlinski, ‘On the exponent of the group of points on elliptic curves in extension fields’, *Intern. Math. Research Notices*, **2005** (2005), 1391–1409.

[9] R. Schoof, ‘The exponents of the group of points on the reduction of an elliptic curve’, *Arithmetic Algebraic Geometry*, Progr. Math., vol. 89, Birkhäuser, Boston, MA, 1991, 325–335.

[10] I. E. Shparlinski, ‘Orders of points on elliptic curves’, *Affine Algebraic Geometry*, Contemp. Math., vol. 369, Amer. Math. Soc., Providence, RI, 2005, 245–252.

[11] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, Berlin, 1995.

*Igor E. Shparlinski*  
Department of Computing, Macquarie University, North Ryde,  
Sydney, NSW 2109, Australia  
`igor@ics.mq.edu.au`

*Recibido: 7 de octubre de 2007*  
*Aceptado: 21 de mayo de 2008*