Journal de Théorie des Nombres
de Bordeaux **18** (2006), 471–476

Small exponent point groups on elliptic curves

par Florian LUCA, James MCKEE et Igor E. SHPARLINSKI

Résumé. Soit $\mathbf{E}$ une courbe elliptique définie sur $\mathbb{F}_q$, le corps fini à q éléments. Nous montrons que pour une constante $\eta > 0$ dépendant seulement de q, il existe une infinité d'entiers positifs n tels que l'exposant de $\mathbf{E}(\mathbb{F}_{q^n})$, le groupe des points $\mathbb{F}_{q^n}$-rationnels sur $\mathbf{E}$, est au plus $q^n \exp\left(-n^{\eta/\log\log n}\right)$. Il s'agit d'un analogue d'un résultat de R. Schoof sur l'exposant du groupe $\mathbf{E}(\mathbb{F}_p)$ des points $\mathbb{F}_p$-rationnels, lorsqu'une courbe elliptique fixée $\mathbf{E}$ est définie sur $\mathbb{Q}$ et le nombre premier p tend vers l'infini.

Abstract. Let $\mathbf{E}$ be an elliptic curve defined over $\mathbb{F}_q$, the finite field of q elements. We show that for some constant $\eta > 0$ depending only on q, there are infinitely many positive integers n such that the exponent of $\mathbf{E}(\mathbb{F}_{q^n})$, the group of $\mathbb{F}_{q^n}$-rational points on $\mathbf{E}$, is at most $q^n \exp\left(-n^{\eta/\log\log n}\right)$. This is an analogue of a result of R. Schoof on the exponent of the group $\mathbf{E}(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points, when a fixed elliptic curve $\mathbf{E}$ is defined over $\mathbb{Q}$ and the prime p tends to infinity.

1. Introduction

Let $\mathbf{E}$ be an elliptic curve defined over $\mathbb{F}_q$, the finite field of q elements, where q is a prime power, defined by a Weierstrass equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\,.$$

We consider extensions $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$ and, accordingly, we consider the sets $\mathbf{E}(\mathbb{F}_{q^n})$ of $\mathbb{F}_{q^n}$-rational points on $\mathbf{E}$ (including the point at infinity $\mathcal{O}$).

We recall that $\mathbf{E}(\mathbb{F}_{q^n})$ forms an abelian group (with $\mathcal{O}$ as the identity element). The cardinality $\#\mathbf{E}(\mathbb{F}_{q^n})$ of this group satisfies the Hasse–Weil inequality

$$|\#\mathbf{E}(\mathbb{F}_{q^n}) - q^n - 1| \le 2q^{n/2} \tag{1.1}$$

(see [2, 13, 14] for this, and other general properties of elliptic curves).

It is well-known that the group of $\mathbb{F}_{q^n}$-rational points $\mathbf{E}(\mathbb{F}_{q^n})$ is of the form

$$\mathbf{E}(\mathbb{F}_{q^n}) \cong \mathbb{Z}/L\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z}, \tag{1.2}$$

Manuscrit reçu le 1er janvier 2005.

where the integers L and M are uniquely determined with $M \mid L$. In particular, $\#\mathbf{E}(\mathbb{F}_{q^n}) = LM$. The number $\ell(q^n) = L$ is called the *exponent* of $\mathbf{E}(\mathbb{F}_{q^n})$, and is the largest possible order of points $P \in \mathbf{E}(\mathbb{F}_{q^n})$.

Trivially, from the definition (1.2), and from the equation (1.1), we see that the inequality

$$\ell(q^n) \geq (\#\mathbf{E}(\mathbb{F}_{q^n}))^{1/2} \geq (q^n + 1 - 2q^{n/2})^{1/2} = q^{n/2} - 1$$

holds for all q and n.

For a fixed elliptic curve $\mathbf{E}$ which is defined over $\mathbb{Q}$ that admits no complex multiplication, it has been shown by Schoof [11] that the inequality

$$\ell(p) \geq C(\mathbf{E}) \frac{p^{1/2} \log p}{\log \log p}$$

holds for all prime numbers p of good reduction, where the constant $C(\mathbf{E}) > 0$ depends only on the curve $\mathbf{E}$.

Duke [7], has recently shown, unconditionally for elliptic curves with complex multiplication, and under the *Extended Riemann Hypothesis* for elliptic curves without complex multiplication, that for any function $f(x)$ that tends to infinity as x tends to infinity, the lower bound $\ell(p) \geq p/f(p)$ holds for almost all primes p. However, for elliptic curves without complex multiplication, the only unconditional result available is also in [7], and asserts that the weaker inequality $\ell(p) \geq p^{3/4}/\log p$ holds for almost all primes p. It has also been shown in [11], that, under the Extended Riemann Hypothesis, for any curve $\mathbf{E}$ over $\mathbb{Q}$,

$$\liminf_{p\to\infty} \frac{\ell(p)}{p^{7/8}\log p} < \infty \tag{1.3}$$

where p runs through prime numbers. This bound rests on an explicit form of the *Chebotarev Density Theorem*. Accordingly, unconditional results of [9] lead to an unconditional, albeit much weaker, upper bound on $\ell(p)$.

In extension fields of $\mathbb{F}_q$, with $\mathbf{E}$ defined over $\mathbb{F}_q$, stronger lower bounds on $\ell(q^n)$ can be obtained. For example, it has recently been shown in [10] that for any $\varepsilon > 0$, the inequality $\ell(q^n) \leq q^{n(1-\varepsilon)}$ holds only for finitely many values of n. In particular, this means that no result of the same strength as (1.3) is possible for elliptic curves in extension fields. Accordingly, here we obtain a much more modest bound which asserts that for some positive constant $\eta > 0$ depending only on q,

$$\liminf_{n\to\infty} \frac{\ell(q^n)}{q^n \exp\left(-n^{\eta/\log\log n}\right)} < \infty. \tag{1.4}$$

The question of cyclicity, that is, whether $\ell(q^n) = \#\mathbf{E}(\mathbb{F}_{q^n})$, has also been addressed in the literature. For curves in extension fields, this question has been satisfactorily answered by Vlăduţ [16]. In the situation where $\mathbf{E}$ is defined over $\mathbb{Q}$, the question about the cyclicity of the reduction $\mathbf{E}(\mathbb{F}_p)$ when p runs over the primes appears to be much harder (see [4, 5, 6] for recent advances and surveys of other related results). In particular, this problem is closely related to the famous *Lang–Trotter conjecture*.

Finally, one can also study an apparently easier question about the distribution of $\ell(q)$ "on average" over various families of elliptic curves defined over $\mathbb{F}_q$ (see [12, 15]).

Throughout this paper, all the explicit and implied constants in the symbol 'O' may depend only on q. For a positive real number $z > 0$, we write $\log z$ for the maximum between 1 and the natural logarithm of z.

Acknowledgements. The authors would like to thank Joseph Silverman for useful discussions. During the preparation of this paper, F. L. was supported in part by grants SEP-CONACYT 37259-E and 37260-E, and I. S. was supported in part by ARC grant DP0211459. This paper was written during a visit of I. S. to Royal Holloway, University of London (supported by an EPSRC Visiting Fellowship), whose hospitality is gratefully acknowledged.

2. The field of definition of torsion points

Let $\overline{\mathbb{F}}_q$ be the algebraic closure of $\mathbb{F}_q$. Given an elliptic curve $\mathbf{E}$ over $\mathbb{F}_q$, the points $P \in \mathbf{E}(\overline{\mathbb{F}}_q)$ with $kP = \mathcal{O}$ for some fixed integer $k \geq 1$, form a group, which is called the *k-torsion group* and denoted by $\mathbf{E}[k]$. If $\gcd(k, q) = 1$, then

$$\mathbf{E}[k] \cong \mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}\,. \tag{2.1}$$

Henceforth, we assume that $\gcd(k, q) = 1$, so that (2.1) holds. Let $\mathbb{K}_k$ be the field of definition of $\mathbf{E}[k]$, that is the field generated by the coordinates of all the k-torsion points, and let $d(k)$ denote the degree of $\mathbb{K}_k$ over $\mathbb{F}_q$. Then $\mathbb{K}_k$ is a Galois extension of $\mathbb{F}_q$. Let $\mathcal{G}_k$ denote the Galois group of this extension. Having chosen generators P_1, P_2 for the k-torsion group, one gets a representation of $\mathcal{G}_k$ as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z})$: any element of $\mathcal{G}_k$ maps each P_i to a $(\mathbb{Z}/k\mathbb{Z})$-linear combination of P_1 and P_2 for $i = 1, 2$.

Although the following statement does not seem to appear in the literature, it is based on an approach which is not new. For example, for the PGL_2 analogue, see Proposition VII.2 of [2].

Lemma 2.1. *Let $t = q + 1 - \#\mathbf{E}\,(\mathbb{F}_q)$. If r is a prime with $\gcd(r, q(t^2 - 4q)) = 1$ and such that $t^2 - 4q$ is a quadratic residue modulo r, then $d(r) \mid (r - 1)$.*

Proof. Since r does not divide q, $\mathbf{E}[r] \cong \mathbb{F}_r \times \mathbb{F}_r$, and the above Galois representation exhibits $\mathcal{G}_r$ as a subgroup of $\mathrm{GL}_2(\mathbb{F}_r)$. Since $\mathbb{F}_q$ is a finite field, $\mathcal{G}_r$ is cyclic, generated by the Frobenius map $\tau(\vartheta) = \vartheta^q$. Let $A \in \mathrm{GL}_2(\mathbb{F}_r)$ correspond to τ. Now $d(r)$ is the order of A in $\mathrm{GL}_2(\mathbb{F}_r)$.

If A is a scalar multiple of the identity matrix, then it has order dividing $r-1$. Otherwise, the characteristic polynomial of A equals its minimal polynomial. Since the relation $\tau^2 - t\tau + q = 0$ holds in the endomorphism ring, we have $A^2 - tA + qI = 0$ over $\mathbb{F}_r$, and this must be the minimal polynomial of A. Since $t^2 - 4q$ is a quadratic residue in $\mathbb{F}_r$, A has two distinct eigenvalues in $\mathbb{F}_r$, from which the result follows immediately. □

We remark that without the condition that $t^2 - 4q$ is a quadratic residue modulo r, similar arguments imply that the relation $d(r) \mid (r^2 - 1)$ holds for any prime r with $\gcd(r, q(t^2 - 4q)) = 1$.

3. Main result

Lemma 2.1 immediately implies that $\ell(q^n) = O(q^n n^{-1})$ infinitely often (namely for each $n = d(r)$, where r is a prime with $\gcd(r, q(t^2 - 4q)) = 1$ and such that $t^2 - 4q$ is a quadratic residue modulo r). Here, we prove a much stronger bound.

Theorem 3.1. *There exists a positive constant $\eta > 0$ such that for infinitely many pairs of positive integers (m, n) we have $\mathbf{E}[m] \subseteq \mathbf{E}(\mathbb{F}_{q^n})$ and*

$$m \geq \exp\left(n^{\eta/\log\log n}\right).$$

Proof. We let $\Delta = 4(t^2 - 4q)$ and we show that there exists a constant $\kappa > 0$ such for any sufficiently large x there exists a set of primes $\mathcal{R}$ such that each $r \in \mathcal{R}$ has the properties that

$$\gcd(r, q) = 1 \qquad \text{and} \qquad r \equiv 1 \pmod{\Delta}, \tag{3.1}$$

and also that

$$\#\mathcal{R} \geq \exp(\kappa \log x / \log\log x) \qquad \text{and} \qquad \mathrm{lcm}\{r - 1 \mid r \in \mathcal{R}\} \leq x^2. \tag{3.2}$$

We follow closely the proof of Proposition 10 of [1]. However, we replace the condition of $r-1$ being squarefree by the conditions (3.1). Namely, let k_0 be the integer of Proposition 8 of [1]. Assuming that x is sufficiently large, as in Proposition 10 of [1], we define k_1 as the product of all primes up $0.5\delta \log x$ for a sufficiently small positive constant δ. We now put $k_2 = k_1 / \gcd(k_1, \Delta)$ and finally $k = k_1 / P(\gcd(k_0, k_2))$. It is clear that $k_0 \nmid \Delta k$ (note that we have not imposed the squarefreeness condition, and thus we do not need the condition $k_0^2 \nmid \Delta k$ to hold, as in [1]). For each $d \mid k$, we denote by A_d the number pairs (m, r) consisting of a positive integer $m \leq x$ and a prime $r \leq x$, with

$$\gcd(r, q) = 1 \qquad \text{and} \qquad \gcd(m, k) = k/d,$$

and which satisfy the system of congruences

$$m(r-1) \equiv 0 \pmod{k} \qquad \text{and} \qquad r \equiv 1 \pmod{\operatorname{lcm}(\Delta, d)}.$$

As in [1], we derive that for some constant $C > 0$, the inequality

$$A_d \geq C \frac{x^2 \varphi(d)}{dk \log x}$$

holds uniformly in d, where $\varphi(d)$ is the Euler function. Repeating the same steps as in the proof of Proposition 10 of [1], we obtain the desired set $\mathcal{R}$ satisfying (3.1) and (3.2). It is clear that $t^2 - 4q$ is a quadratic residue modulo every $r \in \mathcal{R}$ and thus, by Lemma 2.1, the relation $d(r) \mid (r-1)$ holds for all $r \in \mathcal{R}$.

We now define

$$m = \prod_{r \in \mathcal{R}} r \qquad \text{and} \qquad n = \operatorname{lcm}\{r - 1 \mid r \in \mathcal{R}\}.$$

Since, $\mathbf{E}[r] \subseteq \mathbf{E}(\mathbb{F}_{q^n})$ holds for every $r \in \mathcal{R}$, it follows that $\mathbf{E}[m] \subseteq \mathbf{E}(\mathbb{F}_{q^n})$. We now derive, from (3.2), that $n \leq x^2$, and using the Prime Number Theorem, we get

$$m \geq \exp\left((1 + o(1))\#\mathcal{R}\right) \geq \exp\left((1 + o(1)) \exp(\kappa \log x / \log\log x)\right),$$

which finishes the proof. □

It is now clear that Theorem 3.1 implies relation (1.4).

4. Applications to Lucas sequences

Let $u_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ be a Lucas sequence, where α and β are roots of the characteristic polynomial $f(X) = X^2 + AX + B \in \mathbb{Z}[X]$. Then the arguments of the proof of Theorem 3.1 show that there are many primes r such that $A^2 - 4B$ is a quadratic residue modulo r and the least common multiple of all the $r - 1$ is small. In a quantitive form this implies that, for infinitely many positive integers n,

$$\omega(u_n) \geq n^{\eta/\log\log n}$$

for some positive constant $\eta > 0$, where $\omega(u)$ is the number of distinct prime divisors of an integer $u \geq 2$.

Moreover, given $s \geq 2$ Lucas sequences $u_{i,n}$, $i = 1, \ldots, s$, one can use the same arguments to show that, for infinitely many positive integers n,

$$\omega(\gcd(u_{1,n}, \ldots, u_{s,n})) \geq n^{\eta/\log\log n}.$$

This generalises and refines a remark made in [3]. In particular, we see that for any integers $a > b > 1$, the result of [1] immediately implies that

$$\gcd(a^n - 1, b^n - 1) \geq \exp\left(n^{\eta/\log\log n}\right)$$

infinitely often (which shows that the upper bound of [3] is rather tight).

References

[1] L. M. ADLEMAN, C. POMERANCE, R. S. RUMELY, *On distinguishing prime numbers from composite numbers.* Annals Math. **117** (1983), 173–206.
[2] I. BLAKE, G. SEROUSSI, N. SMART, *Elliptic curves in cryptography.* London Math. Soc., Lecture Note Series **265**, Cambridge Univ. Press, 1999.
[3] Y. BUGEAUD, P. CORVAJA, U. ZANNIER, *An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$.* Math. Zeitschrift **243** (2003), 79–84.
[4] A. COJOCARU, *On the cyclicity of the group of $\mathbb{F}_p$ -rational points of non-CM elliptic curves.* J. Number Theory **96** (2002), 335–350.
[5] A. COJOCARU, *Cyclicity of CM elliptic curves modulo p.* Trans. Amer. Math. Soc. **355** (2003), 2651–2662.
[6] A. COJOCARU, M. R. MURTY, *Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem.* Mathematische Annalen **330** (2004), 601–625.
[7] W. DUKE, *Almost all reductions of an elliptic curve have a large exponent.* Comptes Rendus Mathématiques **337** (2003), 689–692.
[8] P. ERDÖS, C. POMERANCE, E. SCHMUTZ, *Carmichael's lambda function.* Acta Arith. **58** (1991), 363–385.
[9] J. C. LAGARIAS, H. L. MONTGOMERY, A. M. ODLYZKO, *A bound for the least prime ideal in the Chebotarev density theorem.* Invent. Math. **54** (1979), 271–296.
[10] F. LUCA, I. E. SHPARLINSKI, *On the exponent of the group of points on elliptic curves in extension fields.* Intern. Math. Research Notices **23** (2005), 1391–1409.
[11] R. SCHOOF, *The exponents of the group of points on the reduction of an elliptic curve*, Arithmetic Algebraic Geometry. Progr. Math. **89**, Birkhäuser, Boston, MA, 1991, 325–335.
[12] I. E. SHPARLINSKI, *Orders of points on elliptic curves*, Affine Algebraic Geometry. Contemp. Math. **369**, Amer. Math. Soc., 2005, 245–252.
[13] J. H. SILVERMAN, *The arithmetic of elliptic curves.* Springer-Verlag, Berlin, 1995.
[14] J. H. SILVERMAN, J. TATE, *Rational points on elliptic curves.* Springer-Verlag, Berlin, 1992.
[15] S. G. VLĂDUŢ, *Cyclicity statistics for elliptic curves over finite fields.* Finite Fields and Their Appl. **5** (1999), 13–25.
[16] S. G. VLĂDUŢ, *A note on the cyclicity of elliptic curves over finite field extensions.* Finite Fields and Their Appl. **5** (1999), 354–363.

Florian LUCA
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58089, Morelia, Michoacán, México
E-mail : fluca@matmor.unam.mx

James MCKEE
Department of Mathematics
Royal Holloway, University of London
Egham, Surrey, TW20 0EX, UK
E-mail : james.mckee@rhul.ac.uk

Igor E. SHPARLINSKI
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
E-mail : igor@ics.mq.edu.au