

ON THE EXPONENT OF THE GROUP OF POINTS OF AN ELLIPTIC CURVE OVER A FINITE FIELD

FRANCESCO PAPPALARDI

(Communicated by Ken Ono)

ABSTRACT. We present a lower bound for the exponent of the group of rational points of an elliptic curve over a finite field. Earlier results considered finite fields \mathbb{F}_{q^m} where either q is fixed or $m = 1$ and q is prime. Here, we let both q and m vary; our estimate is explicit and does not depend on the elliptic curve.

1. INTRODUCTION

Let \mathbb{F}_q be a finite field with $q = p^m$ elements and let E be an elliptic curve defined over \mathbb{F}_q . It is well known (see for example the book of Washington [7]) that the group of rational point of E over \mathbb{F}_q satisfies

$$E(\mathbb{F}_q) \cong \mathbb{Z}_n \times \mathbb{Z}_{nk},$$

where $n, k \in \mathbb{N}$ are such that $n \mid q - 1$. The *exponent* of $E(\mathbb{F}_q)$ is

$$\exp(E(\mathbb{F}_q)) = nk.$$

The problem of studying $\exp(E(\mathbb{F}_q))$ is a natural one and was started by Schoof [6] in 1989. He proved that if E is an elliptic curve over \mathbb{Q} without complex multiplication, then for every prime $p > 2$ of good reduction for E , one has the estimate

$$\exp(E(\mathbb{F}_p)) > C_E \sqrt{p} \frac{\log p}{(\log \log p)^2},$$

where $C_E > 0$ is a constant depending only on E .

In 2005, Luca and Shparlinski [4] considered the case when q is fixed and they proved that if E/\mathbb{F}_q is ordinary, there exists an effectively computable constant $\vartheta(q)$ depending only on q such that

$$(1) \quad \exp(E(\mathbb{F}_{q^m})) > q^{m/2 + \vartheta(q)m / \log m}$$

holds for all positive integers $m > 1$.

Other lower bounds that hold for families of primes (resp. for families of powers of fixed primes) with density one were proven by Duke in [2] (resp. by Luca and Shparlinski in [4]).

Here we let both p and m vary, and we prove the following:

Received by the editors December 23, 2009 and, in revised form, June 13, 2010 and June 21, 2010.

2010 *Mathematics Subject Classification*. Primary 11G20; Secondary 11G05.

Key words and phrases. Elliptic curves, finite fields.

Theorem. *Let E be any elliptic curve over \mathbb{F}_{p^m} where $m \geq 3$. Then either $m = 2r$ is even and*

$$E(\mathbb{F}_{p^{2r}}) \cong \mathbb{Z}_{p^r \pm 1} \times \mathbb{Z}_{p^r \pm 1}$$

or

$$\exp(E(\mathbb{F}_{p^m})) \geq 2^{-46} p^{m/2} \frac{m^{1/3}}{(\log m)^{8/3} (\log \log m)^{1/3}}.$$

Note that the result also applies to supersingular elliptic curves and that it improves on that in (1) for values of m which are small with respect to p .

2. LEMMAS

The proof is based on estimates for the distance between perfect powers due to Bugeaud. More precisely, we will apply the following result from [1]:

Lemma 1. *Let $f \in \mathbb{Z}[X]$ be a monic polynomial of degree $d \geq 2$ without multiple roots. Let H be the maximum of the absolute values of its coefficients and D be its discriminant. Let a, x, y , and m be rational integers satisfying $a \neq 0, |y| \geq 2, m \geq 2, f(x) = ay^m$. Denote by \log_2 the logarithm in base 2 and write $\log_* x$ for $\max\{\log x, 1\}$. The following inequality holds:*

$$m < \max \left\{ d \log_2(2H + 3), 2^{15(d+6)} d^{7d} |D|^{3/2} (\log |D|)^{3d} (\log_* |a|)^2 \log_* \log_* |a| \right\}.$$

We need the following elementary lemma:

Lemma 2. *If q is a prime power and E is an elliptic curve defined over \mathbb{F}_q such that $E(\mathbb{F}_q) \cong \mathbb{Z}_n \times \mathbb{Z}_{nk}$, then $q = n^2k + n\ell + 1$ for some integer ℓ that satisfies $|\ell| \leq 2\sqrt{k}$.*

Proof. By the Hasse bound, we can write $n^2k = q + 1 - a_q$ for some integer a_q that satisfies $a_q^2 \leq 4q$. Using the Weil pairing one also sees that $q \equiv 1 \pmod{n}$. Hence $a_q = 2 + n\ell$ for some integer ℓ and $q = n^2k + n\ell + 1$. Finally

$$n^2\ell^2 + 4n\ell + 4 = a_q^2 \leq 4q = 4n^2k + 4n\ell + 4,$$

and the result follows. □

We will also need the classical characterizations of the group structures due to Waterhouse (see [7, Theorem 4.3, page 98]) which describes possible cardinalities $\#E(\mathbb{F}_q)$ of the set of \mathbb{F}_q -rational points of elliptic curves over \mathbb{F}_q .

Lemma 3. *Let $q = p^m$ be a power of a prime p and let $N = q + 1 - a$. There is an elliptic curve E defined over \mathbb{F}_q such that $\#E(\mathbb{F}_q) = N$ if and only if $|a| \leq 2\sqrt{q}$ and a satisfies one of the following:*

- (i) $\gcd(a, p) = 1$;
- (ii) m even and $a = \pm 2\sqrt{q}$;
- (iii) m is even, $p \not\equiv 1 \pmod{3}$, and $a = \pm\sqrt{q}$;
- (iv) m is odd, $p = 2$ or 3 , and $a = \pm p^{(m+1)/2}$;
- (v) m is even, $p \not\equiv 1 \pmod{4}$, and $a = 0$;
- (vi) m is odd and $a = 0$.

For each admissible cardinality, Rück (see Washington [7, Theorem 4.4, page 98]) describes the possible group structures.

Lemma 4. *Let N be an integer that occurs as the order of an elliptic curve over a finite field \mathbb{F}_q , where $q = p^m$ is a power of a prime p . Write $N = p^e n_1 n_2$ with $p \nmid n_1 n_2$ and $n_1 \mid n_2$ (possibly $n_1 = 1$). There is an elliptic curve E over \mathbb{F}_q such that*

$$E(\mathbb{F}_q) \cong \mathbb{Z}_{p^e} \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$$

if and only if

- (1) $n_1 = n_2$ in case (ii) of Lemma 3;
- (2) $n_1 \mid q - 1$ in all other cases of Lemma 3.

Finally we need the following numerical statement:

Lemma 5. *Assume that α and β are real numbers with $\alpha > 4$ and $\beta \geq 4$. If*

$$\alpha \leq \beta^{3/2} \cdot (\log \beta)^8 \cdot \log \log \beta,$$

then

$$\beta \geq \frac{\alpha^{2/3}}{(\log \alpha)^{16/3} (\log \log \alpha)^{2/3}}.$$

Proof. If $\alpha \geq \beta \geq 4$, then

$$\beta \geq \left(\frac{\alpha}{(\log \beta)^8 \log \log \beta} \right)^{2/3} \geq \left(\frac{\alpha}{(\log \alpha)^8 \log \log \alpha} \right)^{2/3}.$$

If $4 < \alpha \leq \beta$,

$$\beta \geq \alpha \geq \frac{\alpha^{2/3}}{(\log \alpha)^{16/3} (\log \log \alpha)^{2/3}}.$$

□

3. PROOF OF THE THEOREM

Assume that $E(\mathbb{F}_{p^m}) \cong \mathbb{Z}_n \times \mathbb{Z}_{nk}$. Then, by Lemma 2, we have that

$$p^m = kn^2 + \ell n + 1 \quad \text{for some } \ell \text{ with } |\ell| \leq 2\sqrt{k}.$$

If $\ell = \pm 2\sqrt{k}$, then k must be a perfect square, and we write $k = M^2$ so that $\ell = \pm 2M$. Therefore in the above identity we have

$$p^m = (Mn \pm 1)^2,$$

which implies that $m = 2r$ is even and that $Mn = p^r \mp 1$. Furthermore, in this case

$$p^m + 1 - \#E(\mathbb{F}_{p^m}) = \ell n + 2 = \pm 2Mn + 2 = \pm 2p^{m/2}.$$

This happens precisely in case (ii) of Lemma 3. Note also that in this case $p \nmid \#E(\mathbb{F}_{p^m})$. Hence, by case (1) in Lemma 4, we have that $n = nk$ so that $k = 1$.

We conclude that if $\ell = \pm 2\sqrt{k}$, then $k = 1$, $n = p^r \mp 1$ and finally

$$E(\mathbb{F}_{p^{2r}}) \cong \mathbb{Z}_{p^r \pm 1} \times \mathbb{Z}_{p^r \pm 1}.$$

From now on, we can assume that $|\ell| < 2\sqrt{k}$. We apply Lemma 1 with the following data:

$$\begin{aligned} f(X) &= X^2 + \ell X + k, & d &= 2, & |D| &= 4k - \ell^2, & H &= k, \\ x &= kn, & y &= p & \text{and} & a &= k. \end{aligned}$$

Note that since $|\ell| < 2\sqrt{k}$, we have that $D \neq 0$ so that f has two distinct roots.

From the identity $kp^m = (kn)^2 + \ell(kn) + k$ and from Lemma 1, it follows that

$$m \leq \max\{2 \log_2(2k + 3), 2^{134}(4k)^{3/2}(\log 4k)^6(\log_* k)^2(\log_* \log_* k)\}.$$

Since we can assume that $k \geq 2$, it follows that

$$m \leq 2^{134}(4k)^{3/2}(\log 4k)^8 \log \log 4k.$$

If $4 \leq m \leq 2^{136}$, then $m^{1/3}/(2^{45}(\log m)^{8/3}(\log \log m)^{1/3}) < 1/4$, and the statement of the Theorem is vacuous since $\exp(E(\mathbb{F}_q)) \geq \sqrt{q} - 1$ for every q .

If $m > 2^{136}$, we apply Lemma 5 with $\alpha = m/2^{134} > 4$ and $\beta = 4k$, and we obtain

$$k \geq \frac{1}{4} \cdot \frac{(m/2^{134})^{2/3}}{(\log_* \frac{m}{2^{134}})^{16/3} (\log_* \log_* \frac{m}{2^{134}})^{2/3}} \geq \frac{1}{2^{274/3}} \cdot \frac{m^{2/3}}{(\log m)^{16/3} (\log \log m)^{2/3}},$$

and so

$$\exp(E(\mathbb{F}_{p^m})) = nk \geq (\sqrt{p^m} - 1)\sqrt{k} \geq p^{m/2} \frac{m^{1/3}}{2^{46}(\log m)^{8/3}(\log \log m)^{1/3}}.$$

This concludes the proof of the Theorem. □

The constant 2^{-46} can be slightly improved with a more careful analysis, but this is not too important.

4. CONCLUSION

To construct curves with a small exponent one can consider a recent result of Matomäki in [5] that states that, for any $\epsilon > 0$, there exist infinitely many primes p of the form $p = an^2 + 1$ with $a < p^{1/2+\epsilon}$.

Let $p > 3$ be one such prime. Since $p + 1 - an^2 = 2$ and p is odd, part (i) of Lemma 3 assures that there exists an ordinary elliptic curve E over \mathbb{F}_p with $\#E(\mathbb{F}_p) = an^2$ points. Furthermore, since $p \equiv 1 \pmod n$, part (2) of Lemma 4 assures that one can choose E in such a way that

$$E(\mathbb{F}_p) \cong \mathbb{Z}_n \times \mathbb{Z}_{na}.$$

This implies that there exists an infinite sequence of primes p , each with an ordinary elliptic curve E/\mathbb{F}_p such that

$$\exp(E(\mathbb{F}_p)) = an < p^{3/4+\epsilon}.$$

One can also consider, for a prime p , the identity

$$p^3 + 1 - (p + 2)(p - 1)^2 = 3p - 1.$$

Since $3p - 1$ is coprime to p and $3p - 1 \leq 2\sqrt{p^3}$, part (i) of Lemma 3 can be applied with $q = p^3$ and $N = (p + 2)(p - 1)^2$. It follows that there exists an elliptic curve E over \mathbb{F}_{p^3} with $\#E(\mathbb{F}_{p^3}) = (p + 2)(p - 1)^2$ points. Furthermore, if $p \equiv 7 \pmod 9$, we can write $N = n_1 n_2$, where $n_1 = 3(p - 1)$ and $n_2 = \frac{(p+2)(p-1)}{3}$. It is clear that $n_1 \mid n_2$ and that $n_1 \mid p^3 - 1$, so part (2) of Lemma 4 can be applied. It follows that for every prime $p \equiv 7 \pmod 9$, there exists an ordinary elliptic curve over \mathbb{F}_{p^3} such that

$$E(\mathbb{F}_{p^3}) \cong \mathbb{Z}_{3p-3} \times \mathbb{Z}_{\frac{(p+2)(p-1)}{3}}.$$

We immediately conclude that there exists a infinite sequence of distinct q with an elliptic curve E/\mathbb{F}_q such that

$$(2) \quad \exp(E(\mathbb{F}_q)) = \frac{q^{2/3}}{3}(1 + o(1)).$$

This should be compared on one side with Schoof's result in [6] that (assuming GRH) if E is an elliptic curve over \mathbb{Q} , there exists a constant c_E such that $\exp(E(\mathbb{F}_p)) < c_E p^{7/8} \log p$ for infinitely many primes p and on another side with Luca, McKee and Shparlinski's results in [3] that there exists an absolute constant $\rho > 0$ such that if E/\mathbb{F}_q is a fixed elliptic curve, the inequality

$$\exp(E(\mathbb{F}_{q^m})) < q^m \exp\left(-m^{\rho/\log \log m}\right)$$

holds for infinitely many positive integers m .

We wonder if, for every $\epsilon > 0$, one can construct an infinite family of prime powers q , each with an elliptic curve E/\mathbb{F}_q such that

$$E(\mathbb{F}_q) \not\cong \mathbb{Z}_{\sqrt{q}\pm 1} \times \mathbb{Z}_{\sqrt{q}\pm 1}$$

and

$$\exp(E(\mathbb{F}_q)) \ll_{\epsilon} q^{1/2+\epsilon}$$

or if the $2/3$ in (2) can be improved.

ACKNOWLEDGEMENTS

The author would like to thank Bill Banks, Jorge Jimenez Urroz and Igor Shparlinski for some useful conversations.

REFERENCES

- [1] BUGEAUD, YANN, *Sur la distance entre deux puissances pures*. C. R. Acad. Sci. Paris Sér. I Math. **322** (1996), no. 12, 1119–1121. MR1396651 (97i:11030)
- [2] DUKE, WILLIAM, *Almost all reductions modulo p of an elliptic curve have a large exponent*. C. R. Math. Acad. Sci. Paris **337** (2003), no. 11, 689–692. MR2030403 (2005b:11071)
- [3] LUCA, FLORIAN; MCKEE, JAMES; SHPARLINSKI, IGOR E., *Small exponent point groups on elliptic curves*. J. Théor. Nombres Bordeaux **18** (2006), no. 2, 471–476. MR2289434 (2008a:11070)
- [4] LUCA, FLORIAN; SHPARLINSKI, IGOR E., *On the exponent of the group of points on elliptic curves in extension fields*. Int. Math. Res. Not. 2005, no. 23, 1391–1409. MR2152235 (2006h:11072)
- [5] MATOMÁKI, KAISA, *A note on primes of the form $p = aq^2 + 1$* . Acta Arith. **137** (2009), 133–137. MR2491532 (2009m:11151)
- [6] SCHOOF, RENÉ, *The exponents of the groups of points on the reductions of an elliptic curve*. Arithmetic algebraic geometry (Texel, 1989), 325–335, Progr. Math., 89, Birkhäuser Boston, Boston, MA, 1991. MR1085266 (91j:11043)
- [7] WASHINGTON, LAWRENCE C., *Elliptic curves*. Number theory and cryptography. Second edition. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2008. MR2404461 (2009b:11101)

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ ROMA TRE, LARGO SAN LEONARDO MURIALDO 1, I-00146, ROMA, ITALY

E-mail address: `pappa@mat.uniroma3.it`