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

FRANCESCO PAPPALARDI

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 and our estimate is explicit and does not depend on the elliptic curve.

## 1. INTRODUCTION

Let $\mathbb{F}_q$ be a finite fields 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

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

In 1989 Schoof [6] 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] consider the case when $q$ is fixed and they prove that if $E/\mathbb{F}_q$ is ordinary, the there exists an effectively computable constant $\vartheta(q)$ depending only on $q$ such that

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

holds for all positive integers $m$.

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 [1] (resp. by Luca and Shparlinski in [4]).

Here we let both $p$ and $m$ vary and we prove the following

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

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

*Date*: December 23, 2009.

2000 *Mathematics Subject Classification.* Primary: 11G20; Secondary: 11G5.

*Key words and phrases.* keywords: elliptic curves, finite fields.

*or*

$$\exp(E(\mathbb{F}_{p^m})) \geq 2^{-46} p^{m/2} \frac{m^{1/3}}{(\log m)^{7/3} (\log\log m)^{1/3}}.$$

In the above we assume that log denotes the logarithm in base 2.

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

## 2. LEMMATA

The proof is based on estimates for the distance between perfect powers due to Bugeaud. More precisely, we will apply the following result from [2]:

**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 absolute values of its coefficients and $D$ its discriminant. Let $a$, $x$, $y$, $m$ 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 inequality $m \leq \max\{U, V\}$ holds with $U = d\log_2(2H+3)$ and*

$$V = 2^{15(d+6)} d^{7d} |D|^{3/2} (\log |D|)^{3d} (\log_* |a|)^2 \log_* \log_* |a|.$$

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 $\ell$ 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 $\ell$ 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 $a = \pm p^{(n+1)/2}$;*
- (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 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 the case (ii) of Lemma 3;*
(2) *$n_1 | q - 1$ in all other cases of Lemma 3.*

Finally we need the following numerical statement:

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

$$\alpha \leq \beta^{3/2} \cdot (\log \beta)^7 \cdot \log\log \beta,$$

*then*

$$\beta \geq \frac{\alpha^{2/3}}{(\log \alpha)^{14/3}(\log\log \alpha)^{2/3}}.$$

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

$$\beta \geq \left(\frac{\alpha}{(\log \beta)^7 \log\log \beta}\right)^{2/3} \geq \left(\frac{\alpha}{(\log \alpha)^7 \log\log \alpha}\right)^{2/3}.$$

If $\alpha \leq \beta$,

$$\beta \geq \alpha \geq \frac{\alpha^{2/3}}{(\log \alpha)^{14/3}(\log\log \alpha)^{2/3}}.$$

□

## 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

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

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 the 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 $l = \pm 2\sqrt{k}$, 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:

$$f(X) = X^2 + \ell X + k, \quad d = 2, \quad |D| = 4k - \ell^2, \quad H = k,$$

$$x = kn, \quad y = p \quad \text{and} \quad a = k.$$

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

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

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

$$m \leq 2^{134}(4k)^{3/2}(\log 4k)^7 \log\log 4k.$$

If $4 \leq m \leq 2^{136}$, then $m^{1/3}/(2^{46}(\log m)^{7/3}(\log\log m)^{1/3}) < 1/4$ 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:

$$k \geq \frac{1}{4} \cdot \frac{(m/2^{134})^{2/3}}{(\log_* \frac{m}{2^{134}})^{\frac{14}{3}}(\log_* \log_* \frac{m}{2^{134}})^{\frac{2}{3}}} \geq \frac{1}{2^{\frac{274}{3}}} \cdot \frac{m^{2/3}}{(\log m)^{14/3}(\log\log m)^{2/3}}.$$

and so

$$\exp(E(\mathbb{F}_{p^m}) = nk \geq (\sqrt{p^m} - 1)\sqrt{k} \geq p^{m/2} \frac{m^{1/3}}{2^{46}(\log m)^{7/3}(\log\log m)^{1/3}}.$$

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

In the opposite direction a recent result of Matomäki in [5] states that, for any $\epsilon > 0$, there exists infinitely many primes $p$ of the form $p = an^2 + 1$ with $a < p^{1/2+\epsilon}$. By Lemma 4 and Lemma 2, it follows that for infinitely many primes $p$ there exists an elliptic curve over $\mathbb{F}_p$ such that

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

This implies that there exists a infinite sequence of distinct $p$ with an ordinary elliptic curve $E/\mathbb{F}_p$ such that

$$\exp(E(\mathbb{F}_p)) = p^{3/4+\epsilon}(1 + o(1)).$$

One can also consider the polynomial identity

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

By Lemma 4 and Lemma 2, it follows that for every prime $p$ there exists an ordinary elliptic curve over $\mathbb{F}_{p^3}$ such that

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

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

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

This should be compared on one side with Schoof 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

$$E(\mathbb{F}_q) \not\cong \mathbb{Z}_{\sqrt{q}\pm1} \times \mathbb{Z}_{\sqrt{q}\pm1}$$

and

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

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

More generally, the polynomial identity

$$X^n = (X-1)^2 \cdot \big(X^{n-2} + 2X^{n-3} + \cdot + (n-2)X + n - 1\big) + n(X-1) + 1$$

leads, for any fixed $n \geq 2$ to an infinite sequence of distinct primes $p$ with an elliptic curve $E/\mathbb{F}_{p^n}$ such that

$$\exp(E(\mathbb{F}_{p^n})) = p^{n-1}(1 + o(1)).$$

Furthermore, if $n \geq 3$ each $E/F_{p^n}$ is ordinary.

**Acknowledgement:** The author would like to thank Bill Banks and Igor Shparlinski for some useful conversations.

## References


[1] 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.

[2] Bugeaud,Yann *Sur la distance entre deux puissances pures* C. R. Acad. Sci. Paris Sér. I Math. **322** (1996), no. 12, 1119–1121

[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.

[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.

[5] Matomäki, Kaisa *A note on primes of the form $p = aq^2 + 1$.* Acta Arith. **137** (2009), 133–137

[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.

[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.


Dipartimento di Matematica, Università Roma Tre, Largo San Leonardo Murialdo 1, I–00146, Roma, ITALY

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