On the ℓ-adic valuation of the cardinality of elliptic curves over finite extensions of $\mathbb{F}_q$

Josep M. Miret   Jordi Pujolàs   Javier Valera

Abstract. Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ of odd characteristic. Let $\ell \neq 2$ be a prime number different from the characteristic and dividing $\#E(\mathbb{F}_q)$. We describe how the ℓ-adic valuation of the number of points grows by taking finite extensions of the base field. We also investigate the group structure of the corresponding ℓ-Sylow subgroups.

1. Introduction

Let q be a power of a prime $p \neq 2$ and let E be an elliptic curve over a finite field $\mathbb{F}_q$. We compute the difference of valuations $v_\ell(\#E(\mathbb{F}_{q^k})) - v_\ell(\#E(\mathbb{F}_q))$, where k is a natural number and $\ell \neq 2, p$ is a prime number dividing $\#E(\mathbb{F}_q)$ (Theorems 1, 2). Our result agrees with the predictions of Iwasawa Theory.

Under the given assumptions, $v_\ell(\#E(\mathbb{F}_{q^k})) - v_\ell(\#E(\mathbb{F}_q)) > 0$ only if $v_\ell(k) > 0$ or if k is divisible by the multiplicative order d of q in $\mathbb{F}_\ell^*$ (see Proposition 2). Hence we can reduce the proofs to the cases $k = \ell$ or $k = d$. We also describe how the group structure of the ℓ-Sylow subgroup $E[\ell^\infty](\mathbb{F}_{q^k})$ changes with k. Namely, if

$$E[\ell^\infty](\mathbb{F}_q) \cong \mathbb{Z}/\ell^r\mathbb{Z} \times \mathbb{Z}/\ell^s\mathbb{Z} \quad \text{with} \quad 0 \leq r \leq s \quad \text{and} \quad r + s \geq 1,$$

we show how to determine integers r_k, s_k such that $E[\ell^\infty](\mathbb{F}_{q^k}) \cong \mathbb{Z}/\ell^{r_k}\mathbb{Z} \times \mathbb{Z}/\ell^{s_k}\mathbb{Z}$.

On this regard, a partial answer appeared in [3, Proposition 6.3] for $k = \ell$. The case of ordinary elliptic curves with $k = \ell$, $q \equiv 1 \pmod{\ell}$ and $t^2 - 4q \equiv 0 \pmod{\ell^2}$, for t the trace of Frobenius endomorphism, was covered in [4, Proposition 4.2] using pairings. The case of supersingular elliptic curves for $k = d$, $q \not\equiv 1 \pmod{\ell}$ and for some other particular cases was set in [6, Section 4].

Notation. For us, q is the power of some prime number $p \neq 2$, E is an elliptic curve over $\mathbb{F}_q$, $\ell \neq 2$, p is a prime number such that $\ell \mid \#E(\mathbb{F}_q)$ and d is the multiplicative order of q in $\mathbb{F}_\ell^*$. We write the multiplication-by-m isogeny $[m]$ as m.

2. A recurrence formula for $\#E(\mathbb{F}_{q^k})$

The cardinality of E over a finite extension of $\mathbb{F}_q$ is

$$\#E(\mathbb{F}_{q^k}) = \deg(1-\phi^k) = q^k + 1 - t_k, \tag{1}$$

where t_k is the trace of the Frobenius endomorphism ϕ^k of E over $\mathbb{F}_{q^k}$ (see [10, Theorem 2.3.1]), and

$$q^k = \phi^k \widehat{\phi^k}, \quad t_k = \phi^k + \widehat{\phi^k}, \tag{2}$$

where $\widehat{\phi^k}$ is the dual of ϕ^k. By varying k, the traces t_k (we set $t = t_1$) satisfy the recurrence

$$t_2 = t^2 - 2q, \qquad t_k = t t_{k-1} - q t_{k-2} \quad \text{for} \quad k \geq 3. \tag{3}$$

The first thing we do is to express (3) in terms of the cardinalities $\#E(\mathbb{F}_{q^k})$.

Proposition 1. *Let k be a natural number. Then*

$$\#E(\mathbb{F}_{q^k}) = \#E(\mathbb{F}_q)\left(k\sum_{i=0}^{k-1} q^i - \sum_{i=1}^{k-1} \#E(\mathbb{F}_{q^i}) \sum_{j=0}^{k-i-1} q^j\right).$$

Proof. We have $\#E(\mathbb{F}_{q^k}) = \deg(1-\phi^k) = \#E(\mathbb{F}_q)\deg(1+\phi+\cdots+\phi^{k-1})$. The expansion of the rightmost factor is $\sum_{i,j=0}^{k-1} \phi^i \widehat{\phi^j} =$

$$\sum_{i=0}^{k-1} \phi^i\widehat{\phi^i} + (\phi+\widehat{\phi})\sum_{i=0}^{k-2}\phi^i\widehat{\phi^i} + (\phi^2+\widehat{\phi^2})\sum_{i=0}^{k-3}\phi^i\widehat{\phi^i} + \cdots + (\phi^{k-1}+\widehat{\phi^{k-1}}),$$

which by (1) and (2) reduces to

$$\sum_{i=0}^{k-1} q^i + \sum_{i=1}^{k-1}(q^i + 1 - \#E(\mathbb{F}_{q^i}))\sum_{j=0}^{k-i-1} q^j = k\sum_{i=0}^{k-1} q^i - \sum_{i=1}^{k-1}\#E(\mathbb{F}_{q^i})\sum_{j=0}^{k-i-1} q^j.$$

□

Proposition 2. *Let $\tau = v_\ell(k)$ and let d be the multiplicative order of q in $\mathbb{F}_\ell^*$. Then*

$$v_\ell(\#E(\mathbb{F}_{q^k})) = \begin{cases} v_\ell(\#E(\mathbb{F}_{q^{\ell^\tau}})) & \text{if } d \nmid k, \\ v_\ell(\#E(\mathbb{F}_{q^{d\ell^\tau}})) & \text{if } d \mid k. \end{cases}$$

Proof. By Proposition 1 with $k = \ell^\tau k'$, $\ell \nmid k'$ and $q^k = (q^{\ell^\tau})^{k'}$, we have

$$\#E(\mathbb{F}_{q^k}) = \#E(\mathbb{F}_{q^{\ell^\tau}})\left(k'\sum_{i=0}^{k'-1} q^{i\ell^\tau} - \sum_{i=1}^{k'-1}\#E(\mathbb{F}_{q^{i\ell^\tau}})\sum_{j=0}^{k'-i-1} q^{j\ell^\tau}\right) \tag{4}$$

at once. If $d \nmid k$ then $q \not\equiv 1 \pmod{\ell}$ and $v_\ell\left(\sum_{i=0}^{k'-1} q^{i\ell^\tau}\right) = v_\ell\left(\frac{q^k-1}{q^{\ell^\tau}-1}\right) = 0$ because the numerator is not 0 modulo ℓ. Since

$$v_\ell\left(\sum_{i=1}^{k'-1} \#E(\mathbb{F}_{q^{i\ell^\tau}}) \sum_{j=0}^{k'-i-1} q^{j\ell^\tau}\right) \geq v_\ell(\#E(\mathbb{F}_{q^{\ell^\tau}})) > 0,$$

we see $v_\ell(\#E(\mathbb{F}_{q^k})) = v_\ell(\#E(\mathbb{F}_{q^{\ell^\tau}}))$. Similarly, if $d \mid k$ then (4) with $k = d\ell^\tau k'$ implies $v_\ell(\#E(\mathbb{F}_{q^k})) = v_\ell(\#E(\mathbb{F}_{q^{d\ell^\tau}}))$ since $v_\ell\left(k' \sum_{i=0}^{k'-1} q^{id\ell^\tau}\right) = 0$. □

Proposition 2 above reduces our problem to two cases: extensions of $\mathbb{F}_q$ of degree ℓ (see Section 3) and, only if $q \not\equiv 1 \pmod{\ell}$, extensions of degree equal to the multiplicative order d of q in $\mathbb{F}_\ell^*$ (see Section 4).

3. Increment of $v_\ell(\#E(\mathbb{F}_{q^\ell}))$

In this section we consider field extensions of degree $k = \ell$.

Theorem 1. *Unless $\ell = 3$ and $q \equiv 1 \pmod 3$ and $\#E(\mathbb{F}_q) \equiv 3 \pmod 9$ hold, we have*

$$v_\ell(\#E(\mathbb{F}_{q^\ell})) = \begin{cases} v_\ell(\#E(\mathbb{F}_q)) + 1 & \text{if } q \not\equiv 1 \pmod{\ell}, \\ v_\ell(\#E(\mathbb{F}_q)) + 2 & \text{if } q \equiv 1 \pmod{\ell}. \end{cases}$$

For $\ell = 3$ and $q \equiv 1 \pmod 3$ and $\#E(\mathbb{F}_q) \equiv 3 \pmod 9$, we have

$$v_3(\#E(\mathbb{F}_{q^3})) - v_3(\#E(\mathbb{F}_q)) = 2\min\{v_3(q-1), v_3(t+1)\} \geq 4,$$

except if $q - 1 \equiv t + 1 \pmod{3^{v_3(q-1)+1}}$, in which case we have

$$v_3(\#E(\mathbb{F}_{q^3})) - v_3(\#E(\mathbb{F}_q)) = 2v_3(q-1) + 1 \geq 3.$$

Proof. Let ξ be a primitive ℓ-th root of unity. Then the ideal (ℓ) factors in $\mathbb{Z}[\xi]$ as $(\ell) = (1-\xi)^{\ell-1}$, and by elementary number theory the corresponding valuations satisfy $v_\ell() = \frac{1}{\ell-1} v_{1-\xi}()$. Therefore, by (1) and the factorization

$$\deg(1 + \phi + \cdots + \phi^{\ell-1}) = \prod_{i=1}^{\ell-1} (\phi - \xi^i)(\widehat{\phi} - \xi^i),$$

$$v_\ell(\#E(\mathbb{F}_{q^\ell})) = v_\ell(\#E(\mathbb{F}_q)) + \frac{1}{\ell-1} \sum_{i=1}^{\ell-1} v_{1-\xi}\left((\phi - \xi^i)(\widehat{\phi} - \xi^i)\right). \qquad (5)$$

Write $q \equiv \bar{q} \pmod{\ell}$, so that $\bar{q} \in \{1, \ldots, \ell-1\}$. Then

$$(\phi - \xi^i)(\widehat{\phi} - \xi^i) = (1 - \xi^i)(\bar{q} - \xi^i) + \ell k_i$$

for some $k_i \in \mathbb{Z}[\xi]$. Hence the second summand in (5) is 1 for $\bar{q} \neq 1$ or 2 for $\bar{q} = 1$, except possibly for $\ell = 3 = (1-\xi)^2(1+\xi)$. In this case, let $q - 1 \equiv 3x \pmod 9$, $t + 1 \equiv 3y \pmod 9$ for $x, y \in \{0, 1, 2\}$. Then

$$(1 - \xi^i)^2 + 3k_i \equiv 3(x - y\xi^i) \pmod 9.$$

Clearly $v_{1-\xi}((1-\xi^i)^2+3k_i)=2$ if $x\neq y$ and $v_{1-\xi}((1-\xi^i)^2+3k_i)\geq 3$ if $x=y$ (which is equivalent to $\#E(\mathbb{F}_q)\equiv 3 \pmod 9$). More explicitly, let

$$\begin{array}{rcll} q-1 & = & 3x_1+9x_2+\cdots+3^w x_w+\cdots, & x_i\in\{0,1,2\},\\ t+1 & =\pm & (3y_1+9y_2+\cdots+3^w y_w+\cdots), & y_i\in\{0,1,2\}. \end{array}$$

Then

$$(\phi-\xi^i)(\widehat{\phi}-\xi^i)=3(x_1\mp y_1\xi^i)+9(x_2\mp y_2\xi^i)+\cdots+3^w(x_w\mp y_w\xi^i)+\cdots.$$

But if $v_3(q-1)<v_3(t+1)$ with $w=v_3(q-1)\geq 2$, then $x_i=0$ for all $1\leq i<w$, $x_w\neq 0$ and $y_i=0$ for all $1\leq i\leq w$. Hence the increment is $2v_3(q-1)$. Similarly, if $v_3(t+1)<v_3(q-1)$ with $w=v_3(t+1)\geq 2$, then $y_i=0$ for $1\leq i<w$, $y_w\neq 0$ and $x_i=0$ for $1\leq i\leq w$, so the increment is $2v_3(t+1)$. Finally, if $v_3(q-1)=v_3(t+1)=w$ then $x_w,y_w\neq 0$, and the increment is $2v_3(q-1)+1$ if $x_w\mp y_w\equiv 0 \pmod 3$ (which is equivalent to $q-1\equiv t+1 \pmod{3^{v_3(q-1)+1}}$) and $2v_3(q-1)$ if not. $\square$

Example 1. Let $q=p=10099\equiv 1 \pmod 3$, and consider the following elliptic curves over $\mathbb{F}_q$:

$$\begin{array}{ll} E_1\colon y^2=x^3+1070x+7959, & E_2\colon y^2=x^3+9599x+1000,\\ E_3\colon y^2=x^3+3690x+2719, & E_4\colon y^2=x^3+2828x+4443. \end{array}$$

Their numbers of points over $\mathbb{F}_q$ satisfy $\#E_i(\mathbb{F}_q)\equiv 3 \pmod 9$, for $i=1,2,3,4$. From Theorem 1 we deduce the increment of the 3-adic valuation of $\#E_i(\mathbb{F}_{q^3})$:

	E_1	E_2	E_3	E_4
$v_3(q-1)$	3	3	3	3
$v_3(t+1)$	2	3	3	4
$q-1 \pmod{3^{v_3(q-1)+1}}$	54	54	54	54
$t+1 \pmod{3^{v_3(q-1)+1}}$	72	27	54	0
$v_3(\#E(\mathbb{F}_{q^3}))-v_3(\#E(\mathbb{F}_q))$	4	6	7	6

Lemma 1. *For all our ℓ,*

$$v_\ell(1+q+\cdots+q^{\ell-1})=\begin{cases}0 & \text{if } q\not\equiv 1 \pmod{\ell},\\ 1 & \text{if } q\equiv 1 \pmod{\ell}.\end{cases}$$

Proof. Assume first $q\not\equiv 1 \pmod{\ell}$. Since $1+q+\cdots+q^{\ell-1}=\frac{q^\ell-1}{q-1}$, Fermat's Little Theorem implies our claim. If $q\equiv 1 \pmod{\ell}$, then q has the form $1+c\ell$, hence $1+q+\cdots+q^{\ell-1}=\ell(1+c\ell(\ldots))$, and since $v_\ell(1+c\ell(\ldots))=0$, then $v_\ell(1+q+\cdots+q^{\ell-1})=v_\ell(\ell)+v_\ell(1+c\ell(\ldots))=1$. $\square$

Let $K=\mathbb{Q}(\sqrt{t^2-4q})$, let d_K be the discriminant of K and let g_k be the conductor of the order $\mathbb{Z}[\phi^k]$. It is well known (see [2, pg. 134] for instance) that

$$t_k^2-4q^k=g_k^2 d_K.$$

Lemma 2. *Let E be ordinary and let $n=v_\ell(\#E(\mathbb{F}_q))\geq 1$. Let ϕ^k be the Frobenius endomorphism of E over $\mathbb{F}_{q^k}$ and let $\sigma_k=\sum_{i=0}^{k-1}\phi^i\widehat{\phi^{k-i-1}}$. Then*

i) $t_k^2 - 4q^k = (t^2 - 4q)\sigma_k^2$,
ii) $\sigma_k \equiv 1 + \cdots + q^{k-1} \pmod{\ell^n}$.

Proof. i) Clearly from (2) we have $t_k^2 - 4q^k = (\phi^k + \widehat{\phi^k})^2 - 4\phi^k\widehat{\phi^k} = (\phi^k - \widehat{\phi^k})^2 = (\phi - \widehat{\phi})^2(\widehat{\phi^{k-1}} + \phi\widehat{\phi^{k-2}} + \cdots + \phi^{k-2}\widehat{\phi} + \phi^{k-1})^2 = (t^2 - 4q)\sigma_k^2$.

ii) From the definition of σ_k, we have $\sigma_k = t\sigma_{k-1} - q\sigma_{k-2}$ for $k \geq 3$. Since $\sigma_1 = 1$ and $\sigma_2 \equiv 1 + q \pmod{\ell^n}$, $\sigma_k \equiv 1 + q + \cdots + q^{k-1} \pmod{\ell^n}$ follows by induction. □

Let f be the conductor of $\mathcal{O} = \mathrm{End}(E)$ in the ring of integers $\mathcal{O}_K$. From [5, 14] and [7] it follows that the smallest exponent r_k in $E[\ell^\infty](\mathbb{F}_{q^k}) \cong \mathbb{Z}/\ell^{r_k}\mathbb{Z} \times \mathbb{Z}/\ell^{s_k}\mathbb{Z}$ is

$$r_k = \begin{cases} \min\{\frac{1}{2}v_\ell(\#E(\mathbb{F}_{q^k})), v_\ell(\frac{g_k}{f})\} & \text{if } v_\ell(\#E(\mathbb{F}_{q^k})) \text{ is even,} \\ v_\ell(\frac{g_k}{f}) & \text{otherwise.} \end{cases} \tag{6}$$

Proposition 3. *Let $E[\ell^\infty](\mathbb{F}_q) \cong \mathbb{Z}/\ell^r\mathbb{Z} \times \mathbb{Z}/\ell^s\mathbb{Z}$ with $r \leq s$ and $n = r + s \geq 1$. For $\ell \geq 5$ we have:*

i) *if $q \not\equiv 1 \pmod{\ell}$ then $r = 0$ and $E[\ell^\infty](\mathbb{F}_{q^\ell}) \cong \mathbb{Z}/\ell^{n+1}\mathbb{Z}$,*
ii) *if $q \equiv 1 \pmod{\ell}$ then $E[\ell^\infty](\mathbb{F}_{q^\ell}) \cong \mathbb{Z}/\ell^{r+1}\mathbb{Z} \times \mathbb{Z}/\ell^{s+1}\mathbb{Z}$.*

For $\ell = 3$ the group structure variation is the same as above except if $q \equiv 1 \pmod{3}$ and $\#E(\mathbb{F}_q) \equiv 3 \pmod{9}$, in which case $E[3^\infty](\mathbb{F}_q) \cong \mathbb{Z}/3\mathbb{Z}$ and

$$E[3^\infty](\mathbb{F}_{q^3}) \cong \mathbb{Z}/3^{r_3}\mathbb{Z} \times \mathbb{Z}/3^{s_3}\mathbb{Z}$$

with $s_3 = r_3 \geq 2$ or $s_3 = r_3 + 1 \geq 3$.

Proof. i) Clearly Theorem 1 follows if both $E[\ell^\infty](\mathbb{F}_q)$, $E[\ell^\infty](\mathbb{F}_{q^\ell})$ are cyclic. If $(t, q) = 1$, then by [8] or [11] neither r nor r_ℓ exceed $v_\ell(q-1) = v_\ell(q^\ell - 1) = 0$, so both subgroups are cyclic. If $(t, q) \neq 1$, then $(t_\ell, q^\ell) \neq 1$ by the trace formula (3), and by [9] and [13] the only possibility is that both subgroups are cyclic.

ii) Let $(t, q) = 1$. Assume first $t^2 - 4q \equiv 0 \pmod{\ell^2}$. Since $t^2 - 4q = (q-1)^2 - 2(q+1)\#E(\mathbb{F}_q) + \#E(\mathbb{F}_q)^2$ and $v_\ell(q-1) \geq 1$, then $n \geq 2$. Hence by Lemma 2 $\sigma_\ell \equiv 1 + q + \cdots + q^{\ell-1} \pmod{\ell^n}$. Since $v_\ell(1 + q + \cdots + q^{\ell-1}) = 1$ by Lemma 1, we see $v_\ell(\sigma_\ell) = 1$. Therefore, again by Lemma 2 we have

$$v_\ell(t_\ell^2 - 4q^\ell) = v_\ell(t^2 - 4q) + 2, \tag{7}$$

which in terms of the conductors g_i is

$$v_\ell(g_\ell) = v_\ell(g_1) + 1. \tag{8}$$

In view of (6), it is easy to deduce $r_\ell = r + 1$ from Theorem 1 and (8). Then by Theorem 1 we conclude $s_\ell = s + 1$ as desired.
In case $t^2 - 4q \not\equiv 0 \pmod{\ell^2}$, (7) holds as well. Indeed, since $t^2 - 4q = (q-1)^2 - 2(q+1)\#E(\mathbb{F}_q) + \#E(\mathbb{F}_q)^2$ then $v_\ell(t^2 - 4q) = 1$ and $n = 1$. Then $v_\ell(\#E(\mathbb{F}_{q^\ell})) = 3$ by Theorem 1 and we deduce $v_\ell(t_\ell^2 - 4q^\ell) = 3$. At this point the proof is the same as above.

If $(t,q)\neq 1$, then as in i) above the only possibility is $E(\mathbb{F}_q)\cong(\mathbb{Z}/(\sqrt{q}\mp 1)\mathbb{Z})^2$ and $E(\mathbb{F}_{q^\ell})\cong(\mathbb{Z}/(\sqrt{q^\ell}\mp 1)\mathbb{Z})^2$ respectively. Then $v_\ell(\sqrt{q^\ell}\mp 1)=v_\ell(\sqrt{q}\mp 1)+1$ by Theorem 1.

Assume now $\ell=3$. If some of the conditions $q\equiv 1\pmod 3$, $\#E(\mathbb{F}_q)\equiv 3\pmod 9$ do not hold, then the proof follows as above. In the exceptional case, if $(t,q)\neq 1$ the result appears in [6, Table 1] for $t=\pm\sqrt{q}$. If $(t,q)=1$, by Theorem 1 we have two possibilities: $v_3(\#E(\mathbb{F}_{q^3}))=1+2c$ for $2\leq c\leq v_3(q-1)$ or else $v_3(\#E(\mathbb{F}_{q^3}))=2+2v_3(q-1)$ with $v_3(q-1)\geq 1$. In both cases one easily deduces $v_3(g_1)=v_3(f)=0$ and $v_3(d_K)=1$. In the first case, then $v_3((q^3-1)^2)>v_3(\#E(\mathbb{F}_{q^3}))$ by Lemma 1, and then $v_3(t_3^2-4q^3)=1+2c$. Therefore $v_3(g_3)=c$ and $r_3=v_3(g_3/f)=c$, $s_3=c+1$. In the second case, then $v_3((q^3-1)^2)=v_3(\#E(\mathbb{F}_{q^3}))$ and $v_3(t_3^2-4q^3)>v_3(\#E(\mathbb{F}_{q^3}))$. Thus $v_3(g_3/f)\geq v_3(q-1)+1$, and by (6), $r_3=1+v_3(q-1)$, hence $s_3=r_3$. $\square$

4. Increment of $v_\ell(\#E(\mathbb{F}_{q^d}))$ for $d=ord_{\mathbb{F}_\ell^*}(q)$

In this section $q\not\equiv 1\pmod\ell$ and k is equal to the multiplicative order d of q modulo ℓ. In this case, our problem for supersingular elliptic curves is solved in [6, Table 1] (where necessarily $d=2$ and $t=0$, $d=3$ and $t^2=q$, or $d=6$ and $t^2=3q$). Therefore we assume E is ordinary. Then by [8] or [11], $E[\ell^\infty](\mathbb{F}_q)$ is cyclic. We let $w_d=v_\ell(q^d-1)$.

Proposition 4. *Let E be ordinary, let $q\not\equiv 1\pmod\ell$ and let $n=v_\ell(\#E(\mathbb{F}_q))\geq 1$. If $E[\ell^\infty](\mathbb{F}_q)=\langle P_n\rangle$ then*

$$E[\ell^\infty](\mathbb{F}_{q^d})=\langle P_n,Q_\mu\rangle,$$

where $Q_\mu\in E(\mathbb{F}_{q^d})$ is a point of order ℓ^μ, $\mu\geq 1$. If $n>\mu$ then $\mu=w_d$.

Proof. It is well known that $E[\ell^\infty](\mathbb{F}_{q^d})$ has rank 2 (see [1, Theorem 1]). Let ℓ^μ be the order of a generator Q_μ of $E[\ell^\infty](\mathbb{F}_{q^d})$ independent of P_n.
We next show that P_n has the property that $\forall e<\ell$ there cannot exist $P\in E(\mathbb{F}_{q^e})$ such that $\ell P=P_n$. By Proposition 3, ℓ such points $P\in E(\overline{\mathbb{F}_q})$ do exist in $E(\mathbb{F}_{q^\ell})$. Assume there exists $T\in E(\mathbb{F}_{q^e})$ such that $\ell T=P_n$. By Proposition 2 we can assume $e=d$. Let $P_1=\ell^{n-1}P_n$ and let $Q_1=\ell^{\mu-1}Q_\mu$. Then $T=P+\alpha P_1+\beta Q_1$ for some integers α,β and clearly $\alpha P_1+\beta Q_1\in E(\mathbb{F}_{q^d})$. Hence $P\in E(\mathbb{F}_{q^\ell})\cap E(\mathbb{F}_{q^d})$ and therefore $\ell\mid d$, which is a contradiction.
Because of this property, if $n\leq\mu$ then P_n is a generator over $\mathbb{F}_{q^d}$. Indeed, the property above extends to the set $\{P_n+T_c\mid \ell^cT_c=0, c<n\}$ by elementary group theory, and this implies P_n is a generator of $E(\mathbb{F}_{q^d})$. If $n>\mu$, P_n is a generator over $\mathbb{F}_{q^d}$ by other reasons. We first show the precise order of Q_μ is given by $\mu=v_\ell(\sigma_d)$. Let f, g_i, d_K be as above. Since $t^2-4q=g_1^2d_K\not\equiv 0\pmod\ell$ then $v_\ell(f)=0$. Since $n>\mu$ then $\mu=v_\ell(g_d/f)$ in (6), and then $\mu=v_\ell(g_d)$. Similarly, since $t_d^2-4q^d=g_d^2d_K=g_1^2d_K\sigma_d^2$ by Lemma 2 and $v_\ell(g_1^2d_K)=0$, then $v_\ell(\sigma_d)=v_\ell(g_d)=\mu$. But also by Lemma 2 we have $\sigma_d\equiv 1+\cdots+q^{d-1}\pmod{\ell^n}$, and since $n>\mu$, we deduce $\mu=w_d$. Now Proposition 1 implies $v_\ell(\#E(\mathbb{F}_{q^d}))=n+w_d$, hence P_n and Q_{w_d} generate. $\square$

Theorem 2. *Let E be ordinary and let $q \not\equiv 1 \pmod{\ell}$.*

i) *If $w_d < v_\ell(\#E(\mathbb{F}_q))$ then $v_\ell(\#E(\mathbb{F}_{q^d})) = v_\ell(\#E(\mathbb{F}_q)) + w_d$.*
ii) *If $w_d = v_\ell(\#E(\mathbb{F}_q))$ then $v_\ell(\#E(\mathbb{F}_{q^d})) \geq 2v_\ell(\#E(\mathbb{F}_q))$.*
iii) *If $w_d > v_\ell(\#E(\mathbb{F}_q))$ then $v_\ell(\#E(\mathbb{F}_{q^d})) = 2v_\ell(\#E(\mathbb{F}_q))$.*

Proof. Let $n = v_\ell(\#E(\mathbb{F}_q))$. *i)* and *ii)* follow from Proposition 1. The same argument for *iii)* implies $v_\ell(\#E(\mathbb{F}_{q^d})) \geq 2n$. Assume $v_\ell(\#E(\mathbb{F}_{q^d})) = 2n + 1$. Then $t_d^2 - 4q^d = (q^d - 1)^2 + \#E(\mathbb{F}_{q^d})(\#E(\mathbb{F}_{q^d}) - 2(q^d + 1))$, therefore $v_\ell(t_d^2 - 4q^d) = 2n + 1$. But this is not possible: by Lemma 2, $v_\ell(t_d^2 - 4q^d) = v_\ell(t^2 - 4q) + 2v_\ell(\sigma_d) = 2v_\ell(\sigma_d)$ is even. Finally, by Proposition 4 we can assume $E[\ell^\infty](\mathbb{F}_{q^d}) = \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^{n+c}\mathbb{Z}$ with $c \geq 2$. Then $v_\ell(t_d^2 - 4q^d) \geq 2n+2$, hence $v_\ell(g_d) \geq n+1$ as in the proof of Proposition 4 above. But then, since $v_\ell(f) = 0$ the value of n contradicts (6). □

The structure of $E[\ell^\infty](\mathbb{F}_{q^d})$ now follows.

Corollary 1. *Let E be ordinary, let $q \not\equiv 1 \pmod{\ell}$, and let $E[\ell^\infty](\mathbb{F}_q) \cong \mathbb{Z}/\ell^n\mathbb{Z}$ with $n \geq 1$.*

i) *If $w_d < n$ then $E[\ell^\infty](\mathbb{F}_{q^d}) \cong \mathbb{Z}/\ell^{w_d}\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$.*
ii) *If $w_d = n$ then $E[\ell^\infty](\mathbb{F}_{q^d}) \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^{n'}\mathbb{Z}$ with $n' \geq n$.*
iii) *If $w_d > n$ then $E[\ell^\infty](\mathbb{F}_{q^d}) \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$.*

In the following example we illustrate *ii)* of Theorem 2 and Corollary 1.

Example 2. Let $q = p = 10^{10} + 19$, $\ell = 7$ and $d = 3$. Consider the elliptic curves

$$E_1 : y^2 = x^3 + 129113198x + 9741773623,$$
$$E_2 : y^2 = x^3 + 4800245152x + 399509715$$

over $\mathbb{F}_q$. For both of them $v_\ell(\#E_i(\mathbb{F}_q)) = w_d = 1$, but E_1 satisfies

$$v_\ell(\#E_1(\mathbb{F}_{q^d})) = 2 \quad \text{and} \quad E_1[\ell^\infty](\mathbb{F}_{q^d}) = \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z},$$

while E_2 satisfies

$$v_\ell(\#E_2(\mathbb{F}_{q^d})) = 5 \quad \text{and} \quad E_2[\ell^\infty](\mathbb{F}_{q^d}) = \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell^4\mathbb{Z}.$$

5. Conclusions

In this section we summarize our data for $\ell \geq 5$ and for an arbitrary degree k. As above, $n = v_\ell(\#E(\mathbb{F}_q))$, $w_d = v_\ell(q^d - 1)$ and we write the exponents of $E[\ell^\infty](\mathbb{F}_q)$ as (r, s) with $0 \leq r \leq s$ and $r + s \geq 1$. We set $k = m\ell^\tau d^\gamma$ with m a natural number prime to ℓ and d, and $\tau, \gamma \geq 0$. Our results relative to $\#E(\mathbb{F}_{q^k})$ are shown in Table 1. The case $k = \ell^\tau$ can be seen as a simple instance of Iwasawa Theory for function fields of elliptic curves over $\mathbb{F}_q$ and the $\mathbb{Z}_\ell$-extension $\cup_\tau \mathbb{F}_{q^{\ell^\tau}}$. In [12, Theorem 13.13 and pg. 130] one finds the prediction $v_\ell(\#E(\mathbb{F}_{q^{\ell^\tau}})) = \lambda\tau + \nu$ for τ sufficiently large, with $0 \leq \lambda \leq 2$ and ν a constant.

E ordinary		
Increment	Exponents	Condition
2τ	$(r+\tau, s+\tau)$	$q \equiv 1 \pmod{\ell}$
τ	$(0, n+\tau)$	$q \not\equiv 1 \pmod{\ell}$ and $\gamma = 0$
$2\tau + w_d$	$(w_d+\tau, n+\tau)$	$q \not\equiv 1 \pmod{\ell}$ and $w_d < n$ and $\gamma \geq 1$
$2\tau + n$	$(n+\tau, n+\tau)$	$q \not\equiv 1 \pmod{\ell}$ and $w_d > n$ and $\gamma \geq 1$
$\geq 2\tau + n$	$(n+\tau, \geq n+\tau)$	otherwise
E supersingular		
Increment	Exponents	Condition
2τ	$(r+\tau, s+\tau)$	$q \equiv 1 \pmod{\ell}$
τ	$(0, n+\tau)$	$q \not\equiv 1 \pmod{\ell}$ and $\gamma = 0$
$2\tau + n$	$(n+\tau, n+\tau)$	otherwise

TABLE 1. Increment and exponents over an extension of $\mathbb{F}_q$ of degree $k = m\ell^\tau d^\gamma$.

Acknowledgments

The authors would like to thank the anonymous referee, whose comments highly improved the quality of this publication. Research of the authors was supported in part by grants MTM2013-46949-P (Spanish Ministerio de Ciencia e Innovación), 2014SGR-1666 (Generalitat de Catalunya).

References

[1] R. Balasubramanian and N. Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes - Okamoto - Vanstone algorithm, *J. Cryptology*, 11 no. 2, pp. 141-145, 1998.

[2] D. A. Cox. *Primes of the form* $x^2 + ny^2$, Wiley-Interscience, 1989.

[3] D. Freeman and K. Lauter. Computing endomorphism rings of Jacobians of genus 2 curves over finite fields, Proceedings of the *First SAGA Conference*, World Sci. Publ., pp. 29-66, 2008.

[4] S. Ionica and A. Joux. Pairing the volcano, *Mathematics of Computation*, 82 no. 281, pp. 581-603, 2013.

[5] H. W. Lenstra, Jr. Complex multiplication structure of elliptic curves, *Journal of Number Theory*, 56 no. 2, pp. 227-241, 1996.

[6] A. J. Menezes, T. Okamoto and S. A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field, *IEEE Trans. Inform. Theory*, 39 no. 5, pp. 1639-1646, 1993.

[7] J. Miret, D. Sadornil, J. Tena, R. Tomàs and M. Valls. Volcanoes of ℓ-isogenies of elliptic curves over finite fields: the case $\ell = 3$, Proceedings of the *Primeras Jornadas de Teoría de Números*, Publicacions Matemàtiques, pp. 165-180, 2007.

[8] H.-G. Rück. A note on elliptic curves over finite fields, *Mathematics of Computation*, 49 no. 179, pp. 301-304, 1987.

[9] R. Schoof. Nonsingular plane cubic curves over finite fields, *Journal of Combinatorial Theory, Series A*, 46 no. 2, pp. 183-211, 1987.

[10] J. H. Silverman. *The Arithmetic of Elliptic Curves, Second Edition*, Graduate Texts in Mathematics 106, Springer, 2009.

[11] J. F. Voloch. A note on elliptic curves over finite fields, *Bulletin de la S.M.F.*, 116 no. 4, pp. 455-458, 1988.

[12] L. C. Washington. *Introduction to Cyclotomic Fields, Second Edition*, Graduate Texts in Mathematics 83, Springer, 1997.

[13] W. C. Waterhouse. Abelian varieties over finite fields, *Ann. Sci. École Norm. Sup. (4)*, 2 no. 4, pp. 521-560, 1969.

[14] C. Wittmann. Group structure of elliptic curves over finite fields, *Journal of Number Theory*, 88 no. 2, pp. 335-344, 2001.

Josep M. Miret Jordi Pujolàs Javier Valera
Departament de Matemàtica, Universitat de Lleida, 25001 Lleida, Spain
{miret, jpujolas, jvalera}@matematica.udl.cat