A note on factorisation patterns of division polynomials of elliptic curves over finite fields

By Josep M. Miret,[*] Daniel Sadornil,[**] Juan Tena[***] and Javier Valera[****]

(Communicated by Kenji Fukaya, m.j.a., Sept. 12, 2023)

Abstract: Let E be an elliptic curve defined over a finite field $\mathbf{F}_q$, $q = p^d$, $p > 3$, and a prime number $\ell > 3$ such that $q \equiv 1 \pmod{\ell}$ and $\ell \mid \#E(\mathbf{F}_q)$. In this paper we study the possible factorisation patterns over $\mathbf{F}_q[x]$ of the ℓ^k-division polynomials associated to E with $k \geq 2$, extending the work of Verdure [6] for $k = 1$.

Key words: Finite field; elliptic curve; division polynomial; factorisation pattern.

1. Introduction. Let $\mathbf{F}_q$ be a finite field with q elements and characteristic $p > 3$. Let E be an elliptic curve defined over $\mathbf{F}_q$ and $\ell > 3$ a prime number such that $\ell \neq p$. In [6], Verdure gave the possible factorisation patterns over $\mathbf{F}_q[x]$ of the ℓ-division polynomial $f_\ell(x)$ associated to E. Nevertheless, the patterns when the ℓ-torsion of the curve is defined over different extension fields were partially incorrect [4] and they have been corrected in [7].

In this paper we extend Verdure's work providing the possible factorisation patterns over $\mathbf{F}_q[x]$ of the ℓ^k-division polynomials with $k \geq 2$ for $q \equiv 1 \pmod{\ell}$ and $\ell \mid \#E(\mathbf{F}_q)$. In order to do this we distinguish when the ℓ-Sylow subgroup of $E/\mathbf{F}_q$ (that is, the points of $E(\mathbf{F}_q)$ whose order is a power of ℓ) is either cyclic or a rank-2 group. For a better understanding of this article, see [2, Section 3], where information about how the points of these subgroups are structured can be found.

The organization of the rest of the paper is as follows: Section 2 is devoted to introducing several concepts related to elliptic curves, among them, the division polynomials. In Section 3, we give for an ℓ^k-torsion point $P \in E(\mathbf{F}_{q^{\ell^e}})$, $e \geq 0$, the factorisation patterns of the polynomial whose roots are the abscissas of the ℓ-divisors points of P. Finally, in Section 4, the possible factorisation patterns of ℓ^k-division polynomials are presented, distinguishing when the ℓ-Sylow subgroup is either cyclic (Theorem 1) or a rank-2 group (Theorem 2).

2. Preliminaries. Let $\mathbf{F}_q$ a finite field of characteristic $p > 3$. We consider an elliptic curve E defined over $\mathbf{F}_q$ given by a Weierstrass equation

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbf{F}_q. \tag{1}$$

The set of $\mathbf{F}_q$-rational points of E is defined as

$$E(\mathbf{F}_q) = \{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q \mid (x, y) \text{ satisfies (1)}\} \cup \{\mathcal{O}\}$$

where $\mathcal{O}$ is the point at infinity of E. This set is endowed with an addition operation [5, Chapter III] whose neutral element is $\mathcal{O}$, under which it forms a finite abelian group. For the sake of simplicity, we will denote $E(\overline{\mathbf{F}_q})$ by E.

The order of a point $P \in E$, denoted by $\mathrm{ord}(P)$, is the smallest positive integer m such that $mP = \mathcal{O}$.

The m-torsion subgroup, $m > 0$, is defined as

$$E[m] = \{P \in E \mid mP = \mathcal{O}\}.$$

Associated to this group one has the m-division polynomials $\psi_m(x, y)$. Such polynomials are defined [1, Chaper III] in a recursive way (for simplicity we will write ψ_m instead of $\psi_m(x, y)$):

$$\begin{aligned}
&\psi_1 = 1, \quad \psi_2 = 2y,\\
&\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2,\\
&\psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx\\
&\qquad - 8b^2 - a^3),\\
&\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3, \quad n \geq 2,
\end{aligned}$$

2020 Mathematics Subject Classification. Primary 11T06, 14H52.

[*] Departament de Matemàtica, Universitat de Lleida, Jaume II, 69, 25001-Lleida, Spain.
[**] Departamento de Matemáticas, Estadística y Computación, Universidad de Cantabria, Avda. Los Castros s/n, 39005-Santander, Spain.
[***] IMUVA, Universidad de Valladolid, Paseo de Belén s/n, 47011-Valladolid, Spain.
[****] Eurecat, Centre Tecnològic de Catalunya, Unitat IT & OT Security, PCiTAL, Ed. H3, 25003-Lleida, Spain.

doi: 10.3792/pjaa.99.011

$$\psi_{2n} = \frac{(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)\psi_n}{\psi_2}, \quad n > 2.$$

Let $P \in E \setminus \{\mathcal{O}\}$. Then $P \in E[m]$ if and only if $\psi_m(x(P), y(P)) = 0$, being $x(P)$ and $y(P)$, respectively, the abscissa and the ordinate of P. The polynomials $\psi_m(x, y)$ fulfill the following properties:

- If m is even, $\psi_m(x, y)$ is the product of $\psi_2(x, y)$ and a polynomial in x.
- If m is odd, $\psi_m(x, y)$ modulo the equation of the elliptic curve is a polynomial in x.

Therefore, working modulo the equation of the elliptic curve, one can define the polynomials in x:

$$f_m(x) = \begin{cases} \psi_m(x, y) & \text{if } m \text{ is odd,} \\ \dfrac{\psi_m(x, y)}{\psi_2(x, y)} & \text{if } m \text{ is even.} \end{cases}$$

If m is odd and $p \nmid m$, then $f_m(x)$ has degree $\frac{m^2-1}{2}$.

The Frobenius endomorphism of E over $\overline{\mathbf{F}_q}$ is defined as

$$\begin{aligned} &\phi : E \to E \\ &(x, y) \mapsto (x^q, y^q). \end{aligned}$$

For a point $P \in E$, we have $P \in E(\mathbf{F}_{q^i})$, $i \geq 1$, if and only if $\phi^i(P) = P$.

Let $\ell > 3$ be a prime such that $q \equiv 1 \pmod{\ell}$ and $\ell \mid \#E(\mathbf{F}_q)$. Let $P, Q \in E$. Then Q is an ℓ-divisor of P if and only if $\ell Q = P$. If Q is an ℓ-divisor of P, then the ℓ-divisors of P are the points of $Q + E[\ell]$, obtaining a total of ℓ^2, since $E[\ell]$ is generated by two linearly independent points of order ℓ (see [5, Chapter III, Corollary 6.4 (b)]). Besides, if $Q \in E(\mathbf{F}_{q^i})$, then it is said that Q ℓ-divides P in $E(\mathbf{F}_{q^i})$.

The ℓ-Sylow subgroup of E over $\mathbf{F}_q$ is defined as

$$E[\ell^\infty](\mathbf{F}_q) = \{P \in E(\mathbf{F}_q) \mid \operatorname{ord}(P) = \ell^e \text{ for some } e\}.$$

This subgroup, if not trivial, is isomorphic to either a cyclic group $\mathbf{Z}/\ell^n\mathbf{Z}$, $n \geq 1$, or a rank-2 group $\mathbf{Z}/\ell^n\mathbf{Z} \times \mathbf{Z}/\ell^r\mathbf{Z}$, $n \geq r \geq 1$.

Given a polynomial over $\mathbf{F}_q[x]$, its factorisation pattern will be expressed as

$$((a_1, b_1), (a_2, b_2), \ldots, (a_m, b_m)),$$

where each (a_i, b_i) indicates that there are b_i irreducible polynomials over $\mathbf{F}_q[x]$ of degree a_i.

3. ℓ-divisor points. First of all, we determine the extension field where the ℓ-divisors points of an ℓ^k-torsion point are defined.

Lemma 1. *Let $P \in E(\mathbf{F}_{q^{\ell^e}})$, $e \geq 0$, such that $\operatorname{ord}(P) = \ell^k$, $k > 0$, and $P \notin E(\mathbf{F}_{q^{\ell^{e-1}}})$ if $e > 0$. Let*

$$S = \{Q \in E \mid \ell Q = P\}.$$

(1) *The case where $E[\ell](\mathbf{F}_q)$ is cyclic:*
If $e = 0$, then either ℓ points of S belong to $E(\mathbf{F}_q)$ and the rest belong to $E(\mathbf{F}_{q^\ell}) \setminus E(\mathbf{F}_q)$ or all of them belong to $E(\mathbf{F}_{q^\ell}) \setminus E(\mathbf{F}_q)$. If $e > 0$, then either all the points of S belong to $E(\mathbf{F}_{q^{\ell^e}}) \setminus E(\mathbf{F}_{q^{\ell^{e-1}}})$ or all of them belong to $E(\mathbf{F}_{q^{\ell^{e+1}}}) \setminus E(\mathbf{F}_{q^{\ell^e}})$.

(2) *The case where $E[\ell](\mathbf{F}_q)$ is not cyclic:*
If $e = 0$, then either all the points of S belong to $E(\mathbf{F}_q)$ or all of them belong to $E(\mathbf{F}_{q^\ell}) \setminus E(\mathbf{F}_q)$. If $e > 0$, then either all the points of S belong to $E(\mathbf{F}_{q^{\ell^e}}) \setminus E(\mathbf{F}_{q^{\ell^{e-1}}})$ or all of them belong to $E(\mathbf{F}_{q^{\ell^{e+1}}}) \setminus E(\mathbf{F}_{q^{\ell^e}})$.

Proof. First we show the case (1). Let $E[\ell] = \langle W_1, W_2 \rangle$ with $W_1 \in E(\mathbf{F}_q)$. The action of ϕ over $E[\ell]$ is given by the following matrix of $GL(2, \mathbf{F}_\ell)$ (see [6, Lemma 1]):

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Therefore, $\phi^i(W_2) = iW_1 + W_2$. Hence $W_2 \in E(\mathbf{F}_{q^\ell}) \setminus E(\mathbf{F}_q)$. Let $Q \in E$ such that $\ell Q = P$. Then

$$S = \{Q + i_1W_1 + i_2W_2 \mid i_1, i_2 \in \mathbf{F}_\ell\}.$$

Each of these points is defined over an extension of degree i of $\mathbf{F}_{q^{\ell^e}}$. In order to know the value of i for each point we must check when $\phi^{i\ell^e}(Q + i_1W_1 + i_2W_2) = Q + i_1W_1 + i_2W_2$. The point $\phi^{\ell^e}(Q) - Q$ is an ℓ-torsion point since

$$\ell(\phi^{\ell^e}(Q) - Q) = \phi^{\ell^e}(\ell Q) - \ell Q = P - P = \mathcal{O}.$$

Hence $\phi^{\ell^e}(Q) = Q + j_1W_1 + j_2W_2$ for certain values $j_1, j_2 \in \mathbf{F}_\ell$. Then, for $e = 0$,

$$\begin{aligned} \phi^i(Q + i_1W_1 + i_2W_2) = Q + \Big(&i_1 + ij_1 + ii_2 \\ &+ \binom{i}{2} j_2\Big)W_1 + (i_2 + ij_2)W_2, \end{aligned}$$

and for $e > 0$,

$$\begin{aligned} &\phi^{i\ell^e}(Q + i_1W_1 + i_2W_2) \\ &\quad = Q + (i_1 + ij_1)W_1 + (i_2 + ij_2)W_2. \end{aligned}$$

In the first case, $e = 0$, we have that if $j_2 = 0$, then ℓ points belong to $E(\mathbf{F}_q)$ and $\ell(\ell - 1)$ points belong to $E(\mathbf{F}_{q^\ell}) \setminus E(\mathbf{F}_q)$. If $j_2 \neq 0$, then the ℓ^2 points belong to $E(\mathbf{F}_{q^\ell}) \setminus E(\mathbf{F}_q)$. In the second case, $e > 0$, if $j_1 = j_2 = 0$, then the ℓ^2 points belong to $E(\mathbf{F}_{q^{\ell^e}}) \setminus$

$E(\mathbf{F}_{q^{\ell^{e-1}}})$. For the remaining cases, we derive that the ℓ^2 points belong to $E(\mathbf{F}_{q^{\ell^{e+1}}}) \setminus E(\mathbf{F}_{q^{\ell^e}})$.

Case (2) is similar to case (1) when $e > 0$ since $\phi(W_2) = W_2$. □

Let $P \in E$ such that $\mathrm{ord}(P) = \ell^k$ with $k > 0$ and let $S = \{Q \in E \mid \ell Q = P\}$. Note that the abscissas of the points of S are defined over the same field, since ℓ is an odd prime. Associated to P we define the following polynomial:

$$\tau_P(x) = \prod_{Q \in S} (x - x(Q)).$$

The degree of this polynomial is ℓ^2.

Proposition 1. *Let $P \in E(\mathbf{F}_{q^{\ell^e}})$, $e \geq 0$, such that $\mathrm{ord}(P) = \ell^k$, $k > 0$, and $P \notin E(\mathbf{F}_{q^{\ell^{e-1}}})$ if $e > 0$. The possible factorisation patterns over $\mathbf{F}_{q^{\ell^e}}[x]$ of $\tau_P(x)$ are*:

(1) *The case where $E[\ell](\mathbf{F}_q)$ is cyclic*:
  (a) $e = 0$:
    (i) $((1, \ell), (\ell, \ell - 1))$;
    (ii) $((\ell, \ell))$.
  (b) $e > 0$:
    (i) $((1, \ell^2))$;
    (ii) $((\ell, \ell))$.

(2) *The case where $E[\ell](\mathbf{F}_q)$ is not cyclic*:
  (a) $((1, \ell^2))$;
  (b) $((\ell, \ell))$.

Proof. From Lemma 1 a point $Q \in E$ such that $\ell Q = P$ is defined either over the same field as P or over an extension of degree ℓ where P belongs. The first case is trivial since we have that $x - x(Q)$ is a factor of degree 1. Consider now the case where the points $Q \in S$ are not defined over the same field as P. Let $R = Q + i_1 W_1 + i_2 W_2$ and let $g(x) = \prod_{i=1}^{\ell}(x - x(\phi^{i\ell^e}(R)))$. According to Lemma 1, we know $\ell\phi^{i\ell^e}(R) = P$, that is, $g(x) \mid \tau_P(x)$. Therefore, it is only needed to show that $g(x)$ belongs to $\mathbf{F}_{q^{\ell^e}}[x]$ and it is an irreducible polynomial. The first part is clear since $\phi^{\ell^e}(g(x)) = g(x)$. Moreover, if $g(x)$ were not irreducible, then it would have a factor $g_1(x) \in \mathbf{F}_{q^{\ell^e}}[x]$ of degree less than ℓ. However, in this case, a point $Q \in S$ would exist in a smaller extension than Lemma 1 affirms. From this the claim follows. □

Lemma 2. *Let $P \in E(\mathbf{F}_{q^{\ell^e}}) \setminus E(\mathbf{F}_{q^{\ell^{e-1}}})$, $e > 0$, such that $\mathrm{ord}(P) = \ell^k$, $k > 0$, and let $P_i = \phi^i(P)$ for some integer $0 < i < \ell^e$. Then the factorisation pattern over $\mathbf{F}_{q^{\ell^e}}[x]$ of $\tau_{P_i}(x)$ is the same as that of $\tau_P(x)$.*

Proof. If $Q \in E$ such that $\ell Q = P$, then the roots of $\tau_{P_i}(x)$ are the abscissas of the points of $S_i = \{\phi^i(Q) + i_1 W_1 + i_2 W_2 \mid i_1, i_2 \in \mathbf{F}_\ell\}$, with W_1, W_2 a basis of the ℓ-torsion subgroup. Note that

$$\begin{aligned}\phi^{j\ell^e}(\phi^i(Q) + i_1 W_1 + i_2 W_2) &= \phi^i(\phi^{j\ell^e}(Q)) + i_1 W_1 + i_2 W_2 \\ &= \phi^i(Q) + (i_1 + jj_1) W_1 + i_2 W_2 + jj_2 \phi^i(W_2),\end{aligned}$$

being $\phi^{\ell^e}(Q) = Q + j_1 W_1 + j_2 W_2$. If $\phi(W_2) = W_2$, then $\phi^{j\ell^e}(\phi^i(Q) + i_1 W_1 + i_2 W_2) = \phi^i(Q) + (i_1 + jj_1) W_1 + (i_2 + jj_2) W_2$. If $\phi^i(W_2) = iW_1 + W_2$, then $\phi^{j\ell^e}(\phi^i(Q) + i_1 W_1 + i_2 W_2) = \phi^i(Q) + (i_1 + jj_1 + ijj_2) W_1 + (i_2 + jj_2) W_2$. In both cases, from the proof of Lemma 1, it is easy to see that the points of S_i belong to the same extension as the points of S. Then, the result follows from the proof of Proposition 1. □

Since we want to describe the factorisation patterns of the ℓ^k-division polynomial over $\mathbf{F}_q$ we must merge $\tau_{P_0}(x), \tau_{P_1}(x), \ldots, \tau_{P_{\ell^e-1}}(x)$ all together when $e > 0$. The case $e = 0$ is included in Proposition 1.

Proposition 2. *Let $P_0 \in E(\mathbf{F}_{q^{\ell^e}}) \setminus E(\mathbf{F}_{q^{\ell^{e-1}}})$, $e > 0$, such that $\mathrm{ord}(P_0) = \ell^k$, $k > 0$, let $P_i = \phi^i(P_0)$, $0 < i < \ell^e$, and let*

$$g(x) = \tau_{P_0}(x)\tau_{P_1}(x) \cdots \tau_{P_{\ell^e-1}}(x).$$

The possible factorisation patterns over $\mathbf{F}_q[x]$ of $g(x)$ are:

(1) $((\ell^e, \ell^2))$;
(2) $((\ell^{e+1}, \ell))$.

Proof. From Proposition 1, $\tau_{P_0}(x)$ factorizes over $\mathbf{F}_{q^{\ell^e}}[x]$ as follows:

$$h_{0,1}(x) h_{0,2}(x) \cdots h_{0,n}(x)$$

with either $n = \ell^2$ and $\deg(h_{0,i}(x)) = 1$ or $n = \ell$ and $\deg(h_{0,i}(x)) = \ell$. Let $x(Q_i)$ a root of $h_{0,i}(x)$ with $Q_i \in E$ such that $\ell Q_i = P_0$. Since $h_{0,i}(x)$ is irreducible over $\mathbf{F}_{q^{\ell^e}}[x]$ then either

$$h_{0,i}(x) = x - x(Q_i)$$

or

$$\begin{aligned}h_{0,i}(x) = (x - x(Q_i))(x - x(\phi^{\ell^e}(Q_i))) \cdots \\ \cdots (x - x(\phi^{(\ell-1)\ell^e}(Q_i))).\end{aligned}$$

From Lemma 2, for $0 < j < \ell^e$, we have over $\mathbf{F}_{q^{\ell^e}}[x]$ the factorisation

$$\tau_{P_j}(x) = h_{j,1}(x) h_{j,2}(x) \cdots h_{j,n}(x),$$

where $x(\phi^j(Q_i))$ is a root of $h_{j,i}(x)$. We can order the factors properly such that if $h_{j,i}(x)$ is a linear

polynomial then

$$h_{j,i}(x) = x - x(\phi^j(Q_i)).$$

Otherwise

$$h_{j,i}(x) = (x - x(\phi^j(Q_i)))(x - x(\phi^{\ell^e}(\phi^j(Q_i)))) \cdots \cdots (x - x(\phi^{(\ell-1)\ell^e}(\phi^j(Q_i)))).$$

Now we define, for $j = 1, \ldots, \ell^e$,

$$H_j(x) = \Pi_{i=0}^{\ell^e - 1} h_{i,j}(x).$$

We need to show for all j that $H_j(x) \in \mathbf{F}_q[x]$ and it is irreducible. If $h_{0,j}(x)$ is a linear polynomial, then the roots of $H_j(x)$ are $x(\phi^i(Q_j))$ with $0 \le i \le \ell^e - 1$. Thus, the roots of $\phi(H_j(x))$ are $x(\phi^{i+1}(Q_j))$, with $0 \le i \le \ell^e - 1$. Since $h_{0,j}(x)$ is linear then $\phi^{\ell^e}(Q_j) = Q_j$. Otherwise, if $h_{0,j}(x)$ has degree ℓ, then the roots of $H_j(x)$ are $x(\phi^i(Q_j))$ with $0 \le i \le \ell^{e+1} - 1$ and the roots of $\phi(H_j(x))$ are the same, since in this case $\phi^{\ell^{e+1}}(Q_j) = Q_j$. In both cases, $H_j(x)$ and $\phi(H_j(x))$ are polynomials with the same roots, hence $\phi(H_j(x)) = H_j(x)$ and $H_j(x) \in \mathbf{F}_q[x]$. Moreover, as in the proof of Proposition 1, if any $H_j(x)$ was reducible, then some of the points P_i or Q_i would be defined over a smaller extension of $\mathbf{F}_q$, which is a contradiction. □

The polynomial $\tau_P(x)$ determines the definition field of the points Q such that $\ell Q = P$. So, if $\tau_P(x)$ has a linear factor, then P ℓ-divides over the same field. Lemma 2 shows that ℓ-division is invariant under the Frobenius endomorphism.

The following result from [2, Proposition 3.3] shows that not all ℓ^k-torsion points are ℓ-divisible when the ℓ-torsion subgroup is not cyclic. Note that if the ℓ-torsion subgroup is cyclic, then ℓ-division can be computed for any point of ℓ^k-torsion until k reaches the structure of the group.

Proposition 3. *Let* $P \in E(\mathbf{F}_{q^{\ell^e}}) \setminus E(\mathbf{F}_{q^{\ell^{e-1}}})$, $e > 0$, *such that* $\mathrm{ord}(P) = \ell^k$, $k > e$. *Let* $E[\ell^\infty](\mathbf{F}_{q^{\ell^e}}) \simeq \mathbf{Z}/\ell^r\mathbf{Z} \times \mathbf{Z}/\ell^s\mathbf{Z}$, $s > 0$, $r > s + 1$. *Assume* $r > k > s$. *Assume also that there exists a point* $P' \in E(\mathbf{F}_{q^{\ell^{e-1}}})$ *such that* $\mathrm{ord}(P') = \ell^k$ *and* P' ℓ-*divides in* $E(\mathbf{F}_{q^{\ell^e}})$. *Then* P *does not* ℓ-*divide in* $E(\mathbf{F}_{q^{\ell^e}})$.

4. Factorisation patterns. Now, with the preceding results, we can determine the factorisation of the ℓ^k-division polynomials, $k \ge 2$, over $\mathbf{F}_q[x]$. For $k = 1$, when $q \equiv 1 \pmod{\ell}$ and $\ell \mid \#E(\mathbf{F}_q)$, Verdure proved [6, Propositions 1 and 2] the factorisation patterns are:

$$\begin{cases} \left(\left(1, \dfrac{\ell^2 - 1}{2}\right)\right) & \text{if } E[\ell] \subset E(\mathbf{F}_q), \\ \left(\left(1, \dfrac{\ell - 1}{2}\right), \left(\ell, \dfrac{\ell - 1}{2}\right)\right) & \text{if } E[\ell] \not\subset E(\mathbf{F}_q). \end{cases}$$

In this section, we give the factorisation patterns of the polynomials $f_{\ell^k}(x)/f_{\ell^{k-1}}(x)$, whose roots are exactly the abcissas of the points with order exactly ℓ^k, distinguishing when the ℓ-Sylow subgroup of $E/\mathbf{F}_q$ is either cyclic or a rank-2 group.

4.1. Cyclic case. Throughout this section, let

$$\lambda = \frac{\ell - 1}{2}, \quad \alpha = \lambda\ell^{k-1} \quad \text{and} \quad \beta = \lambda(\ell - 1)\ell^{k-2}.$$

Theorem 1. *Let* $E[\ell^\infty](\mathbf{F}_q) \simeq \mathbf{Z}/\ell^n\mathbf{Z}$ *with* $n \ge 1$. *The possible factorisation patterns over* $\mathbf{F}_q[x]$ *of* $f_{\ell^k}(x)/f_{\ell^{k-1}}(x)$ *for* $k \ge 2$ *are*:

(1) $n = 1$:

$$((\ell^{k-1}, \alpha), (\ell^k, \alpha)).$$

(2) $n > 1$:

(a) $k \le n$:

$$((1, \alpha), (\ell, \beta), (\ell^2, \beta), \ldots, (\ell^{k-1}, \beta), (\ell^k, \alpha)),$$

(b) $k > n$:

$$((\ell^{k-n}, \alpha), (\ell^{k-n+1}, \beta), (\ell^{k-n+2}, \beta), \ldots, (\ell^{k-1}, \beta), (\ell^k, \alpha)).$$

Proof. From [6, Proposition 2], the factorisation pattern over $\mathbf{F}_q[x]$ of $f_\ell(x)$ is

$$((1, \lambda), (\ell, \lambda)).$$

Case (1). Let $k = 2$. Since in $E(\mathbf{F}_q)$ there are no points of order ℓ^2, by using Proposition 1 (1)(a)(ii), from $(1, \lambda)$ we get $(\ell, \lambda\ell)$. From [3, Proposition 3 (ii)],

$$E[\ell^\infty](\mathbf{F}_{q^\ell}) \simeq \mathbf{Z}/\ell^2\mathbf{Z} \times \mathbf{Z}/\ell\mathbf{Z}.$$

Hence, not every ℓ-torsion point ℓ-divides in $E(\mathbf{F}_{q^\ell})$. Therefore, by Proposition 2 (2), from (ℓ, λ) we get $(\ell^2, \lambda\ell)$. Assume, now, the factorisation pattern is true for $k \ge 2$, that is,

$$((\ell^{k-1}, \alpha), (\ell^k, \alpha)).$$

Next we will see it is also true for $k + 1$. As above, we have that

$$E[\ell^\infty](\mathbf{F}_{q^{\ell^h}}) \simeq \mathbf{Z}/\ell^{h+1}\mathbf{Z} \times \mathbf{Z}/\ell^h\mathbf{Z},$$

with $h > 1$, and in $E(\mathbf{F}_{q^{\ell^{k-1}}})$ there are no points of order ℓ^{k+1}. By Proposition 2 (2), as in the case

$k=2$, from (ℓ^{k-1},α) and (ℓ^k,α) we get $(\ell^k,\alpha\ell)$ and $(\ell^{k+1},\alpha\ell)$.

Case (2)(a). Let $k=2$. Since $E[\ell^\infty](\mathbf{F}_q)\simeq \mathbf{Z}/\ell^n\mathbf{Z}$ with $n\geq 1$, in $E(\mathbf{F}_q)$ there is a total of $2\lambda\ell$ points of order ℓ^2. Then we must consider Proposition 1 (1)(a)(i), so from $(1,\lambda)$ we get $(1,\lambda\ell)$ and $(\ell,\lambda(\ell-1))$. Now, by using again [3, Proposition 3 (ii)],

$$E[\ell^\infty](\mathbf{F}_{q^\ell})\simeq \mathbf{Z}/\ell^{n+1}\mathbf{Z}\times\mathbf{Z}/\ell\mathbf{Z}.$$

Therefore, by using Proposition 2 (2), from (ℓ,λ) we get $(\ell^2,\lambda\ell)$. Assume, now, the factorisation pattern is true for $2\leq k<n$:

$$((1,\alpha),(\ell,\beta),(\ell^2,\beta),\dots,(\ell^{k-1},\beta),(\ell^k,\alpha)).$$

Next we will see it is also true for $k+1$. Indeed, in $E(\mathbf{F}_q)$ there is a total of $2\lambda\ell^k$ points of order ℓ^{k+1} and, by using Proposition 1 (1)(a)(i), from $(1,\alpha)$ we get $(1,\alpha\ell)$ and $(\ell,\alpha(\ell-1))$. From [3, Proposition 3 (ii)] we have that

$$(2)\qquad E[\ell^\infty](\mathbf{F}_{q^{\ell^e}})\simeq \mathbf{Z}/\ell^{n+e}\mathbf{Z}\times\mathbf{Z}/\ell^e\mathbf{Z},\ e\geq 1.$$

Taking this into account and the factorization pattern for k, the points of order ℓ^k which are included in (ℓ^e,β) do not ℓ-divide in $E(F_{q^{\ell^e}})$ from Proposition 3. Therefore, by Proposition 2 (2), from (ℓ^e,β) we get $(\ell^{e+1},\beta\ell)$. Moreover, taking account of the number of ℓ^k-torsion points in $E[\ell^\infty](\mathbf{F}_{q^{\ell^k}})$, by Proposition 2 (2), from (ℓ^k,α) we get $(\ell^{k+1},\alpha\ell)$.

Case (2)(b). From above, the factorisation pattern for $k=n$ is

$$((1,\alpha),(\ell,\beta),(\ell^2,\beta),\dots,(\ell^{n-1},\beta),(\ell^n,\alpha)).$$

Let $k=n+1$. Since in $E(\mathbf{F}_q)$ there are no points of order ℓ^{n+1}, by using Proposition 1 (1)(a)(ii), from $(1,\alpha)$ we get $(\ell,\alpha\ell)$. Therefore, in $E(\mathbf{F}_q)$ there are points of order ℓ^n which ℓ-divide in $E(\mathbf{F}_{q^\ell})$. As before, the structure of $E[\ell^\infty](\mathbf{F}_{q^{\ell^e}})$ is given by (2) and the points of order ℓ^n which are included in (ℓ^e,β), from Proposition 3, do not ℓ-divide in $E(\mathbf{F}_{q^{\ell^e}})$, that is, they have no ℓ-divisors in this extension. Therefore, by using Proposition 2 (2), from (ℓ^e,β) we get $(\ell^{e+1},\beta\ell)$. As in the previous cases, from (ℓ^n,α) we get $(\ell^{n+1},\alpha\ell)$. The remaining cases are similar and the result follows. □

Example 1. Let E be the elliptic curve defined over $\mathbf{F}_{101}$ by

$$y^2=x^3+x+99.$$

For $\ell=5$, we get $E[5^\infty](\mathbf{F}_{101})\simeq\mathbf{Z}/5^2\mathbf{Z}$. Then, for $k=2$, we have $\alpha=10$, $\beta=8$ and the factorisation pattern over $\mathbf{F}_{101}[x]$ of $f_{5^2}(x)/f_5(x)$ is

$$((1,10),(5,8),(25,10)).$$

4.2. Non cyclic case. Throughout this section, let

$$\lambda=\frac{\ell-1}{2},\quad \alpha=\lambda\ell^{k+s-1}\quad\text{and}\quad \beta=\lambda(\ell-1)\ell^{k+s-2}.$$

Theorem 2. *Let* $E[\ell^\infty](\mathbf{F}_q)\simeq\mathbf{Z}/\ell^r\mathbf{Z}\times\mathbf{Z}/\ell^s\mathbf{Z}$ *with* $r\geq s\geq 1$. *The possible factorisation patterns over* $\mathbf{F}_q[x]$ *of* $f_{\ell^k}(x)/f_{\ell^{k-1}}(x)$ *for* $k\geq 2$ *are*:

(1) $r=s$:
  (a) $k\leq s$:
  $$((1,\lambda(\ell+1)\ell^{2(k-1)})),$$
  (b) $k>s$:
  $$((\ell^{k-s},\lambda(\ell+1)\ell^{k+s-2})).$$

(2) $r=s+1$:
  (a) $k\leq s$:
  $$((1,\lambda(\ell+1)\ell^{2(k-1)})),$$
  (b) $k>s$:
  $$((\ell^{k-s-1},\alpha),(\ell^{k-s},\alpha)).$$

(3) $r>s+1$:
  (a) $k\leq s$:
  $$((1,\lambda(\ell+1)\ell^{2(k-1)})),$$
  (b) $k=s+1$:
  $$((1,\lambda\ell^{2s}),(\ell,\lambda\ell^{2s})),$$
  (c) $s+1<k\leq r$:
  $$((1,\alpha),(\ell,\beta),(\ell^2,\beta),\dots,(\ell^{k-s-1},\beta),(\ell^{k-s},\alpha)),$$
  (d) $k>r$:
  $$((\ell^{k-r},\alpha),(\ell^{k-r+1},\beta),(\ell^{k-r+2},\beta),\dots,(\ell^{k-s-1},\beta),(\ell^{k-s},\alpha)).$$

Proof. Since the three cases are similar, we only consider the third one that involves all possible options.

Case (3)(a). The structure of the group $E[\ell^\infty](\mathbf{F}_q)$ shows that all points of order ℓ^k, in total $2\lambda(\ell+1)\ell^{2(k-1)}$, are $\mathbf{F}_q$-rational. In this case, the factorisation pattern is clearly

$$((1, \lambda(\ell+1)\ell^{2(k-1)})).$$

Case (3)(b). The group $E[\ell^\infty](\mathbf{F}_q)$ has $2\lambda(\ell+1)\ell^{2(s-1)}$ points of order ℓ^s, but there are only $2\lambda\ell^{2(s-1)}$ points which ℓ-divide in $E(\mathbf{F}_q)$. The rest of the ℓ^s-torsion points, in total $2\lambda\ell^{2s-1}$, from Lemma 1 (2), ℓ-divide in $E(\mathbf{F}_{q^\ell})$. So, the factorisation pattern is

$$((1, \lambda\ell^{2s}), (\ell, \lambda\ell^{2s})).$$

Case (3)(c). Let $k = s+2$. As the previous cases, not all the ℓ^{s+1}-torsion points defined over $\mathbf{F}_q$ ℓ-divide in $E(\mathbf{F}_q)$. There are only $2\lambda\ell^{2s-1}$ which ℓ-divide. The remaining ℓ^{s+1}-torsion points, in total $2\lambda(\ell-1)\ell^{2s-1}$, from Lemma 1 (2), ℓ-divide in $E(\mathbf{F}_{q^\ell})$. Therefore, from $(1, \lambda\ell^{2s})$ we get $(1, \lambda\ell^{2s+1})$ and $(\ell, \lambda(\ell-1)\ell^{2s})$. From [3, Proposition 3 (ii)], over an extension of degree ℓ we have

$$E[\ell^\infty](\mathbf{F}_{q^\ell}) \simeq \mathbf{Z}/\ell^{r+1}\mathbf{Z} \times \mathbf{Z}/\ell^{s+1}\mathbf{Z}.$$

Hence, by using Proposition 2 (2), from $(\ell, \lambda\ell^{2s})$ we get $(\ell^2, \lambda\ell^{2s+1})$. Assume, now, the factorisation pattern is true for $s+2 \le k < r$:

$$((1,\alpha), (\ell,\beta), (\ell^2,\beta), \dots, (\ell^{k-s-1},\beta), (\ell^{k-s},\alpha)).$$

Next, we will see that it is also true for $k+1$. As above, among the $2\lambda\ell^{k+s-1}$ $\mathbf{F}_q$-rational points of order ℓ^k, there are $2\lambda\ell^{k+s-2}$ points which ℓ-divide in $E(\mathbf{F}_q)$ and $2\lambda(\ell-1)\ell^{k+s-2}$ points which ℓ-divide in $E(\mathbf{F}_{q^\ell})$ from Lemma 1 (2). Therefore, from $(1,\alpha)$ we get $(1,\alpha\ell)$ and $(\ell,\beta\ell)$. Now, over extensions of degree ℓ^e, $e \ge 1$, we have

$$E[\ell^\infty](\mathbf{F}_{q^{\ell^e}}) \simeq \mathbf{Z}/\ell^{r+e}\mathbf{Z} \times \mathbf{Z}/\ell^{s+e}\mathbf{Z}. \tag{3}$$

If $e \le k-s-1$, then the points of order ℓ^k included in (ℓ^e,β), from Proposition 3, do not ℓ-divide in $E(\mathbf{F}_{q^{\ell^e}})$. Therefore, by Proposition 2 (2), from (ℓ^e,β) we get $(\ell^{e+1},\beta\ell)$. If $e = k-s$, then on the short branches of $E[\ell^\infty](\mathbf{F}_{q^{\ell^{k-s}}})$ there are no points of order ℓ^{k+1}. Therefore, again by Proposition 2 (2), from (ℓ^{k-s},α) we get $(\ell^{k-s+1},\alpha\ell)$.

Case (3)(d). The factorisation pattern for $k = r$ is

$$((1,\alpha), (\ell,\beta), (\ell^2,\beta), \dots, (\ell^{r-s-1},\beta), (\ell^{r-s},\alpha)).$$

Let $k = r+1$. In $E(\mathbf{F}_q)$ there are no points of order ℓ^{r+1}, so by Proposition 1 (2)(b), from $(1,\alpha)$ we get $(\ell,\alpha\ell)$. Therefore, in $E(\mathbf{F}_q)$ there are points of order ℓ^r which ℓ-divide in $E(\mathbf{F}_{q^\ell})$. Since (3) detemines how many points of a given order are in $E[\ell^\infty](\mathbf{F}_{q^{\ell^e}})$, we have that for $e \le r-s-1$ the points of order ℓ^r included in (ℓ^e,β), from Lemma 3, do not ℓ-divide in $E(\mathbf{F}_{q^{\ell^e}})$. Therefore, by Proposition 2 (2), from (ℓ^e,β) we get $(\ell^{e+1},\beta\ell)$. If $e = r-s$, on the short branches of $E[\ell^\infty](\mathbf{F}_{q^{\ell^{r-s}}})$ there are no points of order ℓ^{r+1}. Hence, by using Proposition 2 (2), from (ℓ^{r-s},α) we get $(\ell^{r-s+1},\alpha\ell)$.

For $k > r$ a similar argument shows that the result holds. □

Example 2. Let E be the elliptic curve defined over $\mathbf{F}_{101}$ by

$$y^2 = x^3 + 62x + 86.$$

For $\ell = 5$, we get $E[5^\infty](\mathbf{F}_{101}) \simeq \mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}5\mathbf{Z}$. Then, for $k = 2$, since $r = s = 1$, the factorisation pattern over $\mathbf{F}_{101}[x]$ of $f_{5^2}(x)/f_5(x)$ is $((5,\ 60))$.

Acknowledgments. Research of the authors was supported in part by grants PID2021-124613OB-I00 and 2021SGR-00434.

References

[1] I. F. Blake, G. Seroussi and N. P. Smart, *Elliptic curves in cryptography*, London Mathematical Society Lecture Note Series, 265, Cambridge Univ. Press, Cambridge, 1999.

[2] J. M. Miret, R. Moreno, A. Rio and M. Valls, Computing the l-power torsion of an elliptic curve over a finite field, Math. Comp. **78** (2009), no. 267, 1767–1786.

[3] J. M. Miret, J. Pujolàs and J. Valera, On the ℓ-adic valuation of the cardinality of elliptic curves over finite extensions of $\mathbf{F}_q$, Arch. Math. **105** (2015), no. 3, 261–269.

[4] D. Sadornil, A note on factorisation of division polynomials, arXiv:math/0606684v1.

[5] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, 106, Springer, New York, 1986.

[6] H. Verdure, Factorisation patterns of division polynomials, Proc. Japan Acad. Ser. A Math. Sci. **80** (2004), no. 5, 79–82.

[7] H. Verdure, Factorisation patterns of division polynomials, Proc. Japan Acad. Ser. A Math. Sci. **80** (2004), no. 5, 79–82, Erratum: Proc. Japan Acad. Ser. A Math. Sci. **82** (2006), no. 7, 111.