Scuola Universitaria Superiore
IUSS
Corsi ordinari

Multiplication Polynomials for Elliptic Curves over Finite Local Rings

Classe di Scienze, Tecnologie e Società

Ambito disciplinare: *Scienze e Tecnologie*

Diploma di licenza biennale di secondo livello

Allievo/a Riccardo Invernizzi

Relatore: Chiar.mo Dr. Daniele Taufer

Controrelatore: Chiar.mo Prof. Andrea Tiengo

Anno Accademico 2022 - 2023

MULTIPLICATION POLYNOMIALS FOR ELLIPTIC CURVES OVER FINITE LOCAL RINGS

RICCARDO INVERNIZZI AND DANIELE TAUFER

ABSTRACT. For a given elliptic curve E over a finite local ring, we denote by E^∞ its subgroup at infinity. Every point $P \in E^\infty$ can be described solely in terms of its x-coordinate P_x, which can be therefore used to parameterize all its multiples nP. We refer to the coefficient of $(P_x)^i$ in the parameterization of $(nP)_x$ as the i-th multiplication polynomial. We show that this coefficient is a degree-i rational polynomial without a constant term in n. We also prove that no primes greater than i may appear in the denominators of its terms. As a consequence, for every finite field $\mathbb{F}_q$ and any $k \in \mathbb{N}^*$, we prescribe the group structure of a generic elliptic curve defined over $\mathbb{F}_q[X]/(X^k)$, and we show that their ECDLP on E^∞ may be efficiently solved.

1. INTRODUCTION

Elliptic curves are fascinating objects that have been attracting considerable attention from several different fields, such as number theory [19] and algebraic cryptography [11, 8]. One of the key features of these objects is the fact that they have been proven to be abelian varieties, and as such, they are naturally endowed with a group structure.

Remarkably, the points of such groups can be efficiently handled, but their algebra may almost never be read from their coordinate representation. Thence, the entries of the multiples of a given point usually look random and therefore provide no information about the underlying group operation. This feature has been heavily exploited to design discrete logarithm-based cryptosystems, such as key agreement [10], signature schemes [7], and pseudorandom number generators [16].

However, point multiplication may be read from point coordinates in a few cases. For instance, the algebra on the group at infinity of non-canonical lifting of anomalous curves has been employed for efficiently solving the discrete logarithm problem on these curves [12, 15, 18].

In this work, we adopt a novel approach to address the group at infinity E^∞ of elliptic curves E defined over finite local rings $(\mathcal{R}, \mathfrak{m})$. First, we provide an efficient description of the addition law for these points (Proposition 3.2), and we show that every point $P \in E^\infty$ may be represented as $P = \big(X : 1 : \mathtt{f}(X)\big)$, for a prescribed polynomial $\mathtt{f} \in \mathcal{R}[x]$ (Proposition 4.2). Therefore, one can symbolically compute the n-th multiple of P as $nP = \big((nP)_x : 1 : \mathtt{f}((nP)_x)\big)$. We define the *multiplication polynomials* ψ_i as the maps sending $n \in \mathbb{N}$ to the coefficient of X^i in $(nP)_x$, namely for every $n \in \mathbb{N}$ we have

$$(nP)_x = \psi_1(n)X + \psi_2(n)X^2 + \cdots + \psi_{k-1}(n)X^{k-1},$$

where k is the minimal integer such that $\mathfrak{m}^k = (0)$. These objects are, a priori, just functions of n. However, we prove that every $\psi_i(n)$ is actually a polynomial of degree i over the rationals and the curve coefficients, and that we have $n|\psi_i(n)$ (Theorem 5.9). Furthermore, we show that the prime divisors appearing in the denominators of $\psi_i(n)$ may never be larger than i (Theorem 5.13).

These facts prescribe general arithmetic properties of the scalar multiplication in E^∞, especially when the considered scalar is the characteristic of the residue field $\mathcal{R}/\mathfrak{m}$ (Corollary 5.14). We present an application of these results for determining the group structure of elliptic curves arising

2020 *Mathematics Subject Classification.* Primary 11G07; Secondary 11T55, 11C08, 13B25.

Key words and phrases. Elliptic curve, local finite ring, points at infinity, addition law, multiplication polynomials.

D.T. was supported by the Research Foundation - Flanders (FWO), project 12ZZC23N.

over $\mathcal{R} = \mathbb{F}_q[x]/(x^k)$. This was an open problem [14, Section 11], which we completely solve for *generic* elliptic curves, namely all elliptic curves but those satisfying special conditions (Theorem 6.19 and Corollary 6.20).

We also discuss the structure of E^∞ in the remaining cases, providing their classification under three broad conditions on the curve coefficients (Theorem 6.19). We prove that these conditions always hold for rings of characteristic 2 or 3, and we computationally verify them for all the elliptic curves within the reach of our calculators.

Finally, in Section 6.3 we observe that solving the elliptic curve discrete logarithm problem over these special rings is not substantially harder than the same problem over their residue fields.

1.1. **Paper organization.** In Section 2, we recall the known definitions and results that we employ in the paper. Efficient computation of the addition law is presented in Section 3, while the standard form of points at infinity is presented in Section 4. Section 5 is devoted to the definition of multiplication polynomials and to establishing their main properties. In Section 6, the previous results are applied to determine the group of elliptic curves over $\mathbb{F}_q[x]/(x^k)$. Symbolic verification and computational tests can be found at [6].

2. Notation and standard results

Let $\mathcal{R}$ be a finite local ring, whose maximal ideal will be denoted by $\mathfrak{m}$. Since it is finite, its residue field $\mathcal{R}/\mathfrak{m} \simeq \mathbb{F}_q$ is a finite field, and its size $\#\mathcal{R}$ is a power of q. Moreover, there is $k \in \mathbb{N}$ such that $\mathfrak{m}^k = 0$. The minimal such k will be then referred to as the nilpotence degree of $\mathcal{R}$. Hence, every element $r \in \mathfrak{m}$ is nilpotent, while $\mathcal{R}\backslash\mathfrak{m} = \mathcal{R}^*$, i.e. every non-nilpotent element is invertible.

The projective plane over $\mathcal{R}$ is the set of classes $(X : Y : Z)$ representing primitive triples (X, Y, Z) modulo the action of $\mathcal{R}^*$ given by the component-wise multiplication. In other terms, the elements of $\mathbb{P}^2(\mathcal{R})$ are the projective points $(X : Y : Z)$ with $\langle X, Y, Z\rangle = \langle 1\rangle = \mathcal{R}$, identified by the equivalence relation

$$(X_1 : Y_1 : Z_1) = (X_2 : Y_2 : Z_2) \text{ if and only if}$$
$$X_1Y_2 - X_2Y_1 = X_1Z_2 - X_2Z_1 = Y_1Z_2 - Y_2Z_1 = 0.$$

An elliptic curve E over $\mathcal{R}$ is the set of plane projective points satisfying a non-singular Weierstrass equation over $\mathcal{R}$, namely

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

The non-singularity condition amounts to having an invertible prescribed polynomial combination Δ_E of the coefficients a_i, i.e. $\Delta_E \in \mathcal{R}^*$. The precise definition of such Δ_E may be found in [17, Section III.1], with the following minor correction:

- $b_2 = a_1^2 + 4a_2$ instead of $b_2 = a_1^2 + 4a_4$.

These objects are known to have a group structure defined via the bihomogeneous polynomials of bidegree $(2, 2)$ explicitly given in [3], modulo the corrections, reported by [1], of two minor typos:

- in $X_3^{(2)}$, write the term $a_3a_4(-2X_1Z_2 - X_2Z_1)X_2Z_1$ in place of $a_3a_4(X_1Z_2 - 2X_2Z_1)X_2Z_1$,
- in $Y_3^{(2)}$, write $-(3a_2a_6 - a_4^2)(-2X_1Z_2 - X_2Z_1)X_2Z_1$ instead of $-(3a_2a_6 - a_4^2)(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z1)$.

We will denote the law associated to the point $(0 : 0 : 1)$ as $+_{(0:0:1)}$, and the one associated to $(0 : 1 : 0)$ as $+_{(0:1:0)}$. We recall that a pair of points is exceptional for $+_{(0:0:1)}$ if and only if the z-coordinate of the sum is a zero divisor, while it is exceptional for $+_{(0:1:0)}$ if and only if the y-coordinate of the sum is a zero divisor. Therefore, $+_{(0:0:1)}$ and $+_{(0:1:0)}$ form a complete system of addition laws for any elliptic curve, whose combined action will be simply denoted as $+$. The identity of these groups is $\mathcal{O} = (0 : 1 : 0)$, and the inverse of a given point $(X : Y : Z)$ is given by

$$-(X : Y : Z) = (X : -Y - a_1X - a_3Z : Z).$$

Given a point $P = (X : Y : Z) \in \mathbb{P}(\mathcal{R})$ of an elliptic curve defined over $\mathcal{R}$, it may be uniquely represented as

$$P = \begin{cases} (X \cdot Z^{-1} : Y \cdot Z^{-1} : 1), & \text{if } Z \in \mathcal{R}^*, \\ (X \cdot Y^{-1} : 1 : Z \cdot Y^{-1}), & \text{otherwise.} \end{cases}$$

The points that admit a representation of the first type are called *affine*, while the others are called *at infinity*. Those points lie above the affine (resp. at infinity) points of the underlying curve defined over the residue field $\mathbb{F}_q \simeq \mathcal{R}/\mathfrak{m}$, via the componentwise canonical projection

$$\pi : E(R) \to E(\mathbb{F}_q), \quad (X : Y : Z) \mapsto ([X] : [Y] : [Z]).$$

It is well known that since the addition laws are polynomial in the coordinates of the points, then π is a surjective group homomorphism [9, Sec. 4]. The group of points at infinity of an elliptic curve E is its subgroup denoted by $E^\infty = \pi^{-1}(\mathcal{O})$.

3. Addition Law

Computing the point addition on elliptic curves defined over a ring usually requires computing a valid linear combination of the triples obtained by a complete system of addition laws [9, Sec. 3]. However, over a finite local ring $\mathcal{R}$ this computation is simpler, as the sum is always directly computed by $+_{(0:0:1)}$ or by $+_{(0:1:0)}$.

Proposition 3.1. *Let P_1, P_2 two points of an elliptic curve defined over $\mathcal{R}$. Then $P_1 + P_2$ is always computed by $P_1 +_{(0:0:1)} P_2$ or by $P_1 +_{(0:1:0)} P_2$.*

Proof. Since these addition laws form a complete system, thanks to [9, Sec. 3] at least one between $P_1 +_{(0:0:1)} P_2$ and $P_1 +_{(0:1:0)} P_2$ is guaranteed to contain a non-nilpotent entry. Since non-nilpotent elements of $\mathcal{R}$ are invertible, then one entry is a unit and therefore we have a valid projective point. □

Notation. From now on, we will denote the points symbolically, namely their coordinates will be regarded as variables instead of elements of $\mathcal{R}$. With this slight abuse of notation, we shorten and simplify the statements, and every result we prove holds regardless of the specific point one starts from. As an instance, given a point $P = (X : Y : Z) \in \mathbb{P}^2(\mathcal{R})$, we will consider XYZ as a degree-3 polynomial rather than an element of $\mathcal{R}$.

The following proposition gives an elegant and efficient way of computing $+_{(0:1:0)}$.

Proposition 3.2. *For $i \in \{1, 2\}$, let $P_i = (X_i : Y_i : Z_i) \in \mathbb{P}^2(\mathcal{R})$ be two projective points. Let also*

$$(X_3, Y_3, Z_3) = P_1 +_{(0:1:0)} P_2,$$

and

$$g_1 = X_2(a_1X_1 + a_3Z_1 + Y_1) + X_1Y_2,$$
$$g_2 = Z_2(a_1X_1 + a_3Z_1 + Y_1) + Z_1Y_2.$$

Then there exist four bihomogenous polynomials

$$H_1, \ldots, H_4 \in \mathcal{R}[X_i, Y_i, Z_i]_{i \in \{1,2\}}$$

of bidegree $(1, 1)$ such that

$$X_3 = g_1H_1 + g_2H_2,$$
$$Z_3 = g_1H_3 + g_2H_4,$$
$$Y_3 = H_1H_4 - H_2H_3.$$

Proof. Straightforward computation. The explicit polynomials H_i and the actual formal verification may be found in the Appendix (Proposition A.1). □

Remark 3.3. *As we will show shortly, in this work we will always consider points that are not exceptional for the second addition law. These reduced formulas will be of great help both in terms of understanding the sum and computational speed.*

Remark 3.4. *Proposition 3.2 is the natural generalization of* [13, Lemma 2.1] *and works for every elliptic curve with an extended Weierstrass model over any admissible ring, regardless of the characteristic.*

4. Points over $\mathcal{O}$

In this section, we describe a convenient way of representing points in E^∞. We will establish results that hold symbolically for all such points, i.e. they hold for every specialization of their entries in $\mathcal{R}$.

Remark 4.1. *Let $P = (X : Y : Z) \in E^\infty$. Since by definition $\pi(P) = (0 : 1 : 0)$, its standard form will always be $P = (X : 1 : Z)$ with $X, Z \in \mathfrak{m}$. This also implies that $+_{(0:1:0)}$ is always valid over E^∞. From now when we add two points we are implicitly using this addition law.*

Notation. Given a projective point $P \in \mathbb{P}^2(\mathcal{R})$ at infinity, we will denote by P_x (resp. P_z) the x-coordinate (resp. z-coordinate) of its standard form $(P_x : 1 : P_z)$.

Proposition 4.2. *Let E be an elliptic curve over $\mathcal{R}$. There is a polynomial $\mathtt{f} \in \mathcal{R}[x]$ of degree strictly lower than the nilpotence degree of $\mathcal{R}$, such that for every $P \in E^\infty$ we have $P = \big(P_x : 1 : \mathtt{f}(P_x)\big)$. Moreover, $x^3 | \mathtt{f}(x)$.*

Proof. This is the same idea of [12, Prop. 11]. Every point in E^∞ satisfies

$$z = x^3 - a_1xz + a_2x^2z - a_3z^2 + a_4xz^2 + a_6z^3,$$

or $z = \mathtt{f}(x, z)$. We can hence replace z with $\mathtt{f}(x, z)$ on the right side obtaining

$$z = \mathtt{f}\big(x, \mathtt{f}(x, ...\mathtt{f}(x, z)...)\big).$$

In this way the degree in $\mathcal{R}[x, z]$ of every monomial containing z increases every time, and since in this ring $z^k = x^k = 0$ (because $P_x, P_z \in \mathfrak{m}$), after a finite number of substitutions we are left with $z = \mathtt{f}(x)$. The computation of the explicit expression of $\mathtt{f}$ truncated to small exponents can be found in the Appendix (Proposition A.2), from which one easily observes that $x^3 | \mathtt{f}(x)$. □

By Proposition 4.2 we see that a generic point $P \in E^\infty$ is entirely determined by P_x and the coefficients of the Weierstrass equation of E. Up to now, we assumed to be working with a fixed curve E. However, since the statement of Proposition 4.2 holds independently from the chosen curve E, we can let E and hence its coefficients a_i vary. In this way, we get the multivariate function

$$z = \mathtt{f}(x, a_i) \in \mathbb{F}_q[a_1, \dots, a_6][x].$$

Lemma 4.3. *Given any curve E over $\mathcal{R}$ and three points $P, Q, R \in E^\infty$ such that $P + Q = R$, we have*

$$R_x \in \langle P_x, Q_x \rangle \subset \mathbb{Z}[a_1, \dots, a_6][P_x, Q_x].$$

Proof. It follows from a direct inspection of the addition formulae. Further details can be found in Proposition A.4, applied with $P_1 = P$, $P_2 = Q$ and $P_3 = R$. With that notation, both I_P and all the other terms of R_x are clearly contained in $\langle P_x, Q_x \rangle$. □

Remark 4.4. *When both P and Q are a multiple of a same point $(X : 1 : Z)$, by Lemma 4.3 we have $R_x \in \langle X \rangle$.*

5. Multiplication Polynomials

Lemma 5.1. *Given an elliptic curve E over $\mathcal{R}$, for every $n \in \mathbb{N}$ there are uniquely defined coefficients $\psi_1(n), ..., \psi_{k-1}(n) \in \mathcal{R}$ such that for every symbolic $P = \big(X : 1 : \mathfrak{f}(X)\big) \in E^\infty$ we have*

$$(nP)_x = \sum_{i=1}^{k-1} \psi_i(n) X^i.$$

Proof. From Lemma 4.3 we know that $(nP)_x$ is a polynomial function of X without constant term, which proves the existence. As for uniqueness, let us assume that we can also write

$$(nP)_x = \sum_{i=1}^{k-1} \varphi_i(n) X^i.$$

This implies

$$0 = \sum_{i=1}^{k-1} \left[\psi_i(n) - \varphi_i(n)\right] X^i$$

and since the X^i are a basis for polynomials in X, this shows that $\psi_i(n) = \varphi_i(n)$ for every $1 \leq i \leq k-1$. □

Remark 5.2. *The coefficients $\psi_i(n)$ depend on the coefficients a_i of the given elliptic curve, therefore they may also be regarded as functions $\psi_i(n, a_i)$.*

Definition 5.3. *For every $1 \leq i \leq k-1$ we define the* i-th multiplication polynomial *ψ_i as the unique function over $\mathbb{N}$ such that $\psi_i(n)$ is the coefficient of X^i in $(nP)_x$, as determined in Lemma 5.1.*

At this stage, it may not be clear that they are actual polynomials, as it will be proved in Theorem 5.9.

Remark 5.4. *By definition, it holds $\psi_i(1) = 0$ for all $i \geq 2$.*

Remark 5.5. *Since the addition law is polynomial in the entries of the addenda, computing the coefficient of X^i in $(nP)_x$ never requires computing coefficients of X^j with $j > i$. For this reason, we may perform every computation of $\psi_i(n)$ modulo X^{i+1}, as if the nilpotence of $\mathcal{R}$ was $i+1$.*

Lemma 5.6. *With the above notation, we have*

$$\psi_1(n) = n.$$

Proof. Thanks to Remark 5.5 we may assume $k = 2$. This implies that for every $P \in E^\infty$ we have $P_z = \mathtt{f}(P_x) = 0$, and the addition between two such points becomes

$$(X_1 : 1 : 0) + (X_2 : 1 : 0) = (X_1 + X_2 : 1 : 0).$$

In this case, the curve addition simply corresponds to the standard ring addition in the first entry, then $nP = (nP_x : 1 : 0)$. □

Lemma 5.7. *With the above notation, we have*

$$\psi_2(n) = \binom{n}{2} a_1.$$

Proof. By Remark 5.5 we can assume $k = 3$. Again, this implies that for every $P \in E^\infty$ we have $P_z = 0$, hence $P = (X : 1 : 0)$. We find $\psi_2(n)$ recursively, by computing

$$nP = (X : 1 : 0) + \big(\psi_1(n-1)X + \psi_2(n-1)X^2 : 1 : 0\big).$$

Performing this addition, we obtain

$$nP = \big((1 + \psi_1(n-1))X + (a_1 + 2a_1\psi_1(n-1) + \psi_2(n-1))X^2 : 1 + a_1 X : 0\big).$$

The inverse of its y-coordinate is $1 - a_1X - a_1^2X^2$, therefore

$$nP = \big((1 + \psi_1(n-1))X + (a_1\psi_1(n-1) + \psi_2(n-1))X^2 : 1 : 0\big).$$

Hence, we have

$$\psi_2(n) = a_1\psi_1(n-1) + \psi_2(n-1),$$

which leads to the recurrence relation

$$\psi_2(n) - \psi_2(n-1) = a_1\psi_1(n-1) = a_1(n-1),$$

where the last equality follows from Lemma 5.6. Since $\psi_2(1) = 0$, by Remark 5.4, we get

$$\psi_2(n) = \sum_{m=1}^{n-1} \big(\psi_2(m+1) - \psi_2(m)\big) = a_1\frac{n(n-1)}{2},$$

which concludes the proof. □

The explicit computation of $\psi_i(n)$ becomes increasingly harder for larger values of i. However, the technique used in Lemma 5.7 can be used to infer useful properties about these objects. To prove them, we need the following technical lemma.

Lemma 5.8. *Let $\mathbb{Z}[a_1, \ldots, a_6][\beta_1, \ldots, \beta_{k-1}]$ be the graded ring of weights $\deg_\beta(\beta_j) = j$. For every $2 \le i \le k-1$, there exists*

$$g_i \in \langle \beta_1, \ldots, \beta_{i-1} \rangle, \quad \deg_\beta(g_i) = i - 1,$$

such that, if we symbolically compute

$$S = \big(X : 1 : \mathtt{f}(X)\big) + \left(\sum_{j=1}^{k} \beta_j X^j : 1 : \mathtt{f}\left(\sum_{j=1}^{k} \beta_j X^j\right)\right), \tag{1}$$

then the coefficient of X^i in S_x is $\beta_i + g_i$.

Proof. Let us denote for simplicity the two points involved in the sum (1) by P and Q, respectively. We observe that the coefficient of X^j in Q_x has always $\deg_\beta$ equal to j. Since $Q_z = \mathtt{f}(Q_x)$, this also holds for Q_z. On the other hand, the coefficients of every power of X have $\deg_\beta$ equal to 0 in both P_x and P_z. Since the addition formulae are polynomials in the entries, if we write

$$S_x = \sum_{i=1}^{k} \Psi_i X^i,$$

then we have $\deg_\beta(\Psi_i) \le i$. We now look at all the terms in Ψ_i with $\deg_\beta$ at least $i-1$, namely those terms that involve at most one time P_x, and that never involve P_z. A close inspection of the addition law (detailed in the appendix, see Proposition A.4 with $P_1 = Q$ and $P_2 = P$) shows that these terms only arise from

$$P_x + Q_x + \big(a_1Q_x - a_2Q_x^2 + 2a_3Q_z - 2a_4Q_xQ_z - 3a_6Q_z^2\big)P_x. \tag{2}$$

Since we are considering $i \ge 2$, then $P_x = X$ alone does not produce any term in Ψ_i. Instead, the term β_i of Q_x appears in Ψ_i, and it is therefore its unique term of maximal $\deg_\beta$. We now show that the element

$$g_i = \Psi_i - \beta_i$$

is the required polynomial. By construction we have $\deg_\beta(g_i) \le i - 1$, but from equation (2) we see that it always contain the term $a_1\beta_{i-1}$, which has $\deg_\beta$ equal to $i-1$. Hence, we have $\deg_\beta(g_i) = i - 1$. Finally, an easy inspection of the formulae of Proposition 3.2 shows that the unique term of P that never appears in S_x multiplied by any term of Q is $P_x = X$. However, this term only appears in Ψ_1, therefore for all $i \ge 2$ every monomial composing Ψ_i is divisible by some

β_j. Furthermore, we have $\deg_\beta(\beta_j) = j$, so β_j cannot appear in g_i for every $j \geq i$. In conclusion, we have

$$g_i \in \langle \beta_1, \dots, \beta_{i-1} \rangle,$$

so all such g_i's have the required properties. □

We are now ready to prove the main results of this section.

Theorem 5.9. *For every $1 \leq i \leq k-1$, the i-th multiplication polynomial ψ_i is a polynomial in $\mathbb{Q}[a_1, \dots, a_6][n]$ of degree i in n. Moreover, we have $n|\psi_i(n)$.*

Proof. The case $i = 1$ follows from Lemma 5.6. We prove the thesis by extended induction on $i \geq 2$. The base case $i = 2$ is given by Lemma 5.7. We now assume that this result holds for every $j \leq i-1$, and we show that this implies it also holds for i. Since the addition law is associative, we have

$$(nP)_x = \big(P + (n-1)P\big)_x.$$

The coefficient of X^i on the left-hand side is $\psi_i(n)$. The right-hand side is given by Equation (1) after substituting $\beta_j = \psi_j(n-1)$. Hence by applying Lemma 5.8 we obtain

$$\psi_i(n) - \psi_i(n-1) = g_i\big(\psi_1(n-1), \dots, \psi_{i-1}(n-1)\big).$$

By the inductive hypothesis, $\psi_j(n-1)$ is a degree-j polynomial in n without the constant term. Since $\deg_\beta(\beta_j) = j$, $\deg_\beta(g_i) = i-1$ and g_i has no constant terms, then the evaluation of g_i by $\beta_j = \psi_j(n-1)$ produces a degree-$(i-1)$ polynomial in $n-1$ without a constant term, namely

$$g_i\big(\psi_1(n-1), \dots, \psi_{i-1}(n-1)\big) = c_1(n-1) + \cdots + c_{i-1}(n-1)^{i-1},$$

for some coefficients $c_j \in \mathbb{Q}[a_1, \dots, a_6]$, and $c_{i-1} \neq 0$.

The above arguments hold uniformly on n, therefore we have a system of relations

$$\begin{cases} \psi_i(n) - \psi_i(n-1) & = c_1(n-1) + \cdots + c_{i-1}(n-1)^{i-1}, \\ \psi_i(n-1) - \psi_i(n-2) & = c_1(n-2) + \cdots + c_{i-1}(n-2)^{i-1}, \\ & \vdots \\ \psi_i(2) - \psi_i(1) & = c_1 + \cdots + c_{i-1}. \end{cases}$$

We recall that for every $i \geq 2$, we have $\psi_i(1) = 0$ by Remark 5.4. Therefore, by adding all the above relations we obtain

$$\psi_i(n) = c_1 \sum_{m=1}^{n-1} m + c_2 \sum_{m=1}^{n-1} m^2 + \cdots + c_{i-1} \sum_{m=1}^{n-1} m^{i-1}. \tag{3}$$

Thanks to Faulhaber formulas [4, Sec. 6.5], the sum

$$S_j(n) = 1^j + 2^j + \cdots + (n-1)^j = \sum_{m=1}^{n-1} m^j$$

can be expressed in a closed form as a polynomial in $\mathbb{Q}[n]$ of degree $j+1$ without a constant term. Since

$$\psi_i(n) = \sum_{j=1}^{i-1} c_j \sum_{m=1}^{n-1} m^j = \sum_{j=1}^{i-1} c_j S_j(n), \tag{4}$$

then also $\psi_i(n)$ can be expressed as a polynomial in $\mathbb{Q}[a_1, \dots, a_6][n]$ of degree i and with constant term equal to 0, namely $n|\psi_i(n)$. □

The explicit polynomials $\psi_i(n)$ for the first values of i, as well as further details on their computation, can be found in the Appendix (Section A.4). A more extensive list can be found at [6].

Remark 5.10. *Whenever the elliptic curve is fixed, the a_i's are fixed elements of $\mathcal{R}$, therefore Theorem 5.9 implies that $\psi_i(n)$ will have degree at most i in n. However, its degree might well be strictly lower than i, for instance when dealing with short Weierstrass forms ($a_1 = a_2 = a_3 = 0$).*

Remark 5.11. *While being a polynomial in $\mathbb{Q}[a1, \ldots, a_6][n]$, when evaluated in a specific $\overline{n} \in \mathbb{N}^*$ we always get $\psi_i(\overline{n}) \in \mathbb{Z}[a_1, \ldots, a_6]$. This is expected since we are dealing with integer quantities when adding points. For $\psi_1(\overline{n}) = \overline{n}$ is clear, and also $\psi_2(\overline{n}) \in \mathbb{Z}[a_1, \ldots, a_6]$, since one among $\overline{n}$ and $\overline{n} - 1$ will be even. Following the same induction performed in Theorem 5.9, we eventually conclude that $\psi_i(\overline{n}) \in \mathbb{Z}[a_1, \ldots, a_6]$ for every $1 \leq i \leq k - 1$.*

Notation. We denote the product of the first $i \in \mathbb{N}^*$ factorials as

$$\Pi(i) = \prod_{j=1}^{i} j!.$$

Lemma 5.12. *Let $i, j_1, \ldots, j_m \in \mathbb{N}^*$ such that $\sum_{l=1}^{m} j_l \leq i$. Then*

$$\Pi(j_1) \cdots \Pi(j_m) | \Pi(i).$$

Proof. We prove this by induction on i. For $i = 1$ there is nothing to prove. Now let us assume that it holds for $i - 1$ and every possible $j_1, \ldots, j_m \in \mathbb{N}^*$ such that $\sum_{l=1}^{m} j_l \leq i - 1$. Let $j_1, \ldots j_m \in \mathbb{N}^*$ be such that $\sum_{l=1}^{m} j_l \leq i$. Notice that in general $\Pi(i) = i!\Pi(i-1)$. By the Multinomial Theorem, we have $j_1! \cdots j_m! | i!$, and by inductive hypothesis $\Pi(j_1 - 1) \cdots \Pi(j_m - 1) | \Pi(i-1)$, hence the thesis follows by multiplying the previous relations. □

Theorem 5.13. *With the above notation, for every $1 \leq i \leq k - 1$ we have*

$$\Pi(i)\psi_i(n) \in \mathbb{Z}[a_1, ..., a_6][n].$$

Proof. By Theorem 5.9 we know that $\psi_i(n) \in \mathbb{Q}[a_1, ..., a_6][n]$. The case $i = 1$ follows from Lemma 5.6. We prove the thesis by extended induction on $i \geq 2$, where the base case $i = 2$ is given by Lemma 5.7. Let us assume that the thesis holds for every $j < i$. With the notation of Equation (4) we prove that

(i) for every $1 \leq j \leq i - 1$ we have $\Pi(i-1)c_j \in \mathbb{Z}[a_1, ..., a_6]$,
(ii) for every $1 \leq j \leq i - 1$ we have $i!S_j(n) \in \mathbb{Z}[a_1, ..., a_6]$.

By combining (i) and (ii) with Equation (4), the thesis follows.

(i): By Lemma 5.8 we know that $\deg_\beta(g_i) = i - 1$ and that g_i arises as a polynomial in the $\psi_j(n-1)$ and coefficients in $\mathbb{Z}[a_1, \ldots, a_6]$, whose monomials $\psi_{j_1}(n-1) \cdots \psi_{j_m}(n-1)$ satisfy $\sum_{l=1}^{m} j_l \leq i - 1$. By the inductive hypothesis, for all such monomials we have

$$\Pi(j_1) \cdots \Pi(j_m)\psi_{j_1} \cdots \psi_{j_m} \in \mathbb{Z}[a_1, ..., a_6][n].$$

Since $\Pi(j_1) \cdots \Pi(j_m)$ always divides $\Pi(i-1)$ by Lemma 5.12, then

$$\Pi(i-1)g_i\big(\psi_1(n-1), \ldots, \psi_{i-1}(n-1)\big) \in \mathbb{Z}[a_1, \ldots, a_6][n].$$

(ii): From [4, Eq. 6.80] we obtain

$$(m+1)S_m(n) = n^{m+1} - \sum_{j=0}^{m-1} \binom{m+1}{j} S_j(n).$$

Since $2S_1(n) = n^2 - n$, a simple induction on $m \geq 1$ shows that we have $(j+1)!S_j(n) \in \mathbb{Z}[n]$, therefore also $i!S_j(n) \in \mathbb{Z}[n]$. □

Corollary 5.14. *Let p be a prime number. For every exponent $l \geq 1$ and for every $1 \leq i < p$, we have*

$$\psi_i(p^l) \equiv 0 \mod p^l.$$

Proof. By Theorem 5.13 we have $\Pi(i)\psi_i(p^l) \in \mathbb{Z}[a_1, \dots, a_6]$. Thanks to Theorem 5.9 we also have $\Pi(i)\psi_i(p^l) \equiv 0 \mod p^l$. By definition $\Pi(i) \in (\mathbb{Z}/p^l\mathbb{Z})^*$ for every $i < p$, therefore we conclude $\psi_i(p^l) \equiv 0 \mod p^l$. □

Remark 5.15. *As $\mathcal{R}$ is a finite local ring, its characteristic* $\operatorname{char}(\mathcal{R})$ *is a prime power p^l. Thus, Corollary 5.14 implies that for every $P = \big(X : 1 : f(X)\big) \in E^\infty$ we have $\psi_i(p^l) = 0$ for every $i < p$, hence*

$$X^p \mid (p^l P)_x.$$

Furthermore, since $X \in \mathfrak{m}$, this implies $(p^l P)_x \in \mathfrak{m}^p$. This condition imposes severe restrictions on the possible group structures arising from E^∞.

6. Elliptic curves over $\mathbb{F}_q[x]/(x^k)$

In this section, we fix a prime power $q = p^e$ and a positive integer $k \in \mathbb{N}^*$. Let $\mathbb{F}_q$ be the finite field of size q, and consider the ring

$$R_k = \mathbb{F}_q[x]/(x^k) \simeq \mathbb{F}_q[\epsilon], \text{ with } \epsilon^k = 0.$$

Such an R_k is a finite local ring, whose maximal ideal $\mathfrak{m} = (\epsilon)$ is principal, therefore it underlies the results of the previous sections. From now on, we will work over the ring $\mathcal{R} = R_k$. Notice that k is the nilpotence degree of R_k, consistently with our previous notation. If $k = 1$ then $R_k \simeq \mathbb{F}_q$, while if $k \geq 2$ then every element $r \in R_k$ may be written uniquely as $r = a + b\epsilon$, for some $a \in \mathbb{F}_q$ and a degree-$(k-2)$ polynomial $b \in \mathbb{F}_q[\epsilon]$. Moreover, $r \in R_k^*$ if and only if $a \neq 0$. Hence, every $r \in R_k$ is either a unit or divisible by ϵ.

We will exploit the multiplication polynomials to compute the group structure of elliptic curves over this ring in all but a few exceptional cases given by particular choices of the curve coefficients $a_1, \dots, a_6 \in R_k$.

The canonical projection may be written explicitly as

$$\pi : E(R_k) \to E(\mathbb{F}_q),$$
$$(\alpha_x + \beta_x\epsilon : \alpha_y + \beta_y\epsilon : \alpha_z + \beta_z\epsilon) \mapsto (\alpha_x : \alpha_y : \alpha_z).$$

From [9, Sec. 4] we know that its fibers have size q^{k-1}, so in particular $E^\infty = \pi^{-1}(\mathcal{O})$ is a p-subgroup of $E(R_k)$. Moreover, the structure of E^∞ often prescribe the structure of the whole group, as we have the short exact sequence of groups

$$0 \to E^\infty(R_k) \xhookrightarrow{i} E(R_k) \xrightarrow{\pi} E(\mathbb{F}_q) \to 0.$$

When the above sequence splits, we have

$$E(R_k) \cong E(\mathbb{F}_q) \oplus E^\infty.$$

This is always the case when

$$\gcd\big(\#E(\mathbb{F}_q), p\big) = 1, \tag{5}$$

which happens with overwhelming probability for large primes p, and it is always satisfied by elliptic curves of cryptographic interest. We will therefore address the group structure of elliptic curves underlying this condition.

We can now apply Corollary 5.14 to this setting (with $l = 1$).

Corollary 6.1. *Let $P = \big(X : 1 : f(X)\big) \in E^\infty$ be a point. Then*

$$(pP)_x \equiv \psi_p(p) X^p \bmod X^{p+1}.$$

This result is sufficient to compute the group structure of E^∞ whenever considered exponent k is smaller than the ring characteristic p.

Proposition 6.2. *Let E be an elliptic curve over R_k where $k \leq p$. Then we have the group isomorphism*

$$E^\infty \cong (\mathbb{F}_p)^{e(k-1)}.$$

Proof. From Corollary 6.1 every point has order p. We already observed that E^∞ is a p-group of size $q^{k-1} = p^{e(k-1)}$, from which the thesis follows. □

To address the cases with $k > p$ we by introduce a way for "counting the divisibility" of points with respect to ϵ.

Definition 6.3. *Let $r \in R_k \backslash \{0\}$. We define its* minimal degree $\nu(r)$ *as the maximal $i \geq 0$ such that $\epsilon^i | r$. We also define $\nu(0) = \infty$. Finally, for every point $P \in E^\infty$, we define $\nu(P) = \nu(P_x)$.*

We notice that ν is almost a valuation on R_k, as it satisfies

$$\nu(xy) \geq \nu(x)\nu(y), \quad \text{and} \quad \nu(x+y) \geq \min\{\nu(x), \nu(y)\}.$$

Remark 6.4. *$\nu(P) = \infty$ if and only if $P = \mathcal{O}$.*

Lemma 6.5. *Let $P, Q \in E^\infty$ be two points with $\nu(P) \neq \nu(Q)$. Then*

$$\nu(P+Q) = \min\{\nu(P), \nu(Q)\}.$$

Proof. The statement is trivial if either P or Q is $\mathcal{O}$, so let us assume $P, Q \neq \mathcal{O}$. Let us denote $m = \min\{\nu(P), \nu(Q)\}$. Then e^{m+1} divides P_z, Q_z and all the products involving x and z coordinates of both the points. A close inspection of the formulae (detailed in Proposition A.5, with $P_1 = P$ and $P_2 = Q$) shows that

$$(P+Q)_x \equiv P_x + Q_x \bmod \epsilon^{m+1}$$

Since by assumption $\nu(P_x) \neq \nu(Q_x)$, the conclusion follows. □

Lemma 6.6. *Let $P, Q \in E^\infty$ be points with $\nu(P) = \nu(Q) = m < \infty$. Let $c_p, c_q \in \mathbb{F}_q$ be the coefficients such that*

$$P_x \equiv c_p \epsilon^m \bmod \epsilon^{m+1} \quad \text{and} \quad Q_x \equiv c_q \epsilon^m \bmod \epsilon^{m+1}.$$

Then we have

$$(P+Q)_x = (c_p + c_q)\epsilon^m \bmod \epsilon^{m+1}.$$

Proof. It follows from the same argument of Lemma 6.5. □

Remark 6.7. *In the notation of Lemma 6.6, if $c_p + c_q \neq 0$ then*

$$\nu(P+Q) = m = \nu(P) = \nu(Q).$$

Lemma 6.8. *Let $n \in \mathbb{N}^*$ such that $p \nmid n$. Then*

$$\nu(nP) = \nu(P).$$

Proof. Thanks to Lemma 5.6, we have

$$(nP)_x \equiv nP_x \bmod P_x^2.$$

Since n is invertible in $\mathbb{F}_q$, we have $\nu(nP_x) = \nu(P_x)$. If $P = \mathcal{O}$ the thesis is clear. Otherwise, we have $\nu(nP_x) < \nu(P_x^2)$, therefore by Lemma 6.5 we have

$$\nu\big((nP)_x\big) = \nu(nP_x) = \nu(P_x).$$

The quantity on the left side is $\nu(nP)$, while the right one is $\nu(P)$, so they are equal. □

Definition 6.9. *We define the* trajectory *of $P \in E^\infty$ as*

$$\mathrm{trj}(P) = \{\nu(nP)\}_{n \in \mathbb{N}} \setminus \{\infty\}.$$

Example 6.10. If a point P has order p and $\nu(P) = m$, by applying Lemma 6.8 we see that $\mathrm{trj}(P) = \{m\}$.

Lemma 6.11. *Let $P, Q \in E^\infty$ be points with $\mathrm{trj}(P) \cap \mathrm{trj}(Q) = \emptyset$. For every $n, m \in \mathbb{Z}$ we have $nP + mQ = \mathcal{O}$ if and only if $nP = mQ = \mathcal{O}$.*

Proof. If both nP and mQ are $\mathcal{O}$, then also their sum clearly is. On the other side, since $\mathrm{trj}(P) \cap \mathrm{trj}(Q) = \emptyset$ we have $\nu(nP) \neq \nu(mQ)$, which by Lemma 6.5 implies

$$\infty = \nu(nP + mQ) = \min\{\nu(nP), \nu(mQ)\}.$$

Therefore we have $\nu(nP) = \nu(mQ) = \infty$, i.e. $nP = mQ = \mathcal{O}$. □

As we will see shortly, the group structure of E^∞ depends on $\nu\big(\psi_p(p)\big)$. There are two possible cases:

(1) $\nu\big(\psi_p(p)\big) = 0$, i.e. $\psi_p(p) \in R_k^*$, or
(2) $\nu\big(\psi_p(p)\big) > 0$, i.e. $\epsilon | \psi_p(p)$.

The first case will be referred to as the *main case*, as it occurs with overwhelming probability with a uniform choice of the curve coefficients, and it will be discussed in Section 6.1. The second case will be referred to as the *exceptional case*, and examined in Section 6.2.

6.1. **Main case.** In this section, we focus on case (1), namely we will assume that

$$\psi_p(p) \in R_k^*. \tag{6}$$

The main idea is to use Corollary 6.1 to partition the numbers up to $k-1$ in different point trajectories. For each trajectory, we will pick e independent points P_i such that $\nu(P_i)$ is the minimal value of the trajectory and show that these points generate the whole group.

Lemma 6.12. *Let $P \in E^\infty$ be a point. For every $i \in \mathbb{N}$, we have*

$$\nu(p^i P) = \begin{cases} p^i \nu(P) & \text{if } p^i \nu(P) < k, \\ \infty & \text{otherwise.} \end{cases}$$

Proof. We prove it by induction on i. The base step $i = 0$ holds identically. Let us now assume this holds for $i = j - 1$. Then

$$\nu(p^j P) = \nu\big(p(p^{j-1}P)\big) = \nu(pQ), \quad \text{where} \quad Q = p^{j-1}P.$$

By inductive hypothesis $\nu(Q) = p^{j-1}m$ so we can write

$$Q_x = c_m \epsilon^{p^{j-1}m} \bmod \epsilon^{p^{j-1}m+1}$$

for some $c_m \in R_k^*$. Then by Corollary 6.1 we obtain

$$(pQ)_x = \psi_p(p)(c_m)^p \epsilon^{p^j m} \bmod \epsilon^{p^j m+1}.$$

By assumption (6) we know that $\psi_p(p) \in R_k^*$, which implies that $\nu(pQ) = p^j m = p\nu(Q)$ if $pm < k$, and $\nu(pQ) = \infty$ otherwise. □

Proposition 6.13. *For every $1 \leq m \leq k-1$, if $P \in E^\infty$ has minimal degree $m = \nu(P)$, then its order is*

$$\mathrm{ord}(P) = p^{l_m}, \quad \text{where} \quad l_m = \left\lfloor \log_p \frac{k-1}{m} \right\rfloor + 1.$$

Proof. By definition, the integer l_m is the largest integer such that $mp^{l_m - 1} \leq k - 1$, while $mp^{l_m} > k - 1$. In fact, we have

$$mp^{l_m - 1} = mp^{\lfloor \log_p \frac{k-1}{m} \rfloor} \leq m \frac{k-1}{m} = k - 1,$$

and

$$mp^{l_m} = mp^{\lfloor \log_p \frac{k-1}{m} \rfloor + 1} > m \frac{k-1}{m} = k - 1.$$

From Lemma 6.12 we see that $\nu(p^{l_m-1}P) = mp^{l_m-1} \leq k-1$, and then $p^{l_m-1}P \neq \mathcal{O}$, while $\nu(p^{l_m}P) = mp^{l_m} > k-1$, hence $p^{l_m} = \mathcal{O}$. The thesis follows from the fact that E^∞ is a p-group. □

Remark 6.14. *For every $1 \leq m \leq k-1$, the quantity l_m given in Proposition 6.13 is well defined, since the point $P = \left(\epsilon^m : 1 : \boldsymbol{f}(\epsilon^m)\right)$ satisfies $\nu(P) = m$.*

Lemma 6.15. *For every $1 \leq m \leq k-1$, if $P \in E^\infty$ has minimal degree $m = \nu(P)$, then*

$$\mathrm{trj}(P) = \{mp^i\}_{i<l_m}.$$

Proof. It follows from Lemma 6.12 and Proposition 6.13. □

Lemma 6.16. *For every $1 \leq m \leq k-1$, if $P \in E^\infty$ has minimal degree $m = \nu(P)$, then $\#\,\mathrm{trj}(P) = l_m$.*

Proof. With the same notation of Lemma 6.15, the $\{mp^i\}_{i<l_m}$ are all distinct integers and the index i runs from 0 to $l_m - 1$. □

Lemma 6.17. *With the above notation, we have*

$$\sum_{\substack{1\leq m\leq k-1\\(m,p)=1}} l_m = k-1.$$

Proof. By Lemma 6.15 and 6.16, we know that l_m is the size of $\{mp^i\}_{i<l_m}$. It is enough to show that these sets for $(m,p) = 1$ form a partition of the numbers between 1 and $k-1$. They are disjoint, since $m_1p^{h_1} = m_2p^{h_2}$ with m_1, m_2 coprime with p is possible only if $m_1 = m_2$. Moreover, every number below $k-1$ can be written as mp^h for some $m \leq k-1$ coprime with p and $h < l_m$, by definition of l_m. This completes the proof. □

Proposition 6.18. *Let $\{\gamma_n\}_{1\leq n\leq e}$ be an $\mathbb{F}_p$-basis of $\mathbb{F}_q$. For any given $1 \leq m \leq k-1$, the points*

$$g_{nm} = \left(\gamma_n\epsilon^m : 1 : \boldsymbol{f}(\gamma_n\epsilon^m)\right) \in E^\infty$$

are linearly independent. Moreover, the trajectory of every linear combination of the $\{g_{nm}\}_{1\leq n\leq e}$ lies into $\{mp^j\}_{j<l_m}$.

Proof. We want to show that for every $h_{nm} \in \mathbb{N}$ we have

$$S = \sum_{n=1}^{e} h_{nm}g_{nm} = \mathcal{O} \iff \forall\ 1 \leq n \leq e :\ h_{nm}g_{nm} = \mathcal{O}.$$

Clearly $h_{nm}g_{nm} = \mathcal{O}$ for every n implies $S = \mathcal{O}$. On the other side, let us suppose that $h_{nm}g_{nm} \neq \mathcal{O}$ for some n, i.e. $\nu(h_{nm}g_{nm}) < \infty$. Let $\mu < \infty$ be the minimal degree of such points, we will show that also $\nu(S) = \mu$, hence $S \neq \mathcal{O}$. Let N be the set of n's achieving this minimum, i.e. $\nu(h_{nm}g_{nm}) = \mu$ if $n \in N$, and $\nu(h_{nm}g_{nm}) > \mu$ otherwise. Since $\nu(g_{nm}) = m$ by construction, then by Lemma 6.12 there is $i \in \mathbb{N}$ such that for every $n \in N$ there exists $h_n \in \mathbb{N}$ with $(h_n, p) = 1$, and satisfying $h_{nm} = h_np^i$, and $mp^i = \mu$. By Lemma 6.6 this implies

$$S_x = \psi_p(p)^i \left(\sum_{n\in N} h_n\gamma_n\right)\epsilon^\mu \bmod \epsilon^{\mu+1}.$$

Since $\psi_p(p) \in R_k^*$ by assumption (6) and $\sum_{n\in N} h_n\gamma_n$ is a non-zero element of $\mathbb{F}_q$, then we conclude that $\nu(S_x) = \mu < \infty$, so $S \neq \mathcal{O}$. Moreover, by Lemma 6.15 we have $\mathrm{trj}(S) = \{\mu p^i\}_{i<l_\mu}$, which is contained in $\{mp^j\}_{j<l_m}$ as $\mu = mp^i$. □

Theorem 6.19. *Let E be an elliptic curve over R_k satisfying the condition* (6)*. Then*

$$E^\infty \cong \prod_{\substack{1\le m\le k-1\\(m,p)=1}} \left(\mathbb{Z}_{p^{l_m}}\right)^e.$$

Proof. Let $\{\gamma_n\}_{1\le n\le e}$ be an $\mathbb{F}_p$-basis of $\mathbb{F}_q$. For every $1 \le n \le e$ and $1 \le m \le k-1$ such that $(m,p) = 1$, we define

$$g_{nm} = \left(\gamma_n \epsilon^m : 1 : \mathtt{f}(\gamma_n \epsilon^m)\right) \in E^\infty,$$

as in Proposition 6.18. We will show that these points are linearly independent and generate the whole E^∞.

Let us assume that there are $\{h_{nm}\}_{n,m} \subset \mathbb{N}$ such that

$$\sum_{(m,p)=1}^{k-1} \sum_{n=1}^{e} h_{nm} g_{nm} = \mathcal{O}.$$

By Proposition 6.18 we have

$$\mathrm{trj}\left(\sum_{n=1}^{e} h_{nm} g_{nm}\right) \subseteq \{mp^j\}_{j<l_m},$$

which are all disjoint for $(m,p) = 1$. Thus, by repeatedly applying Lemma 6.11, we conclude that $\sum_{n=1}^{e} h_{nm} g_{nm} = \mathcal{O}$ for all the considered m. But for every fixed m, the point g_{nm} are linearly independent by Proposition 6.18, therefore we conclude that $g_{nm} = \mathcal{O}$, for every considered n and m.

By Lemma 6.13 we have $\mathrm{ord}(g_{nm}) = p^{l_m}$, therefore

$$\prod_{\substack{1\le m\le k-1\\(m,p)=1}} \left(\mathbb{Z}_{p^{l_m}}\right)^e \cong \langle g_{nm}\rangle_{n,m} \subseteq E^\infty.$$

The conclusion follows by comparing the sizes, since $\#\mathbb{Z}^e_{p^{l_m}} = q^{l_m}$ and by Lemma 6.17 we have

$$\prod_{\substack{1\le m\le k-1\\(m,p)=1}} q^{l_m} = q^{k-1},$$

which is precisely $\#E^\infty$. □

Corollary 6.20. *Let E be an elliptic curve over R_k satisfying the conditions* (5) *and* (6)*. Then*

$$E \cong E(\mathbb{F}_q) \times \prod_{\substack{1\le m\le k-1\\(m,p)=1}} \left(\mathbb{Z}_{p^{l_m}}\right)^e, \quad \text{where} \quad l_m = \left\lfloor \log_p \frac{k-1}{m} \right\rfloor + 1.$$

Proof. Under condition (5) we know that

$$E(R_k) \cong E(\mathbb{F}_q) \oplus E^\infty,$$

while under condition (6) the group structure of E^∞ is given by Theorem 6.19. □

Since both the conditions (5) and (6) are satisfied with overwhelming probability for large primes p, the group structure of a generic elliptic curve over R_k is the one given by Corollary 6.20.

6.2. **Exceptional case.** For some special choices of the curve coefficients $a_1, \dots, a_6 \in R_k$, the condition (6) may not hold. In this final section, we examine these cases, namely we will always assume that

$$\epsilon \mid \psi_p(p).$$

This heuristically happens with a probability slightly higher than $1/p$ (Section A.5). Moreover, if we fix the a_i in F_q (for example when lifting a curve in F_q) it cannot happen that $\epsilon|\psi_p(p)$, but only $\psi_p(p) = 0$. In this case, Proposition 6.2 can be slightly extended, as follows.

Proposition 6.21. *Let E be an elliptic curve over R_k with $k \leq p+1$. Then we have the group isomorphism*

$$E^\infty \cong (\mathbb{F}_p)^{ek}.$$

Proof. If follows as in Proposition 6.2, since every point of E^∞ has order p by Corollary 6.1. □

The following example shows why Theorem 6.19 does not hold in this case: depending on the value of $\psi_p(p)$, the points may have different trajectories. However, as long as they remain disjoint, the group structure can still be computed.

Example 6.22. Let us consider $q = p = 3$ and $k = 20$, namely the ring $\mathcal{R} = \mathbb{F}_3[x]/(x^{20}) \simeq \mathbb{F}_3[\epsilon]$, and the curve E defined over $\mathcal{R}$ by

$$y^2z + \epsilon^4 xyz = x^3 + \epsilon^8 x^2 z + xz^2.$$

One can check that $\Delta_E \in \mathcal{R}^*$, hence E is an elliptic curve. We obtain $\psi_3(3) = 2\epsilon^8$ and $\psi_9(3) = 2+\epsilon^{16}$, while all the other $\psi_i(3)$ for $i < 9$ are equal to 0. Since $\nu\big(\psi_3(3)\big) = 8$, this is the exceptional case, so Theorem 6.19 does not hold anymore, but we will see that a slight modification of it does. For $1 \leq m \leq 19$, the trajectories of the points $P_m = \big(\epsilon^m : 1 : \mathtt{f}(\epsilon^m)\big)$ are

$$\mathrm{trj}(P_1) = \{1, 9\}, \quad \mathrm{trj}(P_2) = \{2, 14\}, \quad \mathrm{trj}(P_3) = \{3, 17\},$$

while all the other P_m have order 3 (hence $\mathrm{trj}(P_m) = \{m\}$). In fact, the triple of a generic $P = \big(X : 1 : \mathtt{f}(X)\big) \in E^\infty$ satisfies

$$(3P)_x \equiv \psi_3(3)X^3 + \psi_9(3)X^9 \bmod X^{10}.$$

If we call $m = \nu(P)$, then there are only two possibilities for $\nu(3P)$:

- if $3m + 8 < 9m$, the power of ϵ with minimal degree arises from $\psi_3(3)X^3$, hence $\nu(3P) = 3m + 8$;
- otherwise, the minimal degree arises from X^9, as $\psi_9(3) \in \mathcal{R}^*$, therefore in this case $\nu(3P) = 9m$.

Thus, we define the set $\mathcal{A} = \{1 \dots 19\} \backslash \{9, 14, 17\}$, and the integers $l_1 = l_2 = l_3 = 2$, while $l_m = 1$ for all the other $m \in \mathcal{A}$. The trajectories of the $\{P_m\}_{m\in\mathcal{A}}$ are all disjoint, hence we can follow the proof of Proposition 6.18 to show that the P_i are linearly independent. The group they generate is

$$G = \prod_{m\in\mathcal{A}} \mathbb{Z}_{p^{l_m}}.$$

As in the proof of Lemma 6.17, we have $\sum_{m\in\mathcal{A}} l_m = 19 = k - 1$, since the trajectories of the P_m for $m \in \mathcal{A}$ partition the set $\{1, ..., 19\}$ by construction. This implies that G has exactly p^{k-1} elements, hence it is the whole E^∞. More details on the explicit computations can be found in the Appendix (Example A.6).

The main idea of Theorem 6.19 is finding points with non-intersecting trajectories, which will generate E^∞. Example 6.22 shows that this idea may also be adapted to the exceptional case. We recall that in this case it holds $\nu\big(\psi_p(p)\big) = d > 0$. Moreover, we assume that the following three conditions hold.

(C_1) $\psi_{p^2}(p) \in R_k^*$,

(C_2) $\psi_i(p) = 0$ for all $i < p^2$ such that $(i, p) = 1$,
(C_3) $\psi_i(p) \in \langle \psi_p(p) \rangle$ for all $i < p^2$ such that $p|i$.

We will show that under these conditions we can compute the group structure of E^∞ as we did in the main case. After that, we verify that these conditions always hold within the reach of our computations.

Lemma 6.23. *Let $P \in E^\infty$ be a point. We have*

$$\nu(pP) = \min\{p^2\nu(p), p\nu(p) + d\}.$$

Proof. All the $\psi_i(p)$ with $i < p^2$ are either 0 if $(i, p) = 1$ for (C_2), or multiple of $\psi_p(p)$ if $p|i$ for (C_3). Moreover, every $i > p^2$ cannot be the minimal degree of pP since $\psi_{p^2}(p) \in R_k^*$ for (C_1). Therefore, $\nu(pP)$ is always determined by the minimal degree of $\psi_p(p)X^p$ (which is $p\nu(P) + d$) or that of $\psi_{p^2}(p)$ (which is $p^2\nu(P)$). □

Remark 6.24. *Notice that when $\psi_p(p) = 0$, then $\nu(pP) = p^2\nu(P)$ regardless of $\nu(P)$. This case is the easiest exceptional case, as we know precisely the value of $\nu(pP)$.*

Lemma 6.25. *Let $P, Q \in E^\infty$ be two points such that $\nu(P) = \nu(Q)$. It holds* $\operatorname{trj}(P) = \operatorname{trj}(Q)$.

Proof. Thanks to Lemma 6.23, the trajectory of a point is only determined by its minimal degree. Since $\nu(P) = \nu(Q)$, the thesis follows. □

Lemma 6.26. *Let $P, Q \in E^\infty$ be two points with $\nu(P) < \nu(Q)$. Then*

- *if $\nu(Q) \in \operatorname{trj}(P)$, then $\operatorname{trj}(Q) \subseteq \operatorname{trj}(P)$;*
- *otherwise $\operatorname{trj}(P) \cap \operatorname{trj}(Q) = \emptyset$.*

Proof. The first part is a trivial application of Lemma 6.25. If $\nu(Q) \notin \operatorname{trj}(P)$, let us assume by contradiction that $\operatorname{trj}(P) \cap \operatorname{trj}(Q) \neq \emptyset$. This means that there are two points, multiples of P and Q respectively (we take without loss of generality P and Q themselves) such that $\nu(P) \neq \nu(Q)$ but $\nu(pP) = \nu(pQ)$. By Lemma 6.23, there are four possibilities:

- $p^2\nu(P) = p^2\nu(Q)$;
- $p\nu(P) + d = p\nu(Q) + d$;
- $p^2\nu(P) = p\nu(Q) + d$ or $p^2\nu(Q) = p\nu(P) + d$.

The first two are clearly impossible since $\nu(P) \neq \nu(Q)$. The latter are symmetric, so let us assume $p^2\nu(P) = p\nu(Q) + d$. It is clear that in this case $p|d$, hence we can write $p\nu(P) = \nu(Q) + h$ where $ph = d$. Moreover, Lemma 6.23 implies the existence of a solution to

$$\begin{cases} p\nu(P) = \nu(Q) + h, \\ p\nu(P) < \nu(P) + h. \end{cases}$$

The above system implies $\nu(Q) < \nu(P)$, which contradicts the hypothesis $\nu(P) < \nu(Q)$. □

From now on, we will employ the notation of Proposition 6.18, i.e.

$$g_{nm} = \left(\gamma_n \epsilon^m : 1 : \mathtt{f}(\gamma_n \epsilon^m)\right) \in E^\infty$$

where $\{\gamma_n\}_{1 \le n \le e}$ is an $\mathbb{F}_p$-basis of $\mathbb{F}_q$.

Definition 6.27. *We denote the set*

$$\mathcal{A} = \{1 \le m \le k - 1 | \operatorname{trj}(g_{1m}) \cap \operatorname{trj}(g_{1i}) = \emptyset \ \forall 1 < i < m\},$$

Moreover, for every $m \in \mathcal{A}$ we define

$$l_m = \#\operatorname{trj}(g_{1m}).$$

Remark 6.28. *For any $1 \le n \le e$, we could have chosen g_{nm} instead of g_{1m}. Indeed, the choice of n is irrelevant by Lemma 6.25, since $\nu(g_{nm}) = m$ for every n.*

Lemma 6.29. *With the above notation, we have*

- $\operatorname{ord}(g_{nm}) = p^{l_m}$ *for every* $1 \leq n \leq e$*;*
- $\sum_{m\in\mathcal{A}} l_m = k-1$.

Proof. By definition the trajectory of g_{nm} has l_m elements, so the first power of p that annihilates it is p^{l_m}. Since E^∞ is a p-group, then p^{l_m} is the order of g_{nm}.

As for the second part, we notice that the definition of $\mathcal{A}$ together with Lemma 6.26 imply that for every $1 \leq n \leq e$, we have the disjoint union

$$\bigsqcup_{m\in\mathcal{A}} \operatorname{trj}(g_{nm}) = \{1, \dots, k-1\}.$$

Since by definition of $l_m = \#\operatorname{trj}(g_{nm})$, then the thesis follows. □

Proposition 6.30. *For any given* $1 \leq m \leq k-1$*, the points*

$$g_{nm} = \big(\gamma_n \epsilon^m : 1 : f(\gamma_n \epsilon^m)\big) \in E^\infty$$

are linearly independent. Moreover, the trajectory of every linear combination of the $\{g_{nm}\}_{1\leq n\leq e}$ *is a subset of* $\operatorname{trj}(g_{1m})$.

Proof. We can follow the same argument of Proposition 6.18. Notice that the minimum degree of $(pP)_x$ can now be determined by either the degree d term of $\psi_p(p)$ or $\psi_{p^2}(p)$. In both cases, the coefficient multiplying the point lies in R_k^*. □

Theorem 6.31. *Let* E *be an elliptic curve defined over* R_k*, such that* $\nu\big(\psi_p(p)\big) = d > 0$ *and the conditions* (C_1)*,* (C_2) *and* (C_3) *are satisfied. Then we have the group isomorphism*

$$E^\infty \cong \prod_{m\in\mathcal{A}} \left(\mathbb{Z}_{p^{l_m}}\right)^e.$$

Proof. We can follow again the proof of Theorem 6.19, with the $\{g_{nm}\}_{m\in\mathcal{A},1\leq n\leq e}$ as generators. Proposition 6.30 gives us the independence, while Lemma 6.29 gives us both the structure of the group they generate and the counting argument to show that it is the whole E^∞. □

Remark 6.32. *In the main case (Section 6.1), condition* (C_1) *is satisfied by* $\psi_p(p)$ *instead of* $\psi_{p^2}(p)$*, so the minimal degree may only arise from* $i \leq p$*. In this setting, Condition* (C_2) *holds thanks to Corollary 5.14, while condition* (C_3) *becomes trivial.*

Proposition 6.33. *Let* $p \in \{2, 3\}$ *and* E *be an elliptic curve over* R_k *such that* $\psi_p(p) \notin R_k^*$*. Then conditions* (C_1)*,* (C_2) *and* (C_3) *are always satisfied.*

Proof. Direct computation (see Lemma A.7). □

Remark 6.34. *By Proposition 6.33, when* $p \in \{2, 3\}$ *the group structure of* E^∞ *is given by either Theorem 6.19 or Theorem 6.31. For all the other* p*, we may work without loss of generality with the short Weierstrass forms, i.e.* $a_1 = a_2 = a_3 = 0$*. A direct computation (Lemma A.7) shows that conditions* (C_1)*,* (C_2) *and* (C_3) *are actually satisfied for every* $p \leq 13$.

6.3. **ECDLP.** Given the coordinates of a point $P \in E$ and those of its multiple $Q = nP$, the discrete logarithm problem amounts to efficiently compute such $n \in \mathbb{Z}$. The supposed high complexity of the discrete logarithm problem over elliptic curves is the underlying assumption of several cryptographic protocols.

From the results of the current paper, we efficiently recover the discrete logarithm of points in E^∞ over R_k. In fact, we can always write $n = b_0 + b_1 p + \cdots + b_{k-1}p^{k-1}$. Let $m_i = \nu(p^i P)$. By a repeated application of Lemma 6.6 (or Lemma 6.23 in the exceptional case), we have

$$b_i = \left(\Big(Q - \sum_{j=1}^{i-1} b_j p^j P\Big)_x \bmod \epsilon^{m_i+1}\right) \Big/ \big((p^i P)_x \bmod \epsilon^{m_i+1}\big).$$

The time complexity of this algorithm is logarithmic in the considered parameters. More precisely, it has a time complexity of $\log(p)\log(n)$ (see Section A.6 in the appendix).

The above procedure efficiently reduces the discrete logarithm problem over R_k to the corresponding problem over $\mathbb{F}_q$. For this reason, we do not see practical advantages in basing elliptic curve discrete logarithm problems on these families of curves.

Appendix A. Explicit computations

In this section, we give further details and results on some computations omitted for brevity in the paper. Most of the results are obtained using MAGMA [2]. All the referenced source code can be found at [6].

A.1. Efficient addition law.

Proposition A.1. *Let us follow the notation of Proposition 3.2. The coefficients such that*

$$X_1 = g_1H_1 + g_2H_2, \quad Z_3 = g_1H_3 + g_2H_4, \quad Y_3 = H_1H_4 - H_2H_3$$

are

$$\begin{aligned}
H_1 =& - a_1a_3X_1Z_2 - a_3^2Z_1Z_2 + a_1X_2Y_1 - a_2X_1X_2 - a_4X_2Z_1 - a_4X_1Z_2 - 3a_6Z_1Z_2 + Y_1Y_2,\\
H_2 =& - a_2a_3^2Z_1Z_2 + a_1a_3a_4Z_1Z_2 - a_1^2a_6Z_1Z_2 - a_3^2X_1Z_2 + a_4^2Z_1Z_2 - 4a_2a_6Z_1Z_2 + a_3X_2Y_1\\
& - a_4X_1X_2 - 3a_6X_2Z_1 - 3a_6X_1Z_2,\\
H_3 =& \; a_1^2X_1Z_2 + a_1a_3Z_1Z_2 + a_1Y_1Z_2 + a_2X_2Z_1 + a_2X_1Z_2 + a_4Z_1Z_2 + 3X_1X_2,\\
H_4 =& \; a_1a_3X_1Z_2 + a_3^2Z_1Z_2 + a_2X_1X_2 + a_3Y_1Z_2 + a_4X_2Z_1 + a_4X_1Z_2 + 3a_6Z_1Z_2 + Y_1Y_2.
\end{aligned}$$

Proof. The explicit verification of the above equalities in Magma may be found in the file `short_sum_verification.magma`. □

A.2. The polynomial `f`.

Proposition A.2. *Let $\mathtt{f} \in \mathcal{R}[x]$ be the polynomial as defined in Proposition 4.2. We have*

$$\begin{aligned}
\mathtt{f}(x) \equiv\; & x^3 - a_1x^4 + (a_1^2 + a_2)x^5 - (a_1^3 + 2a_1a_2 + a_3)x^6 +\\
& (a_1^4 + 3a_1^2a_2 + 3a_1a_3 + a_2^2 + a_4)x^7 - (a_1^5 - 4a_1^3a_2 - 6a_1^2a_3 - 3a_1a_2^2 - 3a_1a_4 - 3a_2a_3)x^8 +\\
& (a_1^6 + 5a_1^4a_2 + 10a_1^3a_3 + 6a_1^2a_2^2 + 6a_1^2a_4 + 12a_1a_2a_3 + a_2^3 + 3a_2a_4 + 2a_3^2 + a_6)x^9 \bmod x^{10}.
\end{aligned}$$

Proof. The explicit expression for `f` is obtained by applying the method described in the proof of Proposition 4.2. Python scripts implementing that logic can be found in the files `zfx_fast.py` (for the extended form) and `zfxred_fast.py` (for the short form). □

Remark A.3. *Values of $\mathtt{f}(x)$ when $k = 30$ (extended form) and $k = 300$ (short form) may be found in `zfx_stored_30.magma` and `zfxred_stored_300.magma`, respectively. We remark that these scripts can handle even $k = 150$ (extended) and $k = 2000$ (short) in a reasonable time on a commercial laptop. However, the main purpose of these polynomials is to be employed for computing $\psi_i(n)$ (see below). For this reason, the values $k = 30$ and $k = 300$ are considered enough.*

We observe that, when $\mathrm{char}(\mathbb{F}_q) \nmid 6$, we can represent an elliptic curve in its short Weierstrass form, with $a_1 = a_2 = a_3 = 0$, $a_4 = A$ and $a_6 = B$. With this notation, we obtain the same result as [12, Prop. 11], i.e.

$$\mathtt{f}(x) \equiv x^3 + Ax^7 + Bx^9 \bmod x^{10}.$$

A.3. Semi-linearity of the sum.

Proposition A.4. *Let $P_1 = (X_1 : 1 : Z_1), P_2 = (X_2 : 1 : Z_2) \in E^\infty$ be two points and $P_3 = P_1 +_{(0:1:0)} P_2$. Let also $I_P = \langle X_1^2, Z_1\rangle$. Then*

$$(P_3)_x \equiv X_1 + X_2 + \big(a_1X_2 - a_2X_2^2 + 2a_3Z_2 - 2a_4X_2Z_2 - 3a_6Z_2^2\big)X_1 \bmod I_P.$$

Proof. Notice that, in accordance with previous notations, $(P_3)_x$ is the x coordinate of P_3 in standard form while X_3 and Y_3 are the results of the addition as defined in [3]. By Proposition 3.2 we have

$$\begin{aligned}
g_1 &\equiv X_1 + X_2 + a_1X_1X_2 + a_3X_1Z_2 \mod I_P,\\
g_2 &\equiv Z_2 \mod I_P,
\end{aligned}$$

while Proposition A.1 gives

$$\begin{aligned} H_1 &\equiv 1 - a_2X_1X_2 - a_4Z_2X_1 + a_1X_1 \mod I_P,\\ H_2 &\equiv -a_4X_1X_2 - 3a_6X_1Z_2 + a_3X_1 \mod I_P,\\ H_3 &\equiv 3X_1X_2 + a_2X_1Z_2 \mod I_P,\\ H_4 &\equiv 1 + a_2X_1X_2 + a_4X_1Z_2 \mod I_P. \end{aligned}$$

Computing the addition we obtain

$$\begin{aligned} X_3 &\equiv X_1 + X_2 - a_2X_2^2X_1 - 2a_4X_1X_2Z_2 + 2a_1X_1X_2 + 2a_3X_1Z_2 - 3a_6X_1Z_2^2 \mod I_P,\\ Y_3 &\equiv 1 + a_1X_1 \mod I_P. \end{aligned}$$

From here it is clear that the inverse modulo I_P of Y_3 is $1 - a_1X_1$. Multiplying it by X_3 we obtain the required expression for $(P_3)_x$. Explicit computations can be found in `inspection.magma`. □

Proposition A.5. *Let $P_1 = (X_1 : 1 : Z_1), P_2 = (X_2 : 1 : Z_2) \in E^\infty$ be two points and $P_3 = P_1 +_{(0:1:0)} P_2$. Let also $m = \min\{\nu(P_1), \nu(P_2)\}$. Then we have*

$$(P_3)_x \equiv X_1 + X_2 \bmod \epsilon^{m+1}.$$

Proof. It follows from Proposition A.4, by noting that $\epsilon^{m+1} | X_1^2$ and $\epsilon^{m+1} | Z_1$, hence $I_P \subseteq \langle \epsilon^{m+1} \rangle$ and ϵ^{m+1} divides both X_1X_2 and X_1Z_2, so the third term of the expression of $(P_3)_x$ given by Proposition A.4 is $0 \bmod \epsilon^{m+1}$. □

A.4. **Computing $\psi_i(n)$.** Let $P = (X : 1 : \mathtt{f}(X)) \in E^\infty$. Thanks to Proposition A.2 we know the symbolic expression of $\mathtt{f}$ for a fixed k. The i-th multiplication polynomial $\psi_i(n)$ is the coefficient of X^i in $(nP)_x$, which by Theorem 5.9 it is a polynomial of degree i in n.

To compute it we derive the symbolic expression of nP as a function of X for $1 \le n \le i+1$, and for every monomial expression in $a_1, \dots, a_6$, we fit a degree-i polynomial on its coefficients. This is a standard technique for Faulhaber formulas, see [5]. Once we have the interpolated expression for $\psi_i(n)$, we can also validate it: we just check that $(n-1)P + P = np$, where $(n-1)P$ and nP are expressed through the previously computed $\psi_i(n)$. We remark that on all the computations regarding $\psi_i(n)$ we may assume $k = i + 1$.

A script performing this operation can be found in `ind.magma` and `indred.magma`. The parameter k can be modified, while setting `proof=true;` verifies every computed ψ_i. The first few values of ψ_i in the extended form can be found in `psi_stored_30.magma`. The first ones, rearranged, are reported below:

$$\begin{aligned} \psi_1 &= n,\\ \psi_2 &= \binom{n}{2} a_1,\\ \psi_3 &= \binom{n}{3} a_1^2 - 2\binom{n+1}{3} a_2,\\ \psi_4 &= \binom{n}{4} a_1^3 - \binom{n+1}{3}(2n-3)a_1a_2 + \frac{n(n^3-1)}{2} a_3. \end{aligned}$$

The first few values for the short Weirstrass form can be found in `psired_stored_222.magma`. The first nonzero values are reported below:

$$\begin{aligned}\psi_1 &= n,\\ \psi_5 &= -\frac{2}{5}An(n^4-1),\\ \psi_7 &= -\frac{3}{7}Bn(n^6-1),\\ \psi_9 &= \frac{2}{15}A^2(n^4-1)(n^4-5).\end{aligned}$$

A.5. **The exceptional case.** Due to the structure of our rings R_k, a curve E is exceptional if and only if $\pi\big(\psi_p(p)\big) = 0$. For this reason, for every prime p we count the zeros of $\psi_p(p)$ among the non-singular choices of the curve coefficients. For computational reasons, we assume $p > 5$ so we work with the short Weierstrass form. The code can be found in `except_coeff.magma`, while results for primes up to $p = 79$ can be found in Table 1.

p	rate	p	rate	p	rate	p	rate
5	1/5	7	1/7	11	2/11	13	1/13
17	2/17	19	2/19	23	3/23	29	3/29
31	3/31	37	1/37	41	4/41	43	2/43
47	5/47	53	3/53	59	6/59	61	3/61
67	2/67	71	7/71	73	2/73	79	5/79

TABLE 1. Rate of exceptional cases.

Example A.6. Let E be the elliptic curve over R_k as defined in Example 6.22. In `ex1.magma` we perform some computations to verify our claims. First of all, we directly compute the coefficients $\psi_3(3)$ and $\psi_9(3)$, which as shown in Theorem 6.31 are enough to determine the group structure. After that, we pick random points and show how their minimal degree changes when multiplied by 3. Finally, we compute the trajectory of $g_m = \big(\epsilon^m : 1 : \mathtt{f}(\epsilon^m)\big)$ for every $m \in \mathcal{A}$, namely every m not contained in the trajectory of any g_n for $n < m$.

Lemma A.7. *Let $p \leq 13$ and E be an elliptic curve defined over R_k, such that $\nu\big(\psi_p(p)\big) = d > 0$. Then conditions (C_1), (C_2), and (C_3) of Theorem 6.31 are always satisfied.*

Proof. The cases $p \in \{2, 3\}$ can be found in `proof_23.magma`. Conditions (C_2) and (C_3) can be directly computed. For condition (C_1) is enough to check that for both $p = 2, 3$ we symbolically have $\Delta_E \in \langle \psi_p(p), \psi_{p^2}(p)\rangle$ (where Δ_E is the discriminant of the curve E), and since $\psi_p(p) \notin R_k^*$ and $\Delta_E \in R_k^*$, we must have $\psi_{p^2}(p) \in R_k^*$.
Notice that for $5 \leq p \leq 13$ we can restrict ourselves to work with a short Weierstrass form. Again (C_2) and (C_3) are directly computed. (C_1) is similarly implied by verifying that

$$\Delta_E \in \langle A, B\rangle \subseteq \sqrt{\langle \psi_p(p), \psi_{p^2}(p)\rangle},$$

thus $\psi_p(p)$ and $\psi_{p^2}(p)$ cannot both belong to $\mathfrak{m}$.
Explicit computations can be found in `proof_short.magma`. □

A.6. **ECDLP.** We provide here further details about the algorithm introduced in Section 6.3. As already shown, we must compute

$$b_i = \left(\Big(Q - \sum_{j=1}^{i-1} b_j p^j P\Big)_x \bmod \epsilon^{m_i+1}\right) \Big/ \big((p^i P)_x \bmod \epsilon^{m_i+1}\big).$$

To entirely determine n, we compute the $\log_p(n)$ digits b_i of its base-p representation. If we store the partial sum $S_i = \sum_{j=1}^{i} b_j p^j P$ and the point $p^i P$, at every step we can compute b_i using only two point multiplication, since $S_{i+1} = S_i + b_{i+1} p^{i+1} P$ and $p^{i+1} P = p(p^i P)$. Notice that we multiply by $b_i < p$ and p respectively, so these multiplication have complexity $\log(p)$. The inversion is done in $\mathbb{F}_q$ (hence a field operation), so the whole algorithm has complexity $\log(p)\log(n)$. The implemented algorithm, as well as the actual recovery of n for random choices of E and p, can be found in `d_log.magma`.

References

[1] Daniel J Bernstein and Tanja Lange. A complete set of addition laws for incomplete edwards curves. *Journal of Number Theory*, 131(5):858–872, 2011.

[2] Wieb Bosma, John Cannon, and Catherine Playoust. The magma algebra system i: The user language. *Journal of Symbolic Computation*, 24(3-4):235–265, 1997.

[3] Wieb Bosma and Hendrik W. Lenstra. Complete systems of two addition laws for elliptic curves. *Journal of Number theory*, 53(2):229–240, 1995.

[4] Ronald L Graham, Donald E Knuth, Oren Patashnik, and Stanley Liu. Concrete mathematics: a foundation for computer science. *Computers in Physics*, 3(5):106–107, 1989.

[5] David S Gunderson and Kenneth H Rosen. *Handbook of Mathematical Induction*. CRC Press LLC, Boca Raton, Florida US, 2010.

[6] Riccardo Invernizzi and Daniele Taufer. Elliptic curves over local rings. `https://github.com/r98inver/ec-local-rings`, 2023.

[7] Don Johnson, Alfred Menezes, and Scott Vanstone. The elliptic curve digital signature algorithm (ecdsa). *International Journal of Information Security*, 1:36–63, 2001.

[8] Neal Koblitz. Modular elliptic curves and fermat's last theorem. *Mathematics of computation*, 48(177):203–209, 1987.

[9] Hendrik W. Lenstra. Elliptic curves and number-theoretic algorithms. *Proceedings of the International Congress of Mathematicians*, 1986:99–120, 1986.

[10] Ralph C. Merkle. Secure communications over insecure channels. *Communications of the ACM*, 21(4):294–299, 1978.

[11] Victor S. Miller. Use of elliptic curves in cryptography. *Advances in Cryptology — CRYPTO '85 Proceedings*, 218:417–426, 1985.

[12] Massimiliano Sala and Daniele Taufer. The group structure of elliptic curves over z/nz. *arXiv preprint arXiv:2010.15543*, 2020.

[13] Massimiliano Sala and Daniele Taufer. Elliptic loops. *ArXiv:2204.08019*, 2022.

[14] Massimiliano Sala and Daniele Taufer. A survey on the group of points arising from elliptic curves with a weierstrass model over a ring. *International Journal of Group Theory*, 12(3):177–196, 2023.

[15] Takakazu Satoh and Kiyomichi Araki. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. *Commentarii Mathematici Universitatis Sancti Pauli*, 47(1):81–92, 1998.

[16] Igor E. Shparlinski. Pseudorandom number generators from elliptic curves. *Contemporary Mathematics*, 477:121–142, 2009.

[17] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, Berlin, 2009.

[18] Nigel P. Smart. The discrete logarithm on elliptic curves of trace one. *Journal of Cryptology*, 12:193–196, 1999.

[19] Andrew Wiles. Modular elliptic curves and fermat's last theorem. *Annals of Mathematics*, 142(3):443–551, 1995.

Department of Computer Science,, KU Leuven, Celestijnenlaan 200A, Leuven, Belgium
Email address, R. Invernizzi: `riccardo.invernizzi@student.kuleuven.be`
URL, R. Invernizzi: `https://orcid.org/0000-0002-2271-6822`

Department of Computer Science,, KU Leuven, Celestijnenlaan 200A, Leuven, Belgium
Email address, D. Taufer: `daniele.taufer@kuleuven.be`
URL, D. Taufer: `https://orcid.org/0000-0003-3402-4863`