Elliptic Loops

Daniele Taufer

Supervisor: Prof. Massimiliano Sala

A Research Thesis
Submitted in Partial Fulfillment of the Requirements for the
Doctor of Philosophy Degree in Mathematics

Faculty of Mathematics
University of Trento
May, 2020

ABSTRACT

Given an elliptic curve $\mathcal{E}$ over $\mathbb{F}_p$ and an integer $e \geq 1$, we define a new object, called "elliptic loop", as the set of points in $\mathbb{P}^2(\mathbb{Z}/p^e\mathbb{Z})$ lying over $\mathcal{E}$, endowed with an operation inherited by the curve addition. This object is proved to be a power-associative abelian algebraic loop. Its substructures are investigated by means of other algebraic cubics defined over the same ring, which we named "shadow curve" and "layers". When $\mathcal{E}$ has trace 1, a distinctive behavior is detected and employed for producing an isomorphism attack to the discrete logarithm on this family of curves. Stronger properties are derived for small values of e, which lead to an explicit description of the infinity part and to characterizing the geometry of rational $|\mathcal{E}|$-torsion points.

To Massimiliano and Nicolò,
for their constant support, which has turned
a strenuous fight into an amusing affair.

TABLE OF CONTENTS

INTRODUCTION

MOTIVATION

Elliptic curves have been providing number theory with a fertile field of intense research for the last century, even though these objects are rooted in the much older *Arithmetica*[1] of Diophantus. Although their definition is fairly accessible, their grasp has proven to be remarkably challenging, as it often happens to fundamental entities in mathematics.

Over the last decades, the increasing knowledge of these curves has led to terrific conjectures and results. Among them, some instances that are certainly worth to be mentioned are Mordell's Theorem, conjectured by Poincaré and proved in 1922 [52], the positive solution to the Torsion Conjecture proposed by Ogg, settled for any elliptic curves from 1977 to 1996 by Mazur, Kamienny and Merel [48, 49, 30, 31, 50], and the Taniyama–Shimura Conjecture, named Modularity Theorem after being demonstrated by Wiles, Breuil, Conrad, Diamond and Taylor [76, 19, 16, 11] from 1995 to 2001. The latter has grown a huge attention since it had led to a proof of the celebrated Fermat's Last Theorem [76, 69], an emblematic breakthrough that witnesses the deep role played by these fascinating curves in arithmetic geometry. Despite the research on these objects is becoming more and more sophisticated, it is far from being completed: many other conjectures with stunning implications are still open, such as those of Birch and Swinnerton-Dyer or Szpiro, and many others may notably see the light in the years to come.

Not to mention the overwhelming impact that elliptic curves had on the algorithmic community: from 1985 they have been applied, among others, to square roots computing over finite fields [59], primality testing [10, 14, 21, 3] and integer factorization [43].

As for cryptography, the applications of elliptic curves are incalculable. From the early 80s, when Miller and Koblitz had envisioned the use of their points as base group for cryptosystems, these objects have had an all-embracing spread: key exchange and key agreement [51], encryption and decryption [32], digital signature [29] and authentication [63] are only few among the schemes that have benefited from their applications [77]. One of

[1] An English version of this Greek classic may be found in [24]. The problem involving a Weierstrass polynomial is the number 24.

the desirable features provided by these protocols is the capability of maintaining the same level of security with smaller keys with respect to their ancestors. Besides, this attribute makes them a particularly useful tool for the lightweight schemes' design [41]. Further research lines that have been recently seeing florid research are the exploitation of these curves for producing pseudo-random sources [64] and the investigation of isogenies between supersingular elliptic curves, aiming at achieving post-quantum resistance [17].

Given the outstanding range of both theoretical and practical applications of these entities, their understanding has become essential: most of the cryptographic elliptic curves-based protocols rely on the belief that the discrete logarithm problem on their point group (ECDLP) is practically infeasible, an assumption that has proved not to hold for certain families of curves, that need to be carefully avoided consequently.

It is not arduous to realize that the structure and the properties of these objects dramatically depend on their base field, which in this work is always assumed to be finite. What is less evident is that elliptic curves may also be concretely defined over fairly general rings, as remarkably shown by Lenstra [42]. When the considered base ring is the familiar $\mathbb{Z}/N\mathbb{Z}$, this fact has served new cryptographical results [43, 36] and schemes [35, 20], as well as it was used to avoid computation with p-adic numbers during the arithmetic attack to the ECDLP over anomalous curves [56]. However, the theoretical background of the latter algorithm remains solidly based on the properties of these curves over the p-adic field.

The conviction that such an attack shall be viable, even theoretically, only by means of finite arithmetic has moved us, in the first part of the current work, to investigate the group structure of elliptic curves over $\mathbb{Z}/N\mathbb{Z}$, producing a complete classification in terms of their projected components. In fact, we prove (Theorem 2.3.9) that for any non-anomalous elliptic curve $\mathcal{E}$ there is a group isomorphism

$$\mathcal{E}(\mathbb{Z}/N\mathbb{Z}) \simeq \bigoplus_{p|N} \mathcal{E}(\mathbb{F}_p) \oplus \mathbb{Z}/p^{\mathrm{v}_p(N)-1}\mathbb{Z},$$

whereas, if $\mathcal{E}$ is anomalous, both

$$\mathcal{E}(\mathbb{Z}/p^{\mathrm{v}_p(N)}\mathbb{Z}) \simeq \mathbb{Z}/p^{\mathrm{v}_p(N)-1}\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \quad \text{and} \quad \mathcal{E}(\mathbb{Z}/p^{\mathrm{v}_p(N)}\mathbb{Z}) \simeq \mathbb{Z}/p^{\mathrm{v}_p(N)}\mathbb{Z}$$

may occur in the group decomposition of $\mathcal{E}(\mathbb{Z}/N\mathbb{Z})$. This structure suffices to derive, in the cyclic anomalous case, a clear isomorphism attack to efficiently recover the discrete logarithm (Proposition 2.3.12).

Nevertheless, there is still an annoying arbitrariness in the definition of $\mathcal{E}(\mathbb{Z}/p^e\mathbb{Z})$: such a curve may be realized as a lift of $\mathcal{E}(\mathbb{F}_p)$, but many lifts are simultaneously possible. The second part of this work is devoted to addressing this issue by considering a common framework for all the points that legitimately lift a base curve point. Indeed, given an elliptic curve $\mathcal{E}$, we define *elliptic loop* as the subset of $\mathbb{P}^2(\mathbb{Z}/p^e\mathbb{Z})$ made of points that are projected to points of $\mathcal{E}$ modulo p. Under weak assumptions, these objects may be endowed with the curve operation, which turns out to be not associative even in small cases. However, all is not lost: a careful examination shows that these entities are always power-associative abelian algebraic loops (Corollary 3.3.3 and 3.3.8).

The techniques developed for proving such a result (Theorem 3.3.7) have shed light on a special elliptic curve, which is hiding behind the main curve and has almost always trivial intersection with it, so we referred to it as *shadow curve*. A joint use of the curve equation together with its shadow leads to other projective cubics in $\mathbb{P}^2(\mathbb{Z}/p^e\mathbb{Z})$, which we named *layers* as they constitute a complete stratification of the affine part of elliptic loops (Proposition 3.3.13 and 3.3.15). Their group structure is characterized (Theorem 3.5.1), generalizing the behaviour exhibited by elliptic curves over $\mathbb{Z}/N\mathbb{Z}$.

A different story appears in the infinity part of these loops, which is proved to constitute itself a loop generated by two of its cyclic subgroups (Theorem 3.4.3).

Furthermore, stronger results are proved for elliptic loops over $\mathbb{P}^2(\mathbb{Z}/p^e\mathbb{Z})$ with small values of e, which are discussed in the last part of the current manuscript. The infinity part is a proper group whenever $e \leq 5$, with an explicit description if $e \leq 3$ (Proposition 4.2.1 and 4.3.1). Moreover, when $e \leq 2$ several weak forms of associativity hold, with remarkable consequences in the smallest non-trivial case ($e = 2$). In fact, in such case, they underlie the geometry of the $|\mathcal{E}|$-torsion points lying over a fixed point (Theorem 4.5.2), as well as layers' maximality (Proposition 4.5.6).

Besides, connections with existing works and future research lines are outlined in the last part of the manuscript.

CONTENTS ORGANIZATION

The present introduction is meant to motivate and cover the standard notation and results employed in this work, as far as clarifying stylistic choices.

In Chapter 1 we recall some known results about elliptic curves over finite fields, with a special focus on their addition law and group structure, which constitute key ingredients for the following discussion.

Chapter 2 is devoted to detailing the definition of elliptic curves over $\mathbb{Z}/N\mathbb{Z}$ and to characterizing the groups arisen from this construction. An isomorphism attack working on anomalous elliptic curves is also derived.

Elliptic loops are introduced in Chapter 3 and their associativity properties are discussed. Their structure is detailed in terms of large subgroups that are explicitly determined and characterized.

By adding constraints on the exponent parameter of elliptic loops, in Chapter 4 we derive exceptional situations and stronger results.

Conclusions and open problems are drawn in the final chapter of the work.

METHODOLOGY

An aside is needed about the use of appendices. Throughout the whole work a decisive push towards constructive proofs may be detected, explicit methods are always preferred, if possible. However, sometimes direct approaches are burdensome, so much that the classic "by a straightforward computation" might be jokingly considered full-fledged cheating.

In this view, Appendix A, B and C constitute a substantial part of many crucial results and are located at the end of the present work only for expository reasons. The reader is invited to verify that they are designed to let a calculator performing the very same computations a human could carry out, if it were equipped with an "almost-infinite" amount of time and patience.

Conversely, Appendix D is not needed for the current work but it aims at sketching other relevant results obtained by the author during his Ph.D. studies.

NOVEL CONTRIBUTIONS

In a nutshell, the novelty of the present essay consists of Chapter 3, Chapter 4 and roughly half of Chapter 2. However, to avoid disarray about the contents origination, the results of this work are systematized in the following manner.

- If both the statement and a complete proof of the result have already appeared in the literature, only a precise reference is given.
- If only the statement, or part of it, has appeared in a book or paper, the reference is given but a proof is proposed anyway. The same format is used when the proof is only sketched in the given reference, or when it employs different ideas and techniques.
- If the statement itself is original, no references are included and a proof follows the claimed result.

PRELIMINARIES AND NOTATION

We employ standard algebraic notation and results throughout this work. A comprehensive list of books covering the preliminaries that may serve an interested but not expert reader is [2, 27, 28, 37, 44]. Nonetheless, we find that a notation recap may still be of use, therefore it follows.

Algebraic structures

A *magma* $\mathcal{M}$ is a set equipped with a binary operation. In this work such operation will always be an addition $+ : \mathcal{M} \times \mathcal{M} \to \mathcal{M}$, so we call $\mathcal{M}$ *additive.* When it is commutative, $\mathcal{M}$ is said to be *abelian.*

A *quasigroup* $\mathcal{Q}$ is a magma satisfying the Latin square property, i.e.

$$\forall a, b \in \mathcal{Q}, \quad \exists!\ x, y \in \mathcal{Q} : \begin{cases} a + x = b, \\ y + a = b. \end{cases}$$

A *loop* $\mathcal{L}$ is a quasigroup with identity, i.e. there is $e \in \mathcal{L}$ such that

$$\forall a \in \mathcal{L}, \quad a + e = e + a = a.$$

It is immediate that an associative loop is a group.

Given an additive group G, its exponent $\exp(G)$ is defined as the non-negative generator of the ideal $\{n \in \mathbb{Z} \mid \forall\ g \in G,\ ng = 0\}$.

Let R be a commutative ring with unity and $S \subset R$ be a subset. The *annihilator ideal* of S is defined as

$$\mathrm{Ann}_R(S) = \{r \in R \mid \forall\ s \in S,\ rs = 0\}.$$

The *characteristic* of R is denoted by $\mathrm{char}(R)$ and in this work is always assumed to be

$$\mathrm{char}(R) = \min_{\substack{n \in \mathbb{Z} \\ n \geq 1}} \{n1_R = 0_R\} \neq 2, 3.$$

Let K be a field. The algebraic closure of K is denoted by $\overline{K}$, so that we write $K = \overline{K}$ when the field K is algebraically closed.

Short exact sequences

Let A, B and C be groups and $\phi : A \to B$, $\psi : B \to C$ be group morphisms. If ϕ is injective, ψ is surjective and $\mathrm{Im}\phi = \ker \psi$, then we refer to

$$0 \to A \overset{\phi}{\to} B \overset{\psi}{\to} C \to 0$$

as a *short exact sequence* (of groups). Furthermore, if $B \simeq A \oplus C$, then we call it *split exact sequence* or, in short, we say it *splits*. Given a group X, we denote by $\mathrm{id}_X : X \to X$ its identity morphism. In reference to the above sequence, we say that a group morphism $s_1 : B \to A$ is a *left section* if $s_1 \circ \phi = \mathrm{id}_A$ and similarly a group morphism $s_2 : C \to B$ is called a *right section* if $\psi \circ s_2 = \mathrm{id}_C$. These notions are related by the following well-known result.

Lemma (Splitting Lemma, [47] Proposition I.4.3)**.** *For every short exact sequence, the following are equivalent.*

- *The sequence splits.*
- *There exists a left section.*
- *There exists a right section.*

Divisors

Given a field K and a smooth projective irreducible curve $C = \mathcal{V}(F)$ defined by the irreducible polynomial $f \in K[x, y]$, we define its *rational function field* $K(C)$ as the field of fractions of the integral domain $K[x, y]/(f)$. We also denote by $\mathrm{Div}(C) = \bigoplus_{P \in C} \mathbb{Z} \cdot (P)$ the *group of divisors* on C. The *degree* of a divisor $D = \sum_{P \in C} n_P(P) \in \mathrm{Div}(C)$ is defined as $\deg(D) = \sum_{P \in C} n_P$, and D is called *principal* if there exists $f \in \overline{K}(C)$ such that

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)(P) = D.$$

It is known [67, Corollary 3.5] that if $\mathcal{E}$ is an elliptic curve and $\mathcal{O}$ is its point at infinity, then a divisor $D = \sum_{P \in \mathcal{E}} n_P(P)$ is principal if and only if $\deg(D) = 0$ and $\sum_{P \in \mathcal{E}} n_P P = \mathcal{O}$, where the latter sum is intended to be performed with the addition law of $\mathcal{E}$. In particular, the principal divisors of these curves form a subgroup of

$$\mathrm{Div}^0(\mathcal{E}) = \{D \in \mathrm{Div}(\mathcal{E}) \mid \deg(D) = 0\}.$$

Thus, their quotient is well-defined, it is called 0-*Picard Group* and it is denoted by $\mathrm{Pic}^0(\mathcal{E})$.

Integers and p-adics

Let $n \in \mathbb{Z}$ be an integer. The integers greater or equal than n are denoted by

$$\mathbb{Z}_{\geq n} = \{m \in \mathbb{Z} \mid m \geq n\}.$$

The set of all positive prime integers is denoted by

$$\mathcal{P} = \{p \in \mathbb{Z}_{\geq 1} \mid p \text{ is prime in } \mathbb{Z}\}.$$

Let $p \in \mathcal{P}$ be a prime. For every $n \in \mathbb{Z}$ we denote by

$$\mathrm{v}_p(n) = \begin{cases} \max\left\{e \in \mathbb{Z}_{\geq 0} \bigm| p^e | n\right\} & \text{if } n \neq 0, \\ \infty & \text{if } n = 0, \end{cases}$$

the p-adic valuation of n. This may be used to define the *p-adic norm*

$$\begin{aligned} |\cdot|_p : \mathbb{Q} &\to \mathbb{R}, \\ \frac{n}{m} &\mapsto p^{\mathrm{v}_p(m) - \mathrm{v}_p(n)}. \end{aligned}$$

The completion of $\mathbb{Q}$ with respect to this norm is called the field of *p-adic numbers*, first described in [25] and nowadays denoted by $\mathbb{Q}_p$. The unit disc around $0 \in \mathbb{Q}_p$ is

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \bigm| |x|_p \leq 1\}$$

and it is known as the ring of *p-adic integers*.

When working with extensions and lifts, the following lemma is particularly useful. It holds in more generality, but we state only the version we employ in the current work.

Lemma (Hensel's lemma, [38] Proposition II.2)**.** *Let $f(x) \in \mathbb{Z}[x]$ and $m, k \in \mathbb{Z}_{\geq 1}$ be positive integers with $m \leq k$. For every integer $\bar{n} \in \mathbb{Z}$ such that*

$$f(\bar{n}) \equiv 0 \bmod p^m, \qquad f'(\bar{n}) \not\equiv 0 \bmod p^m,$$

there exists a unique (explicitly computable) integer $0 \leq n \leq p^k - 1$ such that

$$f(n) \equiv 0 \bmod p^k, \qquad n \equiv \bar{n} \bmod p^m.$$

More notation

For any prime $p \in \mathcal{P}$ and positive integer $e \in \mathbb{Z}_{\geq 1}$ we denote the finite field with $q = p^e$ elements by $\mathbb{F}_q$. When the exponent is $e = 1$ we write it as $\mathbb{F}_p$ and we call it a *prime field*. We write $\mathbb{F}_q = \mathbb{F}_p(\alpha)$ when we need to identify a generator α of $\mathbb{F}_q^*$.

Let $r \in \mathbb{R}$ be a real number. We denote by $\lfloor r \rfloor$ the *floor* of r, i.e. the largest integer $n \in \mathbb{Z}$ such that $n \leq r$, and by $\lceil r \rceil$ its *ceiling*, i.e. the smallest integer $n \in \mathbb{Z}$ such that $r \leq n$.

CHAPTER 1
CLASSICAL THEORY OF ELLIPTIC CURVES

1.1 BASIC DEFINITIONS

In this section we define the main objects of our interest, elliptic curves, as they are introduced in classical textbooks [26, 67, 74].

1.1.1 The projective space

Let $n \in \mathbb{Z}_{\geq 0}$ be a non-negative integer and K be a field. There is a well-known equivalence relation $\sim$ on K^{n+1} given by

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \iff \exists\, u \in K^* \ \forall\, i \in \{0, \ldots, n\} \ : \ x_i = uy_i.$$

Definition 1.1.1 (Projective n-space)**.** We define the *Projective n-space* over K as the quotient set

$$\mathbb{P}^n(K) = \big(K^{n+1} \setminus \{(0, \ldots, 0)\}\big)/\sim .$$

The equivalence class of $(x_0, \ldots, x_n)$ is denoted by $(x_0 : \ldots : x_n) \in \mathbb{P}^n(K)$.

We refer to points of type $(x_0 : \ldots : x_{n-1} : 1)$ as *affine points*, whereas those of the form $(x_0 : \ldots : x_{n-1} : 0)$ are called *points at infinity.* Since they are a partition of $\mathbb{P}^n(K)$ it is easy to see that, when K is finite, we have

$$|\mathbb{P}^n(K)| = |K|^n + |\mathbb{P}^{n-1}(K)| = \frac{|K|^{n+1} - 1}{|K| - 1}.$$

1.1.2 Definition via Weierstrass equations

Let us now consider the projective plane $\mathbb{P}^2(K)$. We are interested in certain types of plane curves $\big($i.e. curves inside $\mathbb{P}^2(K)\big)$, namely those defined by particular cubic equations.

Definition 1.1.2 (Weierstrass polynomial and equation)**.** Let $\{a_1, a_2, a_3, a_4, a_6\} \subseteq K$. A polynomial $F_{a_1,a_2,a_3,a_4,a_6} \in K[x, y, z]$ of the form

$$F_{a_1,a_2,a_3,a_4,a_6}(x, y, z) = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 - (y^2z + a_1xyz + a_3yz^2)$$

is called *Weierstrass polynomial.* An equation of the form

$$F_{a_1,a_2,a_3,a_4,a_6}(x,y,z)=0$$

is called *Weierstrass equation.*

It is well-known that, if the characteristic of K is not 2, any Weiestrass equation may be simplified by changing the y-coordinate as

$$y \leftarrow y - \frac{a_1}{2}x - \frac{a_3}{2}z.$$

Moreover, if $\mathrm{char}(K) \neq 3$ as well, the further change of the x-coordinate

$$x \leftarrow x - \left(\frac{a_2}{3} + \frac{a_1^2}{12}\right) z$$

leads us to the short Weierstrass polynomial

$$F_{A,B} = x^3 + Axz^2 + Bz^3 - y^2z.$$

where

$$\begin{cases} A = a_4 + \frac{a_1a_3}{2} - \frac{a_2^2}{3} - \frac{a_1^4}{48} - \frac{a_1^2a_2}{6}, \\ B = a_6 + \frac{a_1^6}{864} + \frac{a_1^4a_2}{72} - \frac{a_1^3a_3}{24} + \frac{a_1^2a_2^2}{18} - \frac{a_1^2a_4}{12} - \frac{a_1a_2a_3}{6} + \frac{2a_2^3}{27} - \frac{a_2a_4}{3} + \frac{a_3^2}{4}. \end{cases}$$

Henceforth we consider only fields K such that $6 \in K^*$ and use the short form $E_{A,B}$ of these equations.

Definition 1.1.3 (Discriminant)**.** Let $A, B \in K$. We define the *discriminant* of $F_{A,B}$ as

$$\Delta_{A,B} = -(4A^3 + 27B^2).$$

This quantity is called this way because it is precisely the polynomial discriminant of

$x^3 + Ax + B = (x - r_1)(x - r_2)(x - r_3) \in \overline{K}[x]$, i.e.

$$\Delta_{A,B} = \mathrm{Disc}_x(x^3 + Ax + B) = -\prod_{i \neq j}(r_i - r_j).$$

It is a standard fact [67, Proposition III.1.4] that the projective cubics defined via Weierstrass equations are non-singular if and only if their discriminant is non-zero, which motivates the following definition.

Definition 1.1.4 (Elliptic curve over K)**.** Let $A, B \in K$ such that $\Delta_{A,B} \neq 0$. The *elliptic curve* defined by $F_{A,B}$ over K is

$$\mathcal{E}_{A,B}(K) = \mathcal{V}(F_{A,B}) = \{(X : Y : Z) \in \mathbb{P}^2(K) \mid Y^2Z = X^3 + AXZ^2 + BZ^3\}.$$

The element $\mathcal{O} = (0 : 1 : 0) \in \mathcal{E}_{A,B}(K)$ is referred to as the *zero point* or *point at infinity*, while the others are called *affine points*.

1.1.3 Addition law

Elliptic curves have been deeply studied as they constitute "small" examples of positive-genus abelian varieties. In fact, it is known [67, Section III.2] that the following is a well-defined binary operation, which provides elliptic curves with an abelian group structure.

Definition 1.1.5 (Addition on $\mathcal{E}_{A,B}$)**.** Let K be a field and $\mathcal{E}_{A,B}(K)$ be an elliptic curve. For every pair of points $P_1 = (X_1 : Y_1 : Z_1)$, $P_2 = (X_2 : Y_2 : Z_2) \in \mathcal{E}_{A,B}(K)$, we define their sum $P_1 + P_2$ as

- If $Z_i = 0$ (i.e. $P_i = \mathcal{O}$) for some $i \in \{1, 2\}$:

$$P_i + \mathcal{O} = \mathcal{O} + P_i = P_i.$$

- If $Z_i \neq 0$ for both $i = 1, 2$ and $P_1 = P_2$:

$$P_1 + P_2 = 2P_1 = (X_3 : Y_3 : Z_3),$$

where

$$\begin{cases} X_3 = 2Y_1Z_1\big((3X_1^2+AZ_1^2)^2 - 8X_1Y_1^2Z_1\big), \\ Y_3 = (3X_1^2+AZ_1^2)(12X_1Y_1^2Z_1) - (3X_1^2+AZ_1^2)^3 - 8Y_1^4Z_1^2, \\ Z_3 = 8Y_1^3Z_1^3. \end{cases}$$

- If $Z_i \neq 0$ for both $i = 1, 2$ and $P_1 \neq P_2$:

$$P_1 + P_2 = (X_3 : Y_3 : Z_3),$$

where, by denoting $[X, Z] = X_1Z_2 - X_2Z_1$ and $[Y, Z] = Y_1Z_2 - Y_2Z_1$,

$$\begin{cases} X_3 = Z_1Z_2[X,Z][Y,Z]^2 - (X_1Z_2 + X_2Z_1)[X,Z]^3, \\ Y_3 = (2X_1Z_2 + X_2Z_1)[X,Z]^2[Y,Z] - Y_1Z_2[X,Z]^3 - Z_1Z_2[Y,Z]^3, \\ Z_3 = Z_1Z_2[X,Z]^3. \end{cases}$$

An easy inspection of the above formulae shows that if two points sum to zero, then $[X, Z] = 0$, which by means of the curve equation also gives $[Y^2, Z^2] = Y_1^2Z_2^2 - Y_2^2Z_1^2 = 0$, i.e. the additive inverse is given by

$$-(X : Y : Z) = (X : -Y : Z),$$

which is the symmetric point with respect to the xz-plane.

The above definition reflects the following geometrical procedure: to double a point P_1, we consider the intersection of the line l_{p_1} through P_1 and tangent to $\mathcal{E}_{A,B}(K)$ with the curve itself:

$$\mathcal{E}_{A,B}(K) \cap l_{p_1} = \{P_1, Q\}.$$

Then $2P_1$ is the inverse of Q, i.e. the point of $\mathcal{E}_{A,B}(K)$ that is vertically aligned with Q.

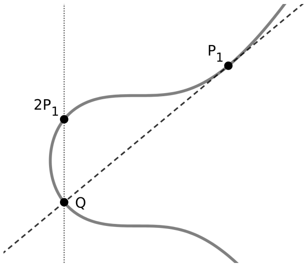


Figure 1.1. Point doubling on $\mathcal{E}_{0,3}$ over $\mathbb{R}$

Likewise, the point $P_1 + P_2$ is the inverse of Q, the third point of intersection between the line l_{P_1,P_2} through P_1, P_2 and $\mathcal{E}_{A,B}(K)$:

$$\mathcal{E}_{A,B}(K) \cap l_{P_1,P_2} = \{P_1, P_2, Q\}.$$

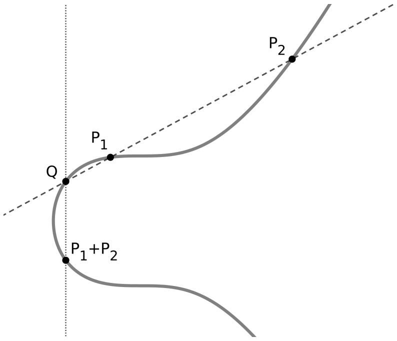


Figure 1.2. Point sum on $\mathcal{E}_{0,3}(\mathbb{R})$

Remark 1.1.6. It is worth noting that the addition formulae stated above work also over finite fields $\mathbb{F}$, in particular over prime ones. They may also be interpreted geometrically, via the toric identification of the affine $(\mathbb{F} \times \mathbb{F})$-plane.

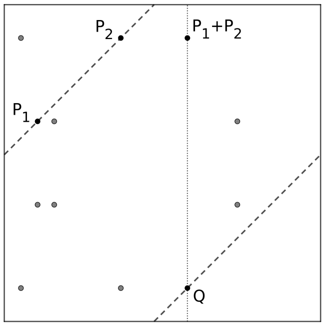


Figure 1.3. Point sum on $\mathcal{E}_{0,3}(\mathbb{F}_{19})$

1.2 COMPLETE SYSTEMS OF ADDITION LAWS

Given an elliptic curve $\mathcal{E} = \mathcal{E}_{A,B}(K)$, the addition formulae discussed in Section 1.1.3 distinguish three different cases. Two of them ($P_{1,2} = \mathcal{O}$, $P_1 = P_2$) work on subsets of $\mathcal{E} \times \mathcal{E}$ that are closed in the product Zariski topology, whereas the remaining case is valid on an open subset of $\mathcal{E} \times \mathcal{E}$.

The question whether or not such addition laws may be found on an open covering of $\mathcal{E} \times \mathcal{E}$ has been positively answered. The existence of such laws has been proved true for abelian varieties over algebraically closed fields in [39]. Such a set of addition laws is called *complete system of addition laws* and in the same work it has been explicitly provided for elliptic curves over fields $K = \overline{K}$ of characteristics $\mathrm{char}(K) \neq 2, 3$ (and of arbitrary characteristic in [40]).

A similar result over not-necessarily closed field has been shown in a further work [9], which has also provided us with specific conditions that these laws have to satisfy. The results and the explicit laws from this paper are recalled in this section, although the formulae have been slightly modified following [74].

Definition 1.2.1 (Addition law)**.** Let $\mu, \nu \in \mathbb{Z}_{\geq 1}$ be positive integers and $\mathcal{E}$ be an elliptic curve defined over K. An *addition law* of bidegree (μ, ν) on $\mathcal{E}$ is a triple of polynomials $S_1, S_2, S_3 \in K[x_1, y_1, z_1, x_2, y_2, z_2]$ such that

- the S_i's are homogeneous of degree μ in the variables x_1, y_1, z_1,
- the S_i's are homogeneous of degree ν in the variables x_2, y_2, z_2,
- for every pair of points $P_1 = (X_1 : Y_1 : Z_1), P_2 = (X_2 : Y_2 : Z_2) \in \mathcal{E}$ either

$$P_1 + P_2 = \big(S_1(X_1, Y_1, Z_1, X_2, Y_2, Z_2) : \ldots : S_3(X_1, Y_1, Z_1, X_2, Y_2, Z_2)\big)$$

or for every $i \in \{1, 2, 3\}$ we have

$$S_i(X_1, Y_1, Z_1, X_2, Y_2, Z_2) = 0.$$

In the latter case, the pair (P_1, P_2) is called *exceptional* for this addition law.

By replacing the polynomials S_i with any of their multiples by non-zero constants, one evidently finds another proper addition law, which we call *equivalent* to the original one since it produces the same values on every pair of points of $\mathcal{E}$.

Definition 1.2.2 (Complete system of addition laws)**.** Let $\mathcal{E}$ be an elliptic curve over K. A collection $\mathcal{C}$ of addition laws on $\mathcal{E}$ is called a *complete system of addition laws* on $\mathcal{E}$ if every pair of points in $\mathcal{E}$ is not exceptional for at least one law of $\mathcal{C}$.

Theorem 1.2.3 ([9], Theorem 2)**.** *Let $\mathcal{E}$ be an elliptic curve over K. For every point $(a : b : c) \in \mathbb{P}^2(K)$ there exists a unique (up to equivalence) non-zero addition law of bidegree $(2, 2)$ on $\mathcal{E}$ such that a pair $P_1, P_2 \in \mathcal{E}$ is exceptional if and only if $P_1 - P_2$ lies on the line $aX + bY + cZ = 0$ in $\mathbb{P}^2(K)$.*

Definition 1.2.4 (Addition law corresponding to P)**.** The addition law of bidegree $(2, 2)$ corresponding as in Theorem 1.2.3 to the projective point $P \in \mathbb{P}^2(K)$ is denoted by $+_P$.

The following are explicit instances of addition laws of bidegree $(2, 2)$ on $\mathcal{E}$. As in Section 1.1.3, we shorten the notation by writing

$$[X, Y] = X_1Y_2 - X_2Y_1, \quad [X, Z] = X_1Z_2 - X_2Z_1, \quad [Y, Z] = Y_1Z_2 - Y_2Z_1.$$

For $j \in \{1, 2, 3\}$, we also write $S_j(X_i, Y_i, Z_i)$ in place of $S_j(X_1, Y_1, Z_1, X_2, Y_2, Z_2)$.

$+_{(0:0:1)}$**: The addition law corresponding to** $(0 : 0 : 1)$.

$$\begin{aligned} S_1(X_i, Y_i, Z_i) = {} & [X, Y](Y_1Z_2 + Y_2Z_1) + [X, Z]Y_1Y_2 - A[X, Z](X_1Z_2 + X_2Z_1) \\ & - 3B[X, Z]Z_1Z_2, \end{aligned}$$

$$\begin{aligned} S_2(X_i, Y_i, Z_i) = {} & -3X_1X_2[X, Y] - Y_1Y_2[Y, Z] - A[X, Y]Z_1Z_2 \\ & + A[Y, Z](X_1Z_2 + X_2Z_1) + 3B[Y, Z]Z_1Z_2, \end{aligned}$$

$$S_3(X_i, Y_i, Z_i) = 3X_1X_2[X, Z] - [Y, Z](Y_1Z_2 + Y_2Z_1) + A[X, Z]Z_1Z_2.$$

$+_{(0:1:0)}$**: The addition law corresponding to** $(0:1:0)$.

$$\begin{aligned} S_1(X_i, Y_i, Z_i) = {} & Y_1Y_2(X_1Y_2 + X_2Y_1) - AX_1X_2(Y_1Z_2 + Y_2Z_1) \\ & - A(X_1Y_2 + X_2Y_1)(X_1Z_2 + X_2Z_1) - 3B(X_1Y_2 + X_2Y_1)Z_1Z_2 \\ & - 3B(X_1Z_2 + X_2Z_1)(Y_1Z_2 + Y_2Z_1) + A^2(Y_1Z_2 + Y_2Z_1)Z_1Z_2, \end{aligned}$$

$$\begin{aligned} S_2(X_i, Y_i, Z_i) = {} & Y_1^2Y_2^2 + 3AX_1^2X_2^2 + 9BX_1X_2(X_1Z_2 + X_2Z_1) \\ & - A^2X_1Z_2(X_1Z_2 + 2X_2Z_1) - A^2X_2Z_1(2X_1Z_2 + X_2Z_1) \\ & - 3ABZ_1Z_2(X_1Z_2 + X_2Z_1) - (A^3 + 9B^2)Z_1^2Z_2^2, \end{aligned}$$

$$\begin{aligned} S_3(X_i, Y_i, Z_i) = {} & 3X_1X_2(X_1Y_2 + X_2Y_1) + Y_1Y_2(Y_1Z_2 + Y_2Z_1) \\ & + A(X_1Y_2 + X_2Y_1)Z_1Z_2 + A(X_1Z_2 + X_2Z_1)(Y_1Z_2 + Y_2Z_1) \\ & + 3B(Y_1Z_2 + Y2Z_1)Z_1Z_2. \end{aligned}$$

Although in this work we only make use of $+_{(0:0:1)}$ and $+_{(0:1:0)}$, we also recall the addition law corresponding to $(1:0:0)$ since $\{+_{(0:0:1)}, +_{(1:0:0)}\}$ constitutes an interesting example of a system of two addition laws that is never complete (all the pairs (P, P) are exceptional for both the laws).

$+_{(1:0:0)}$**: The addition law corresponding to** $(1:0:0)$.

$$\begin{aligned} S_1(X_i, Y_i, Z_i) = {} & [X, Y](X_1Y_2 + X_2Y_1) + AX_1X_2[X, Z] \\ & + 3B[X, Z](X_1Z_2 + X_2Z_1) - A^2[X, Z]Z_1Z_2, \end{aligned}$$

$$\begin{aligned} S_2(X_i, Y_i, Z_i) = {} & [X, Y]Y_1Y_2 - 3AX_1X_2[Y, Z] + A(X_1Y_2 + X_2Y_1)[X, Z] \\ & + 3B[X, Y]Z_1Z_2 - 3B(X_1Z_2 + X_2Z_1)[Y, Z] + A^2[Y, Z]Z_1Z_2, \end{aligned}$$

$$\begin{aligned} S_3(X_i, Y_i, Z_i) = {} & - (X_1Y_2 + X_2Y_1)[Y, Z] - [X, Z]Y_1Y_2 \\ & - A[X, Z](X_1Z_2 + X_2Z_1) - 3B[X, Z]Z_1Z_2. \end{aligned}$$

Remark 1.2.5. Since the projective point $(1:0:0)$ cannot lie inside any elliptic curve as in Definition 1.1.4, then the addition laws $\{+_{(0:0:1)}, +_{(0:1:0)}\}$ always form a complete system of addition laws on $\mathcal{E}$. However, if the considered curve has no 2-torsion points (e.g. if it has an odd prime order) then for every pair of points $P_1, P_2 \in \mathcal{E}$ we have $(P_1 - P_2)_y \neq 0$. Hence, in this case the addition law corresponding to $(0 : 1 : 0)$ forms itself a complete system of addition laws.

1.3 THE POINT GROUP OVER FINITE FIELDS

Several significant results about the point group structure of elliptic curves have been developed in the last century. The characterization of these groups substantially varies depending on the field underlying the curve [67, Chapters V-VIII] and in this work we focus only on finite ones, which play a relevant role in practical applications.

A crucial theorem about their size has been conjectured by Artin [1] and proved by Hasse [23], from whom it has been named.

Theorem 1.3.1 (*Hasse's Theorem*, [67], Theorem V.1.1)**.** *Let $\mathcal{E} = \mathcal{E}_{A,B}(\mathbb{F}_q)$ be an elliptic curve defined over a finite field $\mathbb{F}_q$. Then*

$$(\sqrt{q} - 1)^2 \leq |\mathcal{E}| \leq (\sqrt{q} + 1)^2.$$

Many algorithms for efficiently computing the size of a given elliptic curve over a finite field have been conceived [58]. Among them, the celebrated Schoof's one [59] surely deserve to be mentioned, being the first deterministic polynomial time algorithm, which has attracted plentiful further research and improvements [4]. Nowadays, highly efficient implementations of the Schoof-Elkies-Atkin algorithm may deal with curves of industrial size ($\sim$ 512-bits) in less than a second [8].

The group structure of elliptic curves is governed by an important invariant of the curve [67, Remark V.2.6].

Definition 1.3.2 (Trace of Frobenius)**.** Let $\mathcal{E} = \mathcal{E}_{A,B}(\mathbb{F}_q)$ be an elliptic curve defined over a finite field $\mathbb{F}_q$. The integer

$$t = q + 1 - |\mathcal{E}|$$

is called the *trace of Frobenius* or the *trace of $\mathcal{E}$*.

By Theorem 1.3.1 every $t \in \mathbb{Z}$ that is the trace of an elliptic curve over $\mathbb{F}_q$ satisfies

$|t| \leq 2\sqrt{q}$, but not all the values in this range can occur as the trace of an elliptic curve.

Theorem 1.3.3 ([75], Theorem 4.1)**.** *Let $p \in \mathcal{P}$ be a prime, $e \in \mathbb{Z}_{\geq 1}$ be an integer and let $q = p^e$. For every integer $|t| \leq 2\sqrt{q}$ there is an elliptic curve $\mathcal{E} = \mathcal{E}_{A,B}(\mathbb{F}_q)$ of trace t if and only if one of the following conditions is satisfied:*

(i) $\mathrm{GCD}(t, p) = 1$,

(ii) $t = \pm 2\sqrt{q}$ *and e is even,*

(iii) $t = \pm\sqrt{q}$, $p \neq 1 \bmod 3$ *and e is even,*

(iv) $t = \pm\sqrt{pq}$, $p \in \{2, 3\}$ *and e is odd,*

(v) $t = 0$ *and either e is odd or $p \not\equiv 1 \bmod 4$.*

From part (i) of Theorem 1.3.3 follows that all the values determined by Hasse's theorem over prime fields actually occur as a group order.

Corollary 1.3.4 ([60], Theorem 4.2)**.** *Let $p \in \mathcal{P}$ be a prime, $p \geq 5$ and $|t| \leq 2\sqrt{p}$ be an integer. Then there is an elliptic curve $\mathcal{E} = \mathcal{E}_{A,B}(\mathbb{F}_p)$ of trace t.*

Proof. If $p|t$ then

$$p^2 \leq t^2 \leq 4p \implies 0 \leq p \leq 4.$$

Therefore, when $p \geq 5$ we have $\mathrm{GCD}(t, p) = 1$ and the statement follows from case (i) of Theorem 1.3.3. □

Remark 1.3.5. By using the long form of Weierstrass equations one can define elliptic curves even over fields K with $\mathrm{char}(K)|6$. In these cases, it may be verified that an analogous of Corollary 1.3.4 holds for every prime $p \in \mathcal{P}$.

Now we focus on the actual group structures.

Definition 1.3.6 (Torsion points)**.** Let $\mathcal{E} = \mathcal{E}_{A,B}(K)$ be an elliptic curve and $m \in \mathbb{Z}_{\geq 1}$ be a non-negative integer. We define the *m-torsion points of $\mathcal{E}$* as

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

The following proposition gives a precise characterization of the possible group structures that torsion points may display.

Proposition 1.3.7 ([74], Theorem 3.2)**.** *Let K be a field and $\mathcal{E} = \mathcal{E}_{A,B}(K)$ be an elliptic curve. Then*

- *if* $\mathrm{char}(K) = 0$ *or* $\mathrm{char}(K) = p$ *and* $\gcd(m, p) = 1$*, then*

$$\mathcal{E}[m] \simeq \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z},$$

- *if* $\mathrm{char}(K) = p$ *and* $m = m'p^e$*, with* $p \nmid m'$*, then*

$$\textit{either} \quad \mathcal{E}[m] \simeq \mathbb{Z}/m'\mathbb{Z} \oplus \mathbb{Z}/m'\mathbb{Z} \quad \textit{or} \quad \mathcal{E}[m] \simeq \mathbb{Z}/m'\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}.$$

From the above proposition a first structure result follows.

Corollary 1.3.8 ([74], Theorem 4.1 and Corollary 3.11)**.** *Let $\mathcal{E} = \mathcal{E}_{A,B}(\mathbb{F}_q)$ be an elliptic curve defined over a finite field $\mathbb{F}_q$. Then there are two positive integers $n, k \in \mathbb{Z}_{\geq 1}$ such that $n|(q-1)$ and*

$$\mathcal{E} \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/nk\mathbb{Z}.$$

Thus, the possible point groups arising from elliptic curves over finite fields are either cyclic or product of two cyclic groups, but deciding which is the case may be burdensome. It is known that the cyclic scenario often happens over small prime fields [7], and asymptotic formulae for their density have been given [22]. Moreover, it has been also studied the frequency with which the group cyclicity is preserved under finite fields extensions [71].

From Theorem 1.3.3 a complete characterization of the possible structures occurring as point groups of elliptic curves over finite fields has seen the light, independently discovered by two different authors.

Theorem 1.3.9 ([54] and [72])**.** *Let $p \in \mathcal{P}$ be a prime, $e \in \mathbb{Z}_{\geq 1}$ be an integer and let $q = p^e$. Let also $|t| \leq 2\sqrt{q}$ be an integer satisfying one of the conditions (i)-(v) of Theorem 1.3.3.*

Then the following is a complete list of the group structures of the trace-t elliptic curves defined over $\mathbb{F}_q$, where the enumeration corresponds to the cases of Theorem 1.3.3.

(*i*) *Let $|\mathcal{E}| = \prod_{l\in\mathcal{P}} l^{e_l}$ be the prime factorization of the curve order. There are integers $0 \leq a_l \leq \min\{\mathrm{v}_l(q-1),\ \lfloor \frac{e_l}{2} \rfloor\}$ such that the group is*

$$\mathbb{Z}/p^{e_p}\mathbb{Z} \oplus \bigoplus_{l\in\mathcal{P}\setminus\{p\}} \left(\mathbb{Z}/l^{a_l}\mathbb{Z} \oplus \mathbb{Z}/l^{e_l-a_l}\mathbb{Z}\right).$$

(*ii*) $\mathbb{Z}/(\sqrt{q}\pm 1)\mathbb{Z} \oplus \mathbb{Z}/(\sqrt{q}\pm 1)\mathbb{Z}$.

(*iii*) *Cyclic.*

(*iv*) *Cyclic.*

(*v*) *The group is*

$$\begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/\frac{q+1}{2}\mathbb{Z} \text{ or cyclic} & \text{if } q \equiv 3 \bmod 4,\\ \text{cyclic} & \text{if } q \not\equiv 3 \bmod 4. \end{cases}$$

We observe that, for every integer $t \in \mathbb{Z}$, Theorem 1.3.9 provides a restrictive but not necessarily trivial list of possible group structures arising from trace-t elliptic curves. The following is an example of an elliptic curve whose group structure cannot be retrieved by a mere application of the aforementioned theorem.

Example 1.3.10. Let $p = 5$, $q = p^2 = 25$ and consider the finite field

$$\mathbb{F}_{25} = \mathbb{F}_5[x]/(x^2 + 4x + 2) = \mathbb{F}_5(\alpha).$$

Let $\mathcal{E}$ be the elliptic curve $\mathcal{E}_{2,0}(\mathbb{F}_{25})$, whose order is $|\mathcal{E}| = 20$ which implies that its trace is $t = 25 + 1 - 20 = 6$. Since $\mathrm{GCD}(t,p) = 1$, then we are in case (i) of Theorem 1.3.9, therefore there is an integer $0 \leq a \leq 1$ such that

$$\mathcal{E} \simeq \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/2^{2-a}\mathbb{Z}.$$

Thus, by applying Theorem 1.3.9 we conclude that the point group of $\mathcal{E}$ may be either cyclic (if $a = 0$) or isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ (if $a = 1$). A further inspection shows that the latter is the case, in fact the point group is given by

$$\mathcal{E} \simeq \langle(0 : 0 : 1)\rangle \oplus \langle(\alpha : \alpha : 1)\rangle.$$

We note that, as prescribed by Theorem 1.3.9, also the cyclic scenario may happen, e.g. by considering the trace-6 elliptic curve

$$\mathcal{E}_{\alpha^2,\alpha^5}(\mathbb{F}_{25}) \simeq \langle(\alpha : \alpha^2 : 1)\rangle.$$

We conclude this section by noting that the problem of efficiently finding generators of the cyclic components of these groups is still open. This task may be fulfilled over a generic finite field $\mathbb{F}_q$ in exponential time $O(q^{\frac{1}{2}+o(1)})$ [34], although it may be sped up for a large class of finite fields [65].

1.4 ECDLP AND ANOMALOUS CURVES

In this section we revise the discrete logarithm problem and its fast solution in the case of trace-1 elliptic curves over prime fields.

Definition 1.4.1 (Discrete logarithm)**.** Let G be a cyclic (additive) group of exponent $\exp(G)$ and let $g \in G$ be one of its generators. The *discrete logarithm based on g* is the group morphism

$$\log_g : G \to \mathbb{Z}/\exp(G)\mathbb{Z}, \quad m \cdot g = (g + \ldots + g) \mapsto m.$$

The *Discrete Logarithm Problem*, shortened as *DLP*, amounts to computing $\log_g(h)$ for any given element $h \in G$. The difficulty of such a problem heavily depends on the considered group G. When G is the group of points of an elliptic curve over a finite (usually prime) field, it is denoted by *ECDLP* and is considered to be hard in general. However, there are instances of curves over which the ECDLP may be efficiently solved.

Definition 1.4.2 (Anomalous curve)**.** Let $p \in \mathcal{P}$ be a prime. An elliptic curve $\mathcal{E} = \mathcal{E}_{A,B}(\mathbb{F}_p)$ is called *anomalous* if its trace is 1, i.e. if $|\mathcal{E}| = p$.

The solution of the ECDLP for anomalous curves over $\mathbb{F}_p$ is known to be feasible in $O(\ln p)$ field operations via different approaches, which we summarize in the following sections.

1.4.1 Semaev's isomorphism

The algebraic geometrical method [61] works on p-subgroups of $\mathcal{E}(\mathbb{F}_{p^e})$, but here we assume for simplicity that $|\mathcal{E}(\mathbb{F}_p)| = p$. We consider the proper extension of the base-field $\mathbb{F}_q = \mathbb{F}_p[x]/(x^3 + Ax + B) \supset \mathbb{F}_p$, over which $\mathcal{E}$ has a 2-torsion point $S = ([x] : [0] : [1])$.

In this way the extended curve $\mathcal{E}' = \mathcal{E}_{A,B}(\mathbb{F}_q)$ contains all the points of $\mathcal{E}$ and at least one, namely S, that does not lay inside $\mathcal{E}$. We consider the well-known [67, Exercise II.2.6] group isomorphism

$$\begin{aligned} \sigma : \mathcal{E}_{A,B}(\mathbb{F}_q) &\to \operatorname{Pic}^0\big(\mathcal{E}_{A,B}(\mathbb{F}_q)\big), \\ P &\mapsto [(P) - (\mathcal{O})]. \end{aligned}$$

For every point $Q \in \mathcal{E}$ we have that $pQ = \mathcal{O}$, hence the same point inside $\mathcal{E}'$ gives rise to a rational function $f_Q \in \overline{\mathbb{F}_q}(\mathcal{E}')$ such that $\operatorname{div}(f_Q) = p(Q + S) - p(S)$, since

$$p[(Q + S) - (S)] = p[(Q) - (\mathcal{O})] = [p\sigma(Q)] = [\sigma(\mathcal{O})] = [0].$$

In [61, Lemma 1] it is proved that for every $f \in \overline{\mathbb{F}_q}(\mathcal{E}')$ such that $(f) = pD$ for some nonprincipal divisor D, its derivative f' with respect to x satisfies $(f') = (f) - (y)$. Thus, for every $R \in \mathcal{E}$ the map

$$\begin{aligned} \phi_R : \mathcal{E} &\to \mathbb{F}_q, \\ Q &\mapsto \begin{cases} (f'_Q/f_Q)(R) & \text{if } Q \neq \mathcal{O}, \\ 0 & \text{if } Q = \mathcal{O}, \end{cases} \end{aligned}$$

is well-defined. Moreover, in the same work this application is proved to be an injective group morphism [61, Lemma 2], therefore the discrete logarithm may be computed as

$$\log_P(Q) = \frac{\phi_R(Q)}{\phi_R(P)}.$$

Since the evaluation of $(f'_Q/f_Q)(R)$ may always be performed in $O(\ln p)$ operations over $\mathbb{F}_q$ [61, Lemma 3], the same asymptotic complexity holds for the computation of $\log_P(Q)$.

This technique has been generalized to higher genus smooth projective curves C over finite fields $\mathbb{F}_q$ of characteristic p, with at least one $\mathbb{F}_q$-rational point. In fact, in [55] it was proved that the discrete logarithm inside the p^e-torsion part of $\mathrm{Pic}^0(C)$ may be evaluated with $O(e^2 \ln p)$ operations in $\mathbb{F}_q$.

1.4.2 Satoh-Araki and Smart lift

A number theoretical solution of the ECDLP over anomalous curves has appeared simultaneously in [68] and in [56], the latter fixed in [57]. It consists of lifting the curve over the p-adic field $\mathbb{Q}_p$ and rephrasing the problem inside the p-adic integers $\mathbb{Z}_p$.

Let $\pi : \mathcal{E}_{A,B}(\mathbb{Q}_p) \to \mathcal{E}_{A,B}(\mathbb{F}_p)$ be the classical reduction map and consider any of its liftings $u : \mathcal{E}_{A,B}(\mathbb{F}_p) \to \mathcal{E}_{A,B}(\mathbb{Q}_p)$, i.e. $\pi \circ u = \mathrm{id}_{\mathcal{E}_{A,B}(\mathbb{F}_p)}$. Let also $\Psi : \ker \pi \to p\mathbb{Z}_p$ be the map defined by $(X : Y : Z) \mapsto X/Y$, and let

$$\log_{\mathcal{E}} : p\mathbb{Z}_p \to p\mathbb{Z}_p, \qquad t \mapsto t - \frac{2A}{5}t^5 + \dots$$

be the formal logarithm as defined in [67, Chapter IV.5]. If $\mathcal{E}_{A,B}(\mathbb{F}_p)$ is anomalous, then [56, Theorem 3.2] the map

$$\lambda_{\mathcal{E}_{A,B}(\mathbb{Q}_p)} : \mathcal{E}_{A,B}(\mathbb{F}_p) \xrightarrow{u} \mathcal{E}_{A,B}(\mathbb{Q}_p) \xrightarrow{\cdot p} \ker \pi \xrightarrow{\Psi} p\mathbb{Z}_p \xrightarrow{\log_{\mathcal{E}}} p\mathbb{Z}_p \xrightarrow{\bmod p^2} p\mathbb{Z}_p/p^2\mathbb{Z}_p \simeq \mathbb{F}_p$$

does not depend of the choice of u and is proved to be either the zero map or a group isomorphism. The case $\lambda_{\mathcal{E}_{A,B}(\mathbb{Q}_p)} = 0$ occurs rarely [57, Theorem 3.7] and may be effortlessly avoided [57, Corollary 3.8] by changing the lifted curve $\mathcal{E}_{A,B}(\mathbb{Q}_p)$.

In [56] an algorithm for evaluating such $\lambda_{\mathcal{E}_{A,B}(\mathbb{Q}_p)}$ by using only operations in $\mathbb{Z}/p^2\mathbb{Z}$ is also provided.

CHAPTER 2

ELLIPTIC CURVES OVER $\mathbb{Z}/N\mathbb{Z}$

2.1 PROJECTIVE n-SPACE

In this section we recall the construction of the projective n-space over commutative rings with unity, mainly following [15]. We draw a special attention to the $\mathbb{Z}/N\mathbb{Z}$-case, as it will be largely employed in the continuation of the present work.

2.1.1 General construction of $\mathbb{P}^n(R)$

Let $n \in \mathbb{Z}_{\geq 0}$ be a non-negative integer and R be a commutative non-zero ring with identity. The construction of the projective n-space over R is classically performed with two main goals in mind: we want the componentwise multiplication to induce an equivalence relation and we wish our construction to respect projections.

The first requirement is achieved by considering only the action of the unit group R^*, defined for every $u \in R^*$ and $(x_0, \ldots, x_n) \in R^{n+1}$ as

$$u(x_0, \ldots, x_n) = (ux_0, \ldots, ux_n). \tag{2.1}$$

The second condition is assured by considering *primitive* entries.

Definition 2.1.1 (Primitivity)**.** A finite collection $\{x_i\}_{i\in\{0,\ldots,n\}} \subseteq R^{n+1}$ is called *primitive* if the ideal $\langle\{x_i\}_{i\in\{0,\ldots,n\}}\rangle_R$ they generate is R itself.

We consider only primitive $(n+1)$-tuples to ensure projections on non-zero subrings. More precisely, if $I = \langle\{x_i\}_{i\in\{0,\ldots,n\}}\rangle_R$ were a proper ideal of R, then the projection $R \to R/I$ would map $(x_i)_{i\in\{0,\ldots,n\}}$ to the zero vector, which is not desirable in a projective space.

The above discussion motivates the following definition.

Definition 2.1.2 (Projective n-space)**.** We define the *Projective n-space* over R as the set of orbits of primitive $(n+1)$-tuples under the action (2.1) of R^*. It is denoted by $\mathbb{P}^n(R)$, while $(x_0 : \ldots : x_n) \in \mathbb{P}^n(R)$ represents the orbit of $(x_0, \ldots, x_n) \in R^{n+1}$.

In accordance with the classical notion of projective spaces over fields, we call *affine* any point of $\mathbb{P}^n(R)$ whose last component is invertible:

$$\mathbb{P}^n_{\text{aff}}(R) = \{(X_0 : \ldots : X_{n-1} : 1) \mid \forall i,\ X_i \in R\}.$$

We may also identify the points whose last coordinate is 0 with a projective space of dimension $n-1$, while the remaining points are called *special*:

$$\mathbb{P}^n_{\text{s}}(R) = \{(X_0 : \ldots : X_n) \mid X_n \in R \setminus (R^* \cup \{0\})\}.$$

This leads to a natural decomposition of the projective n-space as

$$\mathbb{P}^n(R) = \mathbb{P}^n_{\text{aff}}(R) \cup \mathbb{P}^{n-1}(R) \cup \mathbb{P}^n_{\text{s}}(R).$$

2.1.2 The case $R = \mathbb{Z}/N\mathbb{Z}$

Let $N \in \mathbb{Z}_{\geq 2}$. The case of our interest is $R = \mathbb{Z}/N\mathbb{Z}$, which is a suitable ring for number-theoretic algorithms. In this setting an $(n+1)$-tuple $(x_0, \ldots, x_n)$ is primitive if and only if

$$\text{GCD}(x_0, \ldots, x_n, N) = 1.$$

Thus, the elements of $\mathbb{P}^n(\mathbb{Z}/N\mathbb{Z})$ are $(n+1)$-tuples of integers modulo N that are not all divisible by the same prime factor of N. Two tuples are identified if they are equal up to componentwise multiplication for integers that are coprime with N.

A formula to count elements of the projective space over such rings is known and its proof usually involves Möbius inversion formula. However, we find that a constructive proof might well be stimulating and useful for practical reasons, so we propose it below.

Proposition 2.1.3 ([15], Section 10.3.2)**.** *Let $N \in \mathbb{Z}_{\geq 2}$ and $n \in \mathbb{Z}_{\geq 0}$. Then*

$$|\mathbb{P}^n(\mathbb{Z}/N\mathbb{Z})| = N^n \prod_{\substack{p \in \mathcal{P} \\ p \mid N}} \left(1 + \frac{1}{p} + \ldots + \frac{1}{p^n}\right).$$

Proof. Let $N = \prod_{p|N} p^{e_p}$ be the prime factorization of N, i.e. $e_p = \mathrm{v}_p(N)$. Here all the products are ordered according to the increasing value of p.

Since projections respect primitivity, the Chinese Reminder Theorem gives rise to a well-defined bijection

$$\begin{aligned} \mathbb{P}^n(\mathbb{Z}/N\mathbb{Z}) &\to \prod_{\substack{p\in\mathcal{P},\\ p|N}} \mathbb{P}^n(\mathbb{Z}/p^{e_p}\mathbb{Z}), \\ (X_0 : \ldots : X_n) &\mapsto \big((X_0 \bmod p^{e_p} : \ldots : X_n \bmod p^{e_p})\big)_{p|N}. \end{aligned}$$

Thus, it is sufficient to prove the formula for $N = p^e$. We do it by induction on n, exhibiting the size of the three disjoint components of $\mathbb{P}^n(\mathbb{Z}/p^e\mathbb{Z})$.
$[n = 0]$ This case is trivial, since $\mathbb{P}^0(\mathbb{Z}/p^e\mathbb{Z}) = \{(1)\}$, hence $|\mathbb{P}^0(\mathbb{Z}/p^e\mathbb{Z})| = 1$.
$[n \to n+1]$ The affine part is easily counted:

$$|\mathbb{P}^{n+1}_{\text{aff}}(\mathbb{Z}/p^e\mathbb{Z})| = |\{(X_0 : \ldots : X_n : 1) \mid X_i \in \mathbb{Z}/p^e\mathbb{Z}\}| = (p^e)^{n+1},$$

while the inductive hypothesis provides us with the size of the projective part:

$$|\mathbb{P}^n(\mathbb{Z}/p^e\mathbb{Z})| = (p^e)^n \left(1 + \frac{1}{p} + \ldots + \frac{1}{p^n}\right).$$

To count the elements of the special part, we first notice that they can be written as $(X_0, \ldots, X_n, p^\gamma)$ for some $0 < \gamma < e$. Let us consider the projections

$$\begin{aligned} \pi_\gamma : \{(X_0 : \ldots : X_n : p^\gamma) \mid X_i \in \mathbb{Z}/p^e\mathbb{Z}\} &\to \mathbb{P}^n(\mathbb{Z}/p^e\mathbb{Z}), \\ (X_0 : \ldots : X_n : p^\gamma) &\mapsto (X_0 : \ldots : X_n). \end{aligned}$$

For any given point $(X_0 : \ldots : X_n) \in \mathbb{P}^n(\mathbb{Z}/p^e\mathbb{Z})$, its fibers are given by

$$\pi_\gamma^{-1}\big((X_0 : \ldots : X_n)\big) = \{(\alpha X_0 : \ldots : \alpha X_n : p^\gamma) \mid \alpha \in (\mathbb{Z}/p^e\mathbb{Z})^*\}.$$

However, some of these points may be identified, in fact

$$\begin{aligned}(\alpha X_0 : \ldots : \alpha X_n : p^\gamma) = (X_0 : \ldots : X_n : p^\gamma) &\iff \alpha p^\gamma \equiv p^\gamma \bmod p^e \\ &\iff \alpha \equiv 1 \bmod p^{e-\gamma},\end{aligned}$$

which implies that the elements of $\pi_\gamma^{-1}\big((X_0 : \ldots : X_n)\big)$ are precisely (i.e. without repetitions) the $(n+1)$-tuples $(\alpha X_0 : \ldots : \alpha X_n : p^\gamma)$ such that

$$\alpha = h + kp, \quad h \in \{1, \ldots, p-1\},\ k \in \{0, \ldots, p^{e-\gamma-1} - 1\}.$$

Therefore, the size of the fibers is $|\pi_\gamma^{-1}\big((X_0 : \ldots : X_n)\big)| = p^{e-\gamma-1}(p-1)$. Since $\mathbb{P}_{\mathrm{s}}^{n+1}(\mathbb{Z}/p^e\mathbb{Z})$ is the disjoint union of $\big\{\pi_\gamma^{-1}\big(\mathbb{P}^n(\mathbb{Z}/p^e\mathbb{Z})\big)\big\}_{0<\gamma<e}$, then we have

$$\begin{aligned}|\mathbb{P}_{\mathrm{s}}^{n+1}(\mathbb{Z}/p^e\mathbb{Z})| &= \sum_{\gamma=1}^{e-1} |\mathbb{P}^n(\mathbb{Z}/p^e\mathbb{Z})| p^{e-\gamma-1}(p-1) \\ &= (p^e)^n \left(1 + \frac{1}{p} + \ldots + \frac{1}{p^n}\right)(p^{e-1} - 1) \\ &= (p^e)^{n+1} \left(\frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^{n+1}}\right) - |\mathbb{P}^n(\mathbb{Z}/p^e\mathbb{Z})|.\end{aligned}$$

Thus, the size of the whole projective space is

$$|\mathbb{P}^{n+1}(\mathbb{Z}/p^e\mathbb{Z})| = (p^e)^{n+1} + (p^e)^{n+1}\left(\frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^{n+1}}\right),$$

which concludes the inductive step. □

2.2 ELLIPTIC CURVES OVER RINGS

2.2.1 Matrix rank over rings

This section is devoted to recalling the notion of matrix rank when the considered matrices have entries in a commutative ring R with unity. Such a subject is needed to properly characterize, in the next section, the conditions we shall assume on rings over which elliptic curves may be defined. The key reference for this part is [12, Chapter 4].

Definition 2.2.1 (Minor ideal)**.** Let $n, m \in \mathbb{Z}_{\geq 1}$ and $A \in M_{n,m}(R)$. For every integer $1 \leq t \leq \min\{n, m\}$ we define the *t-minor ideal* $I_t(A)$ as the ideal generated by the $t \times t$ minors of A. We also define by convention $I_0(A) = R$ and for every $t > \min\{n, m\}$ we set $I_t(A) = (0)$.

From the Laplace expansion of the determinant we have the ascending chain of ideals

$$(0) = I_{\min\{n,m\}+1}(A) \subseteq I_{\min\{n,m\}}(A) \subseteq \ldots \subseteq I_1(A) \subseteq I_0(A) = R.$$

Thus, we have the reverse chain of their annihilators

$$R = \mathrm{Ann}_R\big((0)\big) \supseteq \mathrm{Ann}_R\big(I_{\min\{n,m\}}(A)\big) \supseteq \ldots \supseteq \mathrm{Ann}_R\big(I_1(A)\big) \supseteq \mathrm{Ann}_R(R) = (0).$$

This motivates the following definitions.

Definition 2.2.2 (Rank)**.** Let $n, m \in \mathbb{Z}_{\geq 1}$ and $A \in M_{n,m}(R)$. The *rank* of A is defined as

$$\overline{\mathrm{rk}}(A) = \max\{t \in \mathbb{Z}_{\geq 0} \mid \mathrm{Ann}_R\big(I_t(A)\big) = (0)\}.$$

Definition 2.2.3 (Strong rank)**.** Let $n, m \in \mathbb{Z}_{\geq 1}$ and $A \in M_{n,m}(R)$. The *strong rank* of A is defined as

$$\mathrm{rk}(A) = \max\{t \in \mathbb{Z}_{\geq 0} \mid I_t(A) \neq (0)\}.$$

The above notions of rank coincide when R is a field, but it easy to see that in general only $\overline{\mathrm{rk}}(A) \leq \mathrm{rk}(A)$ holds, since $\mathrm{Ann}_R\big((0)\big) = R \neq (0)$. The following example shows that the inequality might well be strict.

Example 2.2.4. Let us consider the ring $R = \mathbb{Z}/6\mathbb{Z}$ and the matrix

$$A = \begin{bmatrix} 2 & 2 \\ 3 & 2 \end{bmatrix} \in M_{2,2}(R).$$

We have $I_1(A) = R$ and $I_2(A) = \langle 4 \rangle$, so that $\mathrm{Ann}_R\big(I_2(A)\big) = \langle 3 \rangle$. Therefore $\overline{\mathrm{rk}}(A) = 1$ and $\mathrm{rk}(A) = 2$.

The rank we employ to define a sum operation on elliptic curves over rings is the *strong* one. In fact, we need linear combinations of the columns of certain matrices to produce a unique projective point, which is ensured by the following lemma.

Lemma 2.2.5. *Let $n, m \in \mathbb{Z}_{\geq 1}$ and $A \in M_{n,m}(R)$ be a matrix whose entries are primitive. The following are equivalent.*

(*i*) $\operatorname{rk}(A) = 1$.

(*ii*) *The 2×2 minors of A vanish.*

(*iii*) *All the primitive vectors of R^n that may be obtained from an R-linear combination among the columns of A are equal up to R^*-multiples.*

Proof. Let $A = (a_{i,k})_{\substack{1\leq i\leq n\\ 1\leq k\leq m}}$.
[$i \Rightarrow ii$] Since $\operatorname{rk}(A) = 1$ then $I_2(A) = (0)$, hence all the generators of $I_2(A)$ vanish.
[$ii \Rightarrow iii$] Let $v_1 = (v_{11}, \ldots, v_{1n})$ and $v_2 = (v_{21}, \ldots, v_{2n})$ be two primitive columns combinations. Since v_1 is primitive there are $\alpha_1, \ldots, \alpha_n \in R$ such that

$$\sum_{i=1}^{n} \alpha_i v_{1i} = 1 \in R.$$

It is easy to see that any 2×2 minor of the $(n \times 2)$-matrix $(v_1|v_2)$, whose columns are v_1 and v_2, is an R-linear combination of the 2×2 minors of A, hence it vanishes. Hence, for every $i, j \in \{1, \ldots, n\}$ we have $v_{1i}v_{2j} = v_{1j}v_{2i}$, then

$$v_2 = \left(\sum_{i=1}^{n} \alpha_i v_{1i}\right) v_2 = \left(\sum_{i=1}^{n} \alpha_i v_{1i} v_{2j}\right)_{1\leq j\leq n} = \left(\sum_{i=1}^{n} \alpha_i v_{1j} v_{2i}\right)_{1\leq j\leq n} = \left(\sum_{i=1}^{n} \alpha_i v_{2i}\right) v_1.$$

This proves that v_2 is a multiple of v_1, and since also v_2 is primitive then the scalar factor has to be a unit, i.e. $\sum_{i=1}^{n} \alpha_i v_{2i} \in R^*$.
[$iii \Rightarrow i$] For every pair of columns c_k and c_h of A there is $r_{kh} \in R^*$ such that $c_h = r_{kh}c_k$. Therefore for every $1 \leq i, j \leq n$ we have

$$a_{ik}a_{jh} - a_{ih}a_{jk} = r_{kh}(a_{ik}a_{jk} - a_{ik}a_{jk}) = 0,$$

which shows that $I_2(A) = (0)$. Moreover, since the entries of A are primitive we have $I_1(A) = R$, so that $\mathrm{rk}(A) = 1$. □

Remark 2.2.6. Lemma 2.2.5 provides us with an equivalent and practical way of testing whether two points $(X_0 : \ldots : X_n), (Y_0 : \ldots : Y_n) \in \mathbb{P}^n(R)$ are equal, by testing for every $i, j \in \{0, \ldots, n\}$ if $X_iY_j - X_jY_i = 0$. In the following sections and chapters this procedure is always adopted for verifying projective points equalities.

2.2.2 Elliptic curves over rings

In this section we define elliptic curves over commutative rings R with unity by extending Definition 1.1.4. However, a technical condition on the ring is needed in order to endow these objects with a group structure.

Condition 2.2.7. *For every pair of positive integers $n, m \in \mathbb{Z}_{\geq 1}$ and every matrix*

$$A = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \in M_{n,m}(R)$$

with strong rank $\mathrm{rk}(A) = 1$ *and primitive entries, there exists an R-linear combination of the columns of A whose entries are primitive.*

We notice that when the above combination exists, then it is unique in $\mathbb{P}^n(R)$ by Lemma 2.2.5.

Remark 2.2.8. Condition 2.2.7 is trivially satisfied when R is a field. In fact, if A has primitive entries then it has a non-zero entry a_{ij}, so that the j-th column is primitive.

More generally, in [42] it is pointed out that rings R satisfying Condition 2.2.7 are such that every projective R-module of rank 1 is free or, equivalently, those having vanishing Picard group. We do not use these characterizations in the continuation of the present work, so we refer an interested reader to [5].

Definition 2.2.9 (Elliptic curve over R)**.** Let R be a commutative ring with unity satisfying Condition 2.2.7 and let $A, B \in R$ such that $\Delta_{A,B} = -(4A^3 + 27B^2) \in R^*$. The *elliptic curve* defined by $F_{A,B} = x^3 + Axz^2 + Bz^3 - y^2z \in R[x, y, z]$ is

$$\mathcal{E}_{A,B}(R) = \{(X : Y : Z) \in \mathbb{P}^2(R) \mid Y^2Z = X^3 + AXZ^2 + BZ^3\}.$$

Given an elliptic curve $\mathcal{E} = \mathcal{E}_{A,B}(R)$, we denote by $\mathcal{O} = (0 : 1 : 0) \in \mathcal{E}$ its *zero element*, with $\mathcal{E}^a = \mathcal{E} \cap \mathbb{P}^2_{\text{aff}}(R)$ its *affine points* and with $\mathcal{E}^\infty$ the remaining points, which are called *points at infinity*.

The formulae from Section 1.2, which are guaranteed to work over fields, may also be used to define a sum operation on $\mathcal{E}_{A,B}(R)$. In this more general setting, a pair of points (P_1, P_2) is called *exceptional* for an addition law if the defining polynomials S_1, S_2, S_3 evaluated in the entries of P_1 and P_2 produce a non-primitive set of elements.

Definition 2.2.10 (Point sum on $\mathcal{E}_{A,B}(R)$)**.** Let $P_1, P_2 \in \mathcal{E}_{A,B}(R)$. We define their *sum* $P_1 + P_2$ as any primitive R-combination of the vectors $P_1 +_{(0:1:0)} P_2$ and $P_1 +_{(0:0:1)} P_2$, where the latter two sums are those defined in Section 1.2.

Proposition 2.2.11 ([42], Section 3)**.** *The point sum always defines a unique point on the elliptic curve $\mathcal{E}_{A,B}(R)$. Moreover, $\mathcal{E}_{A,B}(R)$ with this sum is an abelian group whose unity is $\mathcal{O}$ and the inverse of a point is given by*

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

Proof. Let us consider any triple of points

$$P_1 = (X_1 : Y_1 : Z_1),\ P_2 = (X_2 : Y_2 : Z_2),\ P_3 = (X_3 : Y_3 : Z_3) \in \mathbb{P}^2(R),$$

let $F = x^3 + Axz^2 + Bz^3 - y^2z \in R[x, y, z]$ and define the ideal

$$J = \langle F(P_1), F(P_2), F(P_3) \rangle \subseteq R.$$

First we prove that $P_1 + P_2$ is uniquely defined. Let us define

$$(U_1, U_2, U_3) = P_1 +_{(0:0:1)} P_2,$$
$$(V_1, V_2, V_3) = P_1 +_{(0:1:0)} P_2.$$

We computationally verify [Appendix A.1] that all the 2 × 2-minors of

$$M = \begin{bmatrix} U_1 & V_1 \\ U_2 & V_2 \\ U_2 & V_2 \end{bmatrix}$$

belong to J.[1] Thus, whenever $P_1, P_2 \in \mathcal{E}_{A,B}(R)$ the strong rank of M is 1. We prove that M is also primitive: assume by contradiction that $I = \langle U_i, V_i \rangle_{i \in \{1,2,3\}} \neq R$, then by Zorn's lemma there exists a maximal ideal $I \subseteq \mathfrak{m} \subsetneq R$. Both $(U_i \bmod \mathfrak{m})$ and $(V_i \bmod \mathfrak{m})$ are equal to the zero vector of $(R/\mathfrak{m})^3$, contradicting the fact that $\{+_{(0:1:0)}, +_{(0:0:1)}\}$ is a complete system of addition laws over the field $R/\mathfrak{m}$.

Therefore, M is primitive with $\mathrm{rk}(M) = 1$ and Condition 2.2.7 guarantees that there exists a primitive R-combination among (U_1, U_2, U_3) and (V_1, V_2, V_3). By Lemma 2.2.5 this combination is also unique, so it defines $P_1 + P_2$.

Now we show that this operation satisfies the group axioms. Given two primitive triples $(X_1, Y_1, Z_1),\ (X_2, Y_2, Z_2) \in R^3$, we may define

$$c_1 = [X, Y] = X_1Y_2 - X_2Y_1,$$
$$c_2 = [X, Z] = X_1Z_2 - X_2Z_1,$$
$$c_3 = [Y, Z] = Y_1Z_2 - Y_2Z_1.$$

As observed in Remark 2.2.6, they represent the same point in $\mathbb{P}^2(R)$ if and only if

$$c_1 = c_2 = c_3 = 0.$$

[1] In our computational verification, this is checked by proving that they may be expressed as integer polynomials in elements of R.

If the above triples are coordinates of points in $\mathcal{E}_{A,B}(R)$, it is sufficient to show that

$$c_1,\ c_2,\ c_3 \in J,$$

which may be straightforwardly tested. In fact, we verify [Appendix A.2] that

- [Closure] If $S_1, S_2, S_3 \in R$ are such that $P_1 + P_2 = (S_1 : S_2 : S_3)$ then

$$F(S_1, S_2, S_3) \in J.$$

- [Commutativity] $P_1 + P_2 = P_2 + P_1 \in \mathbb{P}^2(R)$.
- [Associativity] $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3) \in \mathbb{P}^2(R)$.
- [Identity] $P_1 + \mathcal{O} = P_1 \in \mathbb{P}^2(R)$.
- [Inverse] $P_1 + (X_1 : -Y_1 : Z_1) = \mathcal{O} \in \mathbb{P}^2(R)$.

This proves the second part of the statement and concludes the proof. □

For any elliptic curve $\mathcal{E}_{A,B}(R)$ and any proper ideal $I \subsetneq R$, since $\Delta_{A,B} \in R^*$ then $\Delta_{A,B} \notin I$ so $\Delta_{A,B} \in (R/I)^*$, which implies that $\mathcal{E}_{A,B}(R/I)$ is in turn an elliptic curve. Moreover, since the sum is defined by polynomial operations in the entries of the considered points, it commutes with the ring projection $R \twoheadrightarrow R/I$. Thus, the following is a well-defined group morphism.

Definition 2.2.12 (Canonical projection)**.** Let $\mathcal{E}_{A,B}(R)$ be an elliptic curve and $I \subsetneq R$ be a proper ideal of R. We define the *canonical projection* as the group morphism

$$\begin{aligned} \pi : \mathcal{E}_{A,B}(R) &\to \mathcal{E}_{A,B}(R/I), \\ (X_0 : \ldots : X_n) &\mapsto (X_0 \bmod I : \ldots : X_n \bmod I). \end{aligned}$$

We say that $P \in \mathcal{E}_{A,B}(R)$ *lies over* $\overline{P} \in \mathcal{E}_{A,B}(R/I)$ if $\pi(P) = \overline{P}$.

We conclude this section by noting that Definition 2.2.10 is somehow “essential”: the addition formulae that are working over fields have no hope of composing a complete system of addition laws over general rings.

Example 2.2.13. Let $\mathcal{E}_{0,1}(\mathbb{Z}/35\mathbb{Z})$ be the elliptic curve defined by

$$Y^2Z \equiv X^3 + Z^3 \bmod 35.$$

We consider its point $P = (20 : 21 : 15)$ and we sum it with $\mathcal{O}$ by using the addition laws corresponding to $(0 : 0 : 1)$ and $(0 : 1 : 0)$:

$$\begin{aligned} P +_{(0:0:1)} \mathcal{O} &= (20, 0, 15) \notin \mathbb{P}^2(\mathbb{Z}/35\mathbb{Z}),\\ P +_{(0:1:0)} \mathcal{O} &= (0, 21, 0) \notin \mathbb{P}^2(\mathbb{Z}/35\mathbb{Z}). \end{aligned}$$

A primitive linear combination of the triples is obtained by componentwisely adding them, so that $P + \mathcal{O} = (20 : 21 : 15)$, which is P. Notice that any other combination $(20, 21\alpha, 15)$ is primitive if and only if $\alpha \not\equiv 0 \bmod 5$. If this is the case, the element β defined by

$$\begin{cases} \beta \equiv 1 \bmod 7,\\ \beta \equiv \alpha \bmod 5, \end{cases}$$

is invertible in $\mathbb{Z}/35\mathbb{Z}$ and satisfies $\beta(20, 21, 15) = (20, 21\alpha, 15)$. Hence, these points are all equal to P inside $\mathbb{P}^2(\mathbb{Z}/35\mathbb{Z})$.

2.3 ELLIPTIC CURVES OVER $\mathbb{Z}/N\mathbb{Z}$

2.3.1 The $\mathbb{Z}/N\mathbb{Z}$-case

Let $N \in \mathbb{Z}_{\geq 2}$ be an integer. Hereafter we consider elliptic curves defined over the ring $R = \mathbb{Z}/N\mathbb{Z}$, over which Condition 2.2.7 is always satisfied. We give a simple proof for these specific rings, although in [42] it has been proved to hold for every finite ring.

Lemma 2.3.1. *Let $N \in \mathbb{Z}_{\geq 2}$ be an integer and A be a matrix over $\mathbb{Z}/N\mathbb{Z}$ whose entries are primitive, then there exists a linear combination of the columns of A that is primitive.*

In particular, $R = \mathbb{Z}/N\mathbb{Z}$ satisfies Condition 2.2.7.

Proof. Let $A = (c_1|c_2|\dots|c_m)$ be the columns of the considered matrix. Since A is primitive, for every prime $p|N$ there are coefficients $\alpha_1^{(p)}, \dots, \alpha_m^{(p)} \in \mathbb{Z}/p\mathbb{Z}$ such that the vector

$$v^{(p)} = \sum_{i=1}^{m} \alpha_i^{(p)} c_i$$

is primitive over $\mathbb{Z}/p\mathbb{Z}$. Therefore by Chinese Reminder Theorem we may find integers $\beta_i \in \mathbb{Z}$ solving the congruence system

$$\left(\beta_i \equiv \alpha_i^{(p)} \pmod p\right)_{p|N}.$$

Thus, $v = \sum_{i=1}^{m} \beta_i c_i$ is primitive. In fact, if there were a prime factor of N dividing all its entries, then v would be the zero-vector modulo p, contradicting its construction. □

Remark 2.3.2. The previous result witnesses how special $\mathbb{Z}/N\mathbb{Z}$ is: Lemma 2.3.1 holds for every matrix with primitive entries, not only for those of strong rank 1 as we require from general rings.

Ascertained the existence of a group operation on elliptic curves over $\mathbb{Z}/N\mathbb{Z}$, we aim at studying their point group structure. For dealing only with short Weierstrass equations, we always assume $2, 3 \nmid N$.

We forthwith notice that, by Chinese Reminder Theorem, the problem may be simplified by considering only its p-subgroups, for p ranging among the prime divisors of N.

Proposition 2.3.3 ([74], Corollary 2.32)**.** *Let N_1, N_2 be coprime integers and $A, B \in \mathbb{Z}$ such that $\Delta_{A,B} \in (\mathbb{Z}/N_1N_2\mathbb{Z})^*$. Then the canonical projections induce a group isomorphism*

$$\mathcal{E}_{A,B}(\mathbb{Z}/N_1N_2\mathbb{Z}) \simeq \mathcal{E}_{A,B}(\mathbb{Z}/N_1\mathbb{Z}) \oplus \mathcal{E}_{A,B}(\mathbb{Z}/N_2\mathbb{Z}).$$

Therefore, for every $N \in \mathbb{Z}_{\geq 2}$ the point group of a curve over $\mathbb{Z}/N\mathbb{Z}$ may de decomposed as a direct sum of groups

$$\mathcal{E}_{A,B}(\mathbb{Z}/N\mathbb{Z}) \simeq \bigoplus_{\substack{p\in\mathcal{P}\\ p|N}} \mathcal{E}_{A,B}(\mathbb{Z}/p^{\mathrm{v}_p(N)}\mathbb{Z}).$$

Hence, it is sufficient to study the group structure of elliptic curves $\mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ for p prime.

First, we notice that the points of such curves always have prescribed representatives.

Lemma 2.3.4. *Let $e \in \mathbb{Z}_{\geq 1}$, $p \in \mathcal{P}$ and $P \in \mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be a point of an elliptic curve.*

- *If P lies over an affine point of $\mathcal{E}_{A,B}(\mathbb{F}_p)$, then there are $X, Y \in \mathbb{Z}/p^e\mathbb{Z}$ such that*

$$P = (X : Y : 1).$$

- *If P lies over $\mathcal{O} \in \mathcal{E}_{A,B}(\mathbb{F}_p)$, then there are $X, Z \in p(\mathbb{Z}/p^e\mathbb{Z})$ such that*

$$P = (X : 1 : Z).$$

Proof. Let $P = (X : Y : Z)$ and $\pi(P) = (\overline{X} : \overline{Y} : \overline{Z})$. If $\pi(P)$ is affine then $\overline{Z} \in (\mathbb{Z}/p\mathbb{Z})^*$ then also $Z \in (\mathbb{Z}/p^e\mathbb{Z})^*$, which implies $P = (\frac{X}{Z} : \frac{Y}{Z} : 1)$. Instead, if $\pi(P) = \mathcal{O}$ then both Z and X belong to $p(\mathbb{Z}/p^e\mathbb{Z})$. But P must have primitive entries, hence $Y \in (\mathbb{Z}/p\mathbb{Z})^*$ so that $P = (\frac{X}{Y} : 1 : \frac{Z}{Y})$. □

Remark 2.3.5. A point cannot be represented by both the forms of Lemma 2.3.4, since either $\mathrm{GCD}(p, Z) = 1$ or $p|Z$. However, if $YZ \equiv 1 \bmod p^e$, then we may write an affine point as $(X : Y : 1) = (XZ : 1 : Z)$. In particular, if the curve is made only of points with an invertible second coordinate, they may all be written as $(X : 1 : Z)$ and the points at infinity are precisely those with a not-invertible X. Nonetheless, we notice that this is not always the case $\big($e.g.: $(3 : 7 : 1) \in \mathcal{E}_{6,4}(\mathbb{Z}/49\mathbb{Z})\big)$.

2.3.2 Points at infinity

Inspired by the ideas of [67, Chapter IV], in this section we develop an explicit description of the sum operation for points at infinity, i.e. those lying over $\mathcal{O}$.

To simplify the exposition, for any $X \in \mathbb{Z}/p^e\mathbb{Z}$ and any integer $0 \leq t \leq e$ we write $p^t|X$ or $X \equiv 0 \bmod p^t$ in place of the more precise $X \in p^t(\mathbb{Z}/p^e\mathbb{Z})$. It can easily be made formally accurate by considering any integer representative of X.

In the same spirit, we assign a p-adic valuation to elements $X \in \mathbb{Z}/p^e\mathbb{Z}$ by writing

$$\mathrm{v}_p(X) = \begin{cases} t & \text{if } X \in p^t(\mathbb{Z}/p^e\mathbb{Z}) \setminus p^{t+1}(\mathbb{Z}/p^e\mathbb{Z}), \\ e & \text{if } X = 0. \end{cases}$$

Proposition 2.3.6. *Let $e \in \mathbb{Z}_{\geq 1}$, $p \in \mathcal{P}$ and $\mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic curve. There is a polynomial $f \in \mathbb{Z}[x]$ of degree at most $e-1$ such that for every $P \in \mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ lying over $\mathcal{O} \in \mathcal{E}_{A,B}(\mathbb{F}_p)$ there is $X \equiv 0 \bmod p$ satisfying*

$$P = \big(X : 1 : f(X)\big).$$

Moreover, we have

$$f(X) \equiv X^3 + AX^7 + BX^9 \bmod p^{10}.$$

Proof. By Lemma 2.3.4 we know that points at infinity inside $\mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ are of the form $(X : 1 : Z)$ with $p|X$, $p|Z$ and they satisfy

$$Z \equiv X^3 + AXZ^2 + BZ^3 \bmod p^e.$$

We recursively define the following sequence of polynomials in $\mathbb{Z}[x, z]$:

$$F_0(x, z) = x^3 + Axz^2 + Bz^3, \qquad \forall\, i \in \mathbb{Z}_{\geq 1} : \; F_i(x, z) = F_{i-1}\big(x, F_0(x, z)\big).$$

It is easy to see by induction on $i \in \mathbb{Z}_{\geq 0}$ that this sequence satisfies

$$Z \equiv F_i(X, Z) \bmod p^e.$$

Moreover, every F_i for $i \in \mathbb{Z}_{\geq 1}$ is obtained from F_{i-1} by substituting all the occurrences of z with terms of degree 3, hence the total degree of terms involving z in F_i is strictly increasing while increasing i. This means that there exists an integer $M \in \mathbb{Z}_{\geq 0}$ such that

$$F_M(x,z) = f(x) + g(x,z), \qquad \text{with } \begin{cases} \deg(g) \geq e, \\ \deg(f) < e. \end{cases}$$

Since both X and Z are divisible by p, this means that

$$Z \equiv F_M(X,Z) \equiv f(X) \bmod p^e,$$

so that $f \in \mathbb{Z}[x]$ is the required polynomial. A direct computation shows that

$$\begin{aligned}
F_1 &= x^3 + z^2(Ax + Bz), \\
F_2 &= x^3 + Ax^7 + Bx^9 + 3ABx^7z^2 + 3B^2x^6z^3 + 3A^2Bx^5z^4 + 2A^2x^5z^2 + 6AB^2x^4z^5 \\
&\quad + 2ABx^4z^3 + (A^3B + 3B^3)x^3z^6 + A^3x^3z^4 + 3A^2B^2x^2z^7 + 2A^2Bx^2z^5 + 3AB^3xz^8 \\
&\quad + AB^2xz^6 + B^4z^9, \\
F_3 &= x^3 + Ax^7 + Bx^9 + (\text{terms of degree} \geq 11),
\end{aligned}$$

which proves the moreover part. □

Proposition 2.3.7. *Let $e \in \mathbb{Z}_{\geq 1}$, $p \in \mathcal{P}$ and $\mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic curve. Let also*

$$P_1 = \big(X_1 : 1 : f(X_1)\big),\ P_2 = \big(X_2 : 1 : f(X_2)\big) \in \mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$$

be two points lying over $\mathcal{O} \in \mathcal{E}_{A,B}(\mathbb{F}_p)$ with $e_1 = \mathrm{v}_p(X_1)$ and $e_2 = \mathrm{v}_p(X_2)$. Then we have $P_1 + P_2 = \big(X_3 : 1 : f(X_3)\big)$ with

$$X_3 \equiv X_1 + X_2 \bmod p^{5\min\{e_1,e_2\}}.$$

Proof. Since the canonical projection is a group morphism, the sum of two points lying over $\mathcal{O}$ lies itself over $\mathcal{O}$, which implies that these points are never exceptional for $+_{(0:1:0)}$. A straightforward computation with this addition formula shows that, modulo monomials in X_1 and X_2 of total degree at least 5 (i.e. modulo $p^{5\min\{e_1,e_2\}}$), the sum $P_1 + P_2$ is given by

$$P_1 + P_2 = \big(X_1 + X_2 : 1 + 3AX_1^2X_2^2 : (X_1 + X_2)^3\big),$$

which is equal to $\big(X_1 + X_2 : 1 : (X_1 + X_2)^3\big)$ as we establish by multiplying its entries by $1 - 3AX_1^2X_2^2 \in (\mathbb{Z}/p^{5\min\{e_1,e_2\}}\mathbb{Z})^*$. □

2.3.3 Group structure

In this section we describe the group structure of elliptic curves over $\mathbb{Z}/p^e\mathbb{Z}$. The size of those curves is known, by means of Hensel's lemma.

Lemma 2.3.8 ([42], Section 4)**.** *Let $e \in \mathbb{Z}_{\geq 1}$ be a positive integer, $p \in \mathcal{P}$ be a prime and $\mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic curve. Then for every $P \in \mathcal{E}_{A,B}(\mathbb{F}_p)$ we have*

$$|\pi^{-1}(P)| = p^{e-1}.$$

In particular, the size of the curve is

$$|\mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})| = p^{e-1}|\mathcal{E}_{A,B}(\mathbb{F}_p)|.$$

Proof. If $P = \mathcal{O}$ we already know by Proposition 2.3.6 that any point over $\mathcal{O}$ may be written for some $X \in p(\mathbb{Z}/p^e\mathbb{Z})$ as $\big(X : 1 : f(X)\big)$. Since every point of this form lies over $\mathcal{O}$, they are as many as the possible choices of X, namely p^{e-1}.

Let us now assume $P = (X : Y : 1)$ affine and consider the curve polynomial

$$F(x, y, z) = x^3 + Axz^2 + Bz^3 - y^2z \in \mathbb{Z}[x, y, z].$$

Since $\mathcal{E}_{A,B}(\mathbb{F}_p)$ is not singular, at least one between $\partial_x F(P)$ and $\partial_y F(P)$ is non-zero modulo p: in fact, if they were both zero, by Euler's Homogeneous Function Theorem we would have

$$\partial_z F(P) \equiv X\partial_x F(P) + Y\partial_y F(P) + \partial_z F(P) \equiv 3F(P) \equiv 0 \bmod p, \tag{2.2}$$

and P would be singular. Thus, let us assume $\partial_x F(P) \not\equiv 0 \bmod p$. For every integer

$\alpha \in \{0, 1, \ldots, p^{e-1} - 1\}$ we may define $g_\alpha \in \mathbb{Z}[w]$ as

$$g_\alpha(w) = F(w, Y + \alpha p, 1).$$

By definition $g_\alpha(X) \equiv 0 \bmod p$, and $\partial_w g_\alpha(X) \equiv \partial_x F(P) \not\equiv 0 \bmod p$, then by Hensel's Lemma there exists a unique $\chi_\alpha \in \mathbb{Z}/p^e\mathbb{Z}$ such that $\chi_\alpha \equiv X \bmod p$ and $g_\alpha(\chi_\alpha) \equiv 0 \bmod p^e$. Therefore, we have constructed a point

$$P_\alpha = (\chi_\alpha : Y + \alpha p : 1) \in \mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$$

lying over P. These $\{P_\alpha\}_{\alpha \in \{0,1,\ldots,p^{e-1}-1\}}$ are all distinct and by uniqueness of Hensel's Lemma every point $(X_1 : Y_1 : 1) \in \mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ over P arises in this way, as

$$(X_1 : Y_1 : 1) = P_{\alpha'}, \quad \text{with} \quad \alpha' = \left(\frac{Y_1 - Y}{p}\right).$$

We conclude that $\{P_\alpha\}_{\alpha \in \{0,1,\ldots,p^{e-1}-1\}}$ are all the points of $\mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ over P.

If, instead, $\partial_x F(P) \equiv 0 \bmod p$ and $\partial_y F(P) \not\equiv 0 \bmod p$, the same result is obtained by considering the polynomial

$$g_\beta(w) = F(X + \beta p, w, 1).$$

In each cases, there are p^{e-1} points lying over P, which concludes the proof. □

We are ready to characterize the point group structure of elliptic curves over $\mathbb{Z}/p^e\mathbb{Z}$.

Theorem 2.3.9. *Let $e \in \mathbb{Z}_{\geq 1}$ be a positive integer, $p \in \mathcal{P}$ be a prime and $\mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic curve. Then*

$$0 \to \big\langle \big(p : 1 : f(p)\big) \big\rangle \xrightarrow{\text{id}} \mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) \xrightarrow{\pi} \mathcal{E}_{A,B}(\mathbb{F}_p) \to 0.$$

is a short exact sequence of groups.

Proof. We know that the canonical projection $\pi : \mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) \twoheadrightarrow \mathcal{E}_{A,B}(\mathbb{F}_p)$ is a surjective group morphism and that $|\ker \pi| = p^{e-1}$ by Lemma 2.3.8. Thus, it is sufficient to prove that

$\big(p : 1 : f(p)\big) \in \ker\pi$ has order p^{e-1}. It lies over $\mathcal{O} \in \mathcal{E}_{A,B}(\mathbb{F}_p)$ by means of Proposition 2.3.6 and its order is a power of p since $\ker\pi$ is a p-group. We prove by induction on $0 \leq \epsilon \leq e-1$ that[2]

$$p^{\epsilon}\big(p : 1 : f(p)\big) = \big(X : 1 : f(X)\big) \quad \text{with } \mathrm{v}_p(X) = \epsilon + 1.$$

In particular, the minimal ϵ such that $X \equiv 0 \bmod p^e$ is $\epsilon = e-1$.
[$\epsilon = 0$] It is trivially seen that

$$p^{0}\big(p : 1 : f(p)\big) = \big(p : 1 : f(p)\big) \quad \text{with } \mathrm{v}_p(p) = 1.$$

[$\epsilon \to \epsilon + 1$] By the inductive hypothesis we know that

$$p^{\epsilon+1}\big(p : 1 : f(p)\big) = p\big(X : 1 : f(X)\big) \quad \text{with } \mathrm{v}_p(X) = \epsilon + 1.$$

By Proposition 2.3.7 and induction on $\alpha \in \{1, \ldots, p-1\}$ we have

$$\big(X : 1 : f(X)\big) + \big(\alpha X : 1 : f(\alpha X)\big) = \big(X_2 : 1 : f(X_2)\big)$$

with

$$X_2 \equiv (\alpha + 1)X \bmod p^{5(\epsilon+1)}.$$

Thus, by specializing the above result for $\alpha = p-1$, the p-adic valuation of the first component of $p\big(X : 1 : f(X)\big)$ is proved to be $\mathrm{v}_p(X) + 1 = \epsilon + 2$. □

The above theorem uniquely determines the group structure when the projected curve is not anomalous.

Corollary 2.3.10. *Let $e \in \mathbb{Z}_{\geq 1}$ be a positive integer, $p \in \mathcal{P}$ be a prime and $\mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic curve such that $|\mathcal{E}_{A,B}(\mathbb{F}_p)| \neq p$. Then*

$$\mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) \simeq \mathcal{E}_{A,B}(\mathbb{F}_p) \oplus \mathbb{Z}/p^{e-1}\mathbb{Z}.$$

[2] If $\epsilon \geq e$ we clearly have $p^{\epsilon}\big(p : 1 : f(p)\big) = \mathcal{O}$, and by definition $\mathrm{v}_p(0) = e$.

Proof. It is sufficient to show that the short exact sequence provided by Theorem 2.3.9 is a split sequence, which by the Splitting Lemma amounts to proving that it is left split.

Let $q = |\mathcal{E}_{A,B}(\mathbb{F}_p)|$ be the size of the projected curve. Since we assumed $p \neq q$ then by Theorem 1.3.1 we have $\mathrm{GCD}(p, q) = 1$, so we can find an integer $k \in \mathbb{Z}$ satisfying

$$\begin{cases} k \equiv 1 \bmod p^{e-1}, \\ k \equiv 0 \bmod q. \end{cases}$$

We prove that the multiplication-by-k is a left section for the considered sequence. In fact, since $k \equiv 0 \bmod q$ then

$$\mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) \xrightarrow{\cdot k} \big\langle \big(p : 1 : f(p)\big) \big\rangle$$

is a well-defined group morphism. Moreover, since $k \equiv 1 \bmod p^{e-1}$ the cyclic group $\big\langle \big(p : 1 : f(p)\big) \big\rangle$ is fixed under this map, hence $\mathrm{id}_1 \circ (\cdot k) = \mathrm{id}_2$, where id_1 is the injection $\big\langle \big(p : 1 : f(p)\big) \big\rangle \hookrightarrow \mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$, while id_2 is the actual identity map on $\big\langle \big(p : 1 : f(p)\big) \big\rangle$. □

In particular, Corollary 2.3.10 shows that if the group of points of a non-anomalous curve $\mathcal{E} = \mathcal{E}_{A,B}(\mathbb{F}_p)$ is cyclic, then the point group of every elliptic curve lying over $\mathcal{E}$ is also cyclic.

When the exponent e is small, an explicit group isomorphism may be exhibited.

Proposition 2.3.11. *Let $1 \leq e \leq 5$ be an integer, $p \in \mathcal{P}$ be a prime, $\mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic curve and $q = |\mathcal{E}_{A,B}(\mathbb{F}_p)|$ be the size of its projected curve. Then the map*

$$\begin{aligned} \Phi : \mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) &\to \mathcal{E}_{A,B}(\mathbb{F}_p) \oplus \mathbb{Z}/p^{e-1}\mathbb{Z}, \\ P &\mapsto \left(\pi(P), \frac{1}{p}\frac{(qP)_x}{(qP)_y} \right), \end{aligned}$$

is a well-defined group morphism. Moreover, if $q \neq p$ then Φ is a group isomorphism.

Proof. It is easy to see that $\Phi(P)$ does not depend on the representative of P. Moreover, since π as in Definition 2.2.12 is a group morphism, then

$$\pi(qP) = q\pi(P) = \mathcal{O} \in \mathcal{E}_{A,B}(\mathbb{F}_p).$$

Hence, by Proposition 2.3.6 we can write $qP = \big(X : 1 : f(X)\big)$ for some $X \equiv 0 \pmod p$. Therefore, $\frac{(qP)_x}{(qP)_y} \in p(\mathbb{Z}/p^e\mathbb{Z})$, which is (canonically) isomorphic to $\mathbb{Z}/p^{e-1}\mathbb{Z}$ via the multiplication by $\frac{1}{p}$. Thus, Φ is a well-defined map between groups having, by Lemma 2.3.8, the same size.

This map is a group morphism: for every pair $P_1, P_2 \in \mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ we have

$$\Phi(P_1) + \Phi(P_2) = \left(\pi(P_1 + P_2), \frac{1}{p}\left(\frac{(qP_1)_x}{(qP_1)_y} + \frac{(qP_2)_x}{(qP_2)_y}\right)\right).$$

Since $e \leq 5 \leq 5 \min\{\mathrm{v}_p\big((qP_1)_x\big), \mathrm{v}_p\big((qP_2)_x\big)\}$ then by Proposition 2.3.7, we get

$$\frac{(qP_1)_x}{(qP_1)_y} + \frac{(qP_2)_x}{(qP_2)_y} = \frac{(qP_1 + qP_2)_x}{(qP_1 + qP_2)_y} = \frac{\big(q(P_1 + P_2)\big)_x}{\big(q(P_1 + P_2)\big)_y},$$

which is precisely the second component of $\Phi(P_1 + P_2)$.

It is now sufficient to prove that if $q \neq p$, then $\ker \Phi = \{\mathcal{O}\}$. From $\Phi(P) = (\mathcal{O}, 0)$ we get that P is a point at infinity, so $P = \big(X : 1 : f(X)\big)$, and since the second entry of $\Phi(P)$ is 0, we also have

$$\frac{qX}{p} \equiv \frac{(qP)_x}{p} \equiv 0 \bmod p^{e-1}.$$

Since $q \neq p$, then by Theorem 1.3.1 also $\mathrm{GCD}(p, q) = 1$ and we conclude that $X \equiv 0 \bmod p^e$, hence $P = \big(0 : 1 : f(0)\big) = \mathcal{O}$. □

2.3.4 The anomalous cases

When the restricted curve $\mathcal{E}_{A,B}(\mathbb{F}_p)$ is anomalous two different scenarios may occur. By Theorem 2.3.9 the curve $\mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ is guaranteed to contain a cyclic subgroup of order p^{e-1}, therefore it may be either cyclic

$$\mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) \simeq \mathbb{Z}/p^e\mathbb{Z}, \tag{Cyclic}$$

or split, i.e.

$$\mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) \simeq \mathbb{Z}/p^{e-1}\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}. \tag{Split}$$

These cases may both occur as it is witnessed by Example 2.3.18 and 2.3.19. Their behaviour is quite dissimilar, so we discuss them separately.

△ **Cyclic**

In the cyclic scenario there is a group morphism from which the discrete logarithm on the projected curve may be immediately read.

Proposition 2.3.12. *Let $e \in \mathbb{Z}_{\geq 2}$ be an integer, $p \in \mathcal{P}$ be a prime and $\mathcal{E} = \mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic curve, whose point group is cyclic of order p^e. Then the map*

$$\begin{aligned} \Theta : \mathcal{E} &\to \mathbb{F}_p, \\ P &\mapsto \frac{1}{p^{e-1}} \frac{(p^{e-1}P)_x}{(p^{e-1}P)_y}, \end{aligned}$$

is a well-defined surjective group morphism, whose kernel is

$$\ker \Theta = \langle (p : 1 : 0) \rangle.$$

Proof. For every $P \in \mathcal{E}$ the point $p^{e-1}P$ is a p-torsion point of $\mathcal{E}$, hence we have

$$p^{e-1}P = \big(X : 1 : f(X)\big), \qquad \text{with } \ \mathrm{v}_p(X) \geq e-1,$$

therefore $\Theta(P) = \frac{X}{p^{e-1}} \in \mathbb{F}_p$ is well-defined. Let $G \in \mathcal{E}$ be a generator of the point group of $\mathcal{E}$, then for every integer $m \in \mathbb{Z}$ we have

$$p^{e-1}mG = m\big(X : 1 : f(X)\big) = \big(mX : 1 : f(mX)\big),$$

where the last equality follows from Proposition 2.3.7, as for every $e \geq 2$ the point $p^{e-1}G$ lies in $\langle (p^{e-1} : 1 : 0) \rangle$. Thus, $\Theta(mG) = m\Theta(G)$, so that Θ is a group morphism. Moreover, from the above equation it follows that

$$\ker \Theta = \{mp\ G \mid m \in \mathbb{Z}\} = \langle (p : 1 : 0) \rangle.$$

By comparing the size of these groups, the surjectivity follows. □

From the above proposition, the discrete logarithm may be immediately recovered.

Corollary 2.3.13. *Let $e \in \mathbb{Z}_{\geq 2}$ be an integer, $p \in \mathcal{P}$ be a prime and $\mathcal{E} = \mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic curve, whose point group is cyclic of order p^e. Then the map*

$$\Theta \circ \pi^{-1} : \mathcal{E}(\mathbb{F}_p) \to \mathbb{F}_p$$

is a well-defined group isomorphism.

Proof. The canonical projection induces a group isomorphism $\mathcal{E}/\langle(p:1:0)\rangle \simeq \mathcal{E}(\mathbb{F}_p)$ by Theorem 2.3.9, whereas the map Θ of Proposition 2.3.12 induces a group isomorphism $\mathcal{E}/\langle(p:1:0)\rangle \simeq \mathbb{F}_p$. By composing those isomorphisms, the result follows. □

△ **Split**

In the split case, the multiplication-by-p morphism sends the p^2-1 points of order p to $\mathcal{O}$. As a result, we see that this map always produces at least a p^2-factor in the x-component of any point.

Proposition 2.3.14. *Let $e \in \mathbb{Z}_{\geq 1}$ be a positive integer, $p \in \mathcal{P}$ be a prime and consider an elliptic curve $\mathcal{E} = \mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ such that $\mathcal{E} \simeq \mathbb{Z}/p^{e-1}\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. Then for every $P \in \mathcal{E}$ there exists $X \in p^2(\mathbb{Z}/p^{e-1}\mathbb{Z})$ such that $pP = \big(X : 1 : f(X)\big)$.*

Proof. By Proposition 2.3.6 we know that $pP = \big(X : 1 : f(X)\big)$ with $p|X$. Moreover, by Theorem 2.3.9 we know that there exists $\alpha \in \{0, 1, \ldots, p^{e-1}-1\}$ such that

$$\big(X : 1 : f(X)\big) = \alpha\big(p : 1 : f(p)\big)$$

Since P has order at most p^{e-1}, then $p^{e-2}(pP) = \mathcal{O}$, so that

$$\mathcal{O} = p^{e-2}\big(X : 1 : f(X)\big) = \alpha p^{e-2}\big(p : 1 : f(p)\big).$$

As $\big(p : 1 : f(p)\big)$ generates a group of order p^{e-1}, we conclude that $p|\alpha$ so that, by Proposition 2.3.7, we have $p^2|X$. □

As a consequence, the explicit group morphism of Proposition 2.3.11 may be made surjective in this setting, by restricting its codomain.

Corollary 2.3.15. *Let $2 \leq e \leq 5$ be an integer, $p \in \mathcal{P}$ be a prime and $\mathcal{E} = \mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic curve such that $\mathcal{E} \simeq \mathbb{Z}/p^{e-1}\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. The map*

$$\begin{aligned}\Psi : \mathcal{E} &\to \mathcal{E}_{A,B}(\mathbb{F}_p) \oplus \mathbb{Z}/p^{e-2}\mathbb{Z},\\ P &\mapsto \left(\pi(P), \frac{1}{p^2}\frac{(pP)_x}{(pP)_y}\right),\end{aligned}$$

is a well-defined surjective group morphism, whose kernel is

$$\ker \Psi = \langle (p^{e-1} : 1 : 0) \rangle.$$

Proof. For every point $P \in \mathcal{E}$ we have $p^2 | (pP)_x$ by Proposition 2.3.14, hence the map Ψ is well-defined. Since it is equal to Φ of Proposition 2.3.11, with the second component divided by p, it is also a group morphism.

Let $P \in \ker \Psi$, then by Proposition 2.3.7 there is an element $X \in \mathbb{Z}/p^e\mathbb{Z}$ such that $P = \big(X : 1 : f(X)\big)$ and $\frac{pX}{p^2} \equiv 0 \bmod p^{e-2}$, hence $X \equiv 0 \bmod p^{e-1}$. Therefore, we have

$$\ker \Psi = \{(\alpha p^{e-1} : 1 : 0)\}_{\alpha \in \{0,\dots,p-1\}} = \langle (p^{e-1} : 1 : 0) \rangle.$$

Finally, by a size comparison (Lemma 2.3.8) the morphism Ψ is also surjective. □

In the split case the short exact sequence of Theorem 2.3.9 splits, therefore there is a right section. Actually, there are many: if $s : \mathcal{E}_{A,B}(\mathbb{F}_p) \to \mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ is a section, it immediately follows that $\forall \alpha \in \{0, 1, \dots, p^{e-1} - 1\}$ also $\cdot(\alpha p + 1) \circ s$ are right sections.

Remark 2.3.16. We shall relate the split case to the canonical lift of $\mathcal{E}_{A,B}(\mathbb{F}_p)$, which has been introduced in [18, 46] and applied to anomalous lifts in [73]. Hence, this case is expected to occur with probability $\frac{1}{p}$ and may be effortlessly overcome by changing the curve coefficients of a p-multiple.

2.3.5 Some examples

In this section we provide concrete instances of the previous results, both in the general case (Example 2.3.17) and in the anomalous ones (Example 2.3.18 and 2.3.19).

Example 2.3.17. Let us consider the curve $\mathcal{E}_{3,3}(\mathbb{Z}/49\mathbb{Z})$, whose projection has size $|\mathcal{E}_{3,3}(\mathbb{F}_7)| = 6$. According to Corollary 2.3.10 its group structure is

$$\mathcal{E}_{3,3}(\mathbb{Z}/49\mathbb{Z}) \simeq \mathcal{E}_{3,3}(\mathbb{F}_7) \oplus \mathbb{F}_7.$$

The proof of the same Corollary also provides us with a left section for the exact sequence of Theorem 2.3.9, i.e. the multiplication-by-36 map. We also have an explicit group isomorphism from Proposition 2.3.11, which is visually represented by the following table.

$\xleftarrow{\cdot 6}$

$\mathbb{F}_7$	6	(42:1:0)	(39:39:1)	(45:5:1)	(8:7:1)	(38:16:1)	(4:31:1)	
	5	(35:1:0)	(32:25:1)	(24:40:1)	(8:14:1)	(10:2:1)	(11:17:1)	
	4	(28:1:0)	(25:11:1)	(3:26:1)	(8:21:1)	(31:37:1)	(18:3:1)	
	3	(21:1:0)	(18:46:1)	(31:12:1)	(8:28:1)	(3:23:1)	(25:38:1)	
	2	(14:1:0)	(11:32:1)	(10:47:1)	(8:35:1)	(24:9:1)	(32:24:1)	
	1	(7:1:0)	(4:18:1)	(38:33:1)	(8:42:1)	(45:44:1)	(39:10:1)	
	0	**(0:1:0)**	**(46:4:1)**	**(17:19:1)**	**(8:0:1)**	**(17:30:1)**	**(46:45:1)**	$\downarrow \pi$
		(0:1:0)	(4:4:1)	(3:5:1)	(1:0:1)	(3:2:1)	(4:3:1)	

$\mathcal{E}_{3,3}(\mathbb{F}_7)$

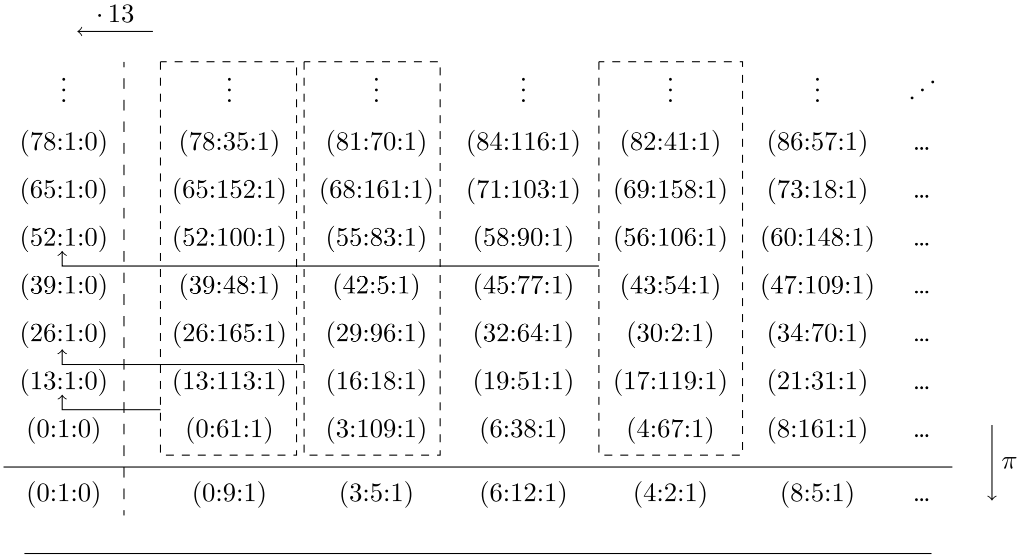
In reference to the above diagram, a right section for the sequence of Theorem 2.3.9 is obtained by sending the points of $\mathcal{E}_{3,3}(\mathbb{F}_7)$ to their bold representatives in $\mathcal{E}_{3,3}(\mathbb{Z}/49\mathbb{Z})$.

It is easily seen that the discrete logarithm problem over the base curve could be efficiently solved if we were able to find lifted points with the same ratio as their base points. As an instance, if we knew that $(10 : 47 : 1) = 2 \cdot (4 : 18 : 1)$, we would immediately recover the (same) discrete logarithm between the corresponding projections $(3 : 5 : 1)$ and $(4 : 4 : 1)$. However, no way are known to consistently perform such lifts [66].

Example 2.3.18. By considering the elliptic curve $\mathcal{E}_{7,3}(\mathbb{Z}/13^2\mathbb{Z})$, we may verify that

$$\mathcal{E}_{7,3}(\mathbb{Z}/169\mathbb{Z}) \simeq \langle (0:61:1) \rangle.$$

Since $\Theta \circ \pi^{-1}$ is a group isomorphism, as prescribed by Corollary 2.3.13, when solving the discrete logarithm the choice of a lift is irrelevant: every lift of the same point is sent to the same point at infinity by the multiplication-by-13 morphism, as depicted below.



⋮	⋮	⋮	⋮	⋮	⋮	⋰
(78:1:0)	(78:35:1)	(81:70:1)	(84:116:1)	(82:41:1)	(86:57:1)	...
(65:1:0)	(65:152:1)	(68:161:1)	(71:103:1)	(69:158:1)	(73:18:1)	...
(52:1:0)	(52:100:1)	(55:83:1)	(58:90:1)	(56:106:1)	(60:148:1)	...
(39:1:0)	(39:48:1)	(42:5:1)	(45:77:1)	(43:54:1)	(47:109:1)	...
(26:1:0)	(26:165:1)	(29:96:1)	(32:64:1)	(30:2:1)	(34:70:1)	...
(13:1:0)	(13:113:1)	(16:18:1)	(19:51:1)	(17:119:1)	(21:31:1)	...
(0:1:0)	(0:61:1)	(3:109:1)	(6:38:1)	(4:67:1)	(8:161:1)	...
(0:1:0)	(0:9:1)	(3:5:1)	(6:12:1)	(4:2:1)	(8:5:1)	...

$\mathcal{E}_{7,3}(\mathbb{F}_{13})$

Thus, we can read the discrete logarithms in $\mathcal{E}_{7,3}(\mathbb{F}_{13})$ from any lift in $\mathcal{E}_{7,3}(\mathbb{Z}/169\mathbb{Z})$. As in instance, in the considered example we have

$$13 \cdot \pi^{-1}\big((4:2:1)\big) = \{(52:1:0)\} = \{4 \cdot (13:1:0)\},$$
$$13 \cdot \pi^{-1}\big((3:5:1)\big) = \{(26:1:0)\} = \{2 \cdot (13:1:0)\},$$

therefore

$$\log_{(3:5:1)}\left((4:2:1)\right) = \frac{\Theta \circ \pi^{-1}\left((4:2:1)\right)}{\Theta \circ \pi^{-1}\left((3:5:1)\right)} = \frac{4}{2} = 2.$$

There are no right sections in this case, as the only 13-subgroup is $\pi^{-1}(\mathcal{O})$.

Finally, it is also worth pointing out that this attack never fails, as for every affine point $P \in \mathcal{E}(\mathbb{F}_p)$ the map $\log_P$ is well-defined.

Example 2.3.19. We now consider the anomalous elliptic curve $\mathcal{E}_{1,6}(\mathbb{F}_{13})$. The point group of this curve over $\mathbb{Z}/169\mathbb{Z}$ is a direct product of two groups, namely

$$\mathcal{E}_{1,6}(\mathbb{Z}/169\mathbb{Z}) \simeq \langle(2:4:1)\rangle \oplus \langle(13:1:0)\rangle.$$

	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋰	
	6	(78:1:0)	(54:4:1)	(113:113:1)	(167:140:1)	(142:24:1)	(94:7:1)	...	
	5	(65:1:0)	(158:4:1)	(9:74:1)	(89:140:1)	(90:76:1)	**(107:33:1)**	...	
$\mathbb{F}_{13}$	4	(52:1:0)	(93:4:1)	(74:35:1)	(11:140:1)	**(38:128:1)**	(120:59:1)	...	
	3	(39:1:0)	(28:4:1)	(139:165:1)	**(102:140:1)**	(155:11:1)	(133:85:1)	...	
	2	(26:1:0)	(132:4:1)	**(35:126:1)**	(24:140:1)	(103:63:1)	(146:111:1)	...	
	1	(13:1:0)	**(67:4:1)**	(100:87:1)	(115:140:1)	(51:115:1)	(159:137:1)	...	
	0	**(0:1:0)**	(2:4:1)	(165:48:1)	(37:140:1)	(168:167:1)	(3:163:1)	...	$\downarrow \pi$
		(0:1:0)	(2:4:1)	(9:9:1)	(11:10:1)	(12:11:1)	(3:7:1)	...	

$\mathcal{E}_{1,6}(\mathbb{F}_{13})$

In this case, the multiplication-by-13 map annihilates every point of $\mathcal{E}_{1,6}(\mathbb{Z}/169\mathbb{Z})$. As mentioned in Remark 2.3.16, this situation may (rarely) occur. To solve the DLP in $\mathcal{E}_{1,6}(\mathbb{F}_{13})$, we can either change the considered coefficients to return to the cyclic scenario $\big($e.g. by considering $\mathcal{E}_{14,6}(\mathbb{Z}/169\mathbb{Z})\big)$ or look at higher ($e \geq 3$) powers of p and try to exploit the morphism given by Corollary 2.3.15. The latter case appears to be problematic, as it works only when the lifted points lie inside the same subgroup of $\mathcal{E}_{1,6}(\mathbb{Z}/2197\mathbb{Z})$, i.e. when the discrete logarithm actually exists in $\mathcal{E}_{1,6}(\mathbb{Z}/2197\mathbb{Z})$.

As an instance of the second approach, let $P = (2:4:1)$ and $Q = (1389:816:1)$, which lie over $(2:4:1)$ and $(11:10:1)$ respectively. Since they belong to the same subgroup of $\mathcal{E}_{1,6}(\mathbb{Z}/169\mathbb{Z})$, the discrete logarithm between the correspondent base points is given by

$$\log_{(2:4:1)}\big((11:10:1)\big) = \frac{(13\cdot Q)_x(13\cdot P)_y}{(13\cdot Q)_y(13\cdot P)_x} = \frac{338}{845} = \frac{2}{5} \equiv 3 \bmod 13.$$

In this case the ratio has not been preserved by lifting, as $Q = 16 \cdot P$.

CHAPTER 3
ELLIPTIC LOOPS

All the objects considered in Chapter 2 have been defined for given integers $A, B \in \mathbb{Z}$, but different choices of these parameters would have led to different, still well-defined, curves. In fact, for every $\alpha, \beta \in \mathbb{Z}$ and $e \in \mathbb{Z}_{\geq 1}$ the classical elliptic curve $\mathcal{E}_{A,B}(\mathbb{F}_p)$ underlies $\mathcal{E}_{A+\alpha p, B+\beta p}(\mathbb{Z}/p^e\mathbb{Z})$ and the projection

$$\pi : \mathcal{E}_{A+\alpha p, B+\beta p}(\mathbb{Z}/p^e\mathbb{Z}) \twoheadrightarrow \mathcal{E}_{A,B}(\mathbb{F}_p)$$

is a group morphism, as in Definition 2.2.12. In this chapter we consider the smallest algebraic object containing all these curves, for which the above projections are instances of the same reduction map.

3.1 SET DESCRIPTION

Definition 3.1.1 (Elliptic set)**.** Let $p \in \mathcal{P}$ be a prime and $e \in \mathbb{Z}_{\geq 1}$ be a positive integer. Let also $A, B \in \mathbb{Z}$ be integers such that $\Delta_{A,B} \not\equiv 0 \bmod p$. We define

$$\mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) = \{(X : Y : Z) \in \mathbb{P}^2(\mathbb{Z}/p^e\mathbb{Z}) \mid p^{e-1}(-Y^2Z + X^3 + AXZ^2 + BZ^3) = 0\},$$

and we call it the *Elliptic set* defined by (A, B) over $\mathbb{Z}/p^e\mathbb{Z}$.

By the same slight abuse of notation of Section 2.3.2, we may write

$$\mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) = \{(X : Y : Z) \in \mathbb{P}^2(\mathbb{Z}/p^e\mathbb{Z}) \mid Y^2Z \equiv X^3 + AXZ^2 + BZ^3 \bmod p\},$$

which is the characterization that we employ in this section.

We have a natural way to project points of elliptic sets onto points of the underlying elliptic curves.

Definition 3.1.2 (Canonical set projection)**.** We define the *canonical (set) projection* as the standard reduction map

$$\begin{aligned}\pi : \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) &\twoheadrightarrow \mathcal{E}_{A,B}(\mathbb{F}_p),\\ (X : Y : Z) &\mapsto (X \bmod p : Y \bmod p : Z \bmod p).\end{aligned}$$

For every pair of integers $\alpha, \beta \in \mathbb{Z}$ we also observe that $\mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ contains $\mathcal{E}_{A+\alpha p,B+\beta p}(\mathbb{Z}/p^e\mathbb{Z})$. In turn, $\mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ can obtained by adding suitable multiples of p to the coordinates of points of $\mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$, as in the following proposition.

Proposition 3.1.3. *Let $p \in \mathcal{P}$ and $e \in \mathbb{Z}_{\geq 1}$. Let also $A, B \in \mathbb{Z}$ defining an elliptic curve $\mathcal{E} = \mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$. Then for every point $P = (X : Y : Z)$ of $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ there exists a unique $\alpha \in \{0, 1, \ldots, p^{e-1} - 1\}$ such that*

(*i*) *If $p \nmid Y$, then $(X : Y + \alpha p : Z) \in \mathcal{E}$.*

(*ii*) *If $p|Y,\ p \nmid X$ and $p \nmid Z$, then $(X : Y : Z + \alpha p) \in \mathcal{E}$.*

(*iii*) *If $p|Y,\ p|X$ and $p \nmid Z$, then $(X + \alpha p : Y : Z) \in \mathcal{E}$.*

In particular, the size of $\mathcal{L}$ is

$$|\mathcal{L}| = p^{e-1}|\mathcal{E}| = p^{2(e-1)}|\mathcal{E}_{A,B}(\mathbb{F}_p)|.$$

Proof. According to P, we define the polynomial $F(\beta) \in \mathbb{Z}[\beta]$ as

$$\begin{aligned}
F(\beta) &= X^3 + AXZ^2 + BZ^3 - (Y+\beta)^2 Z && \text{if } p \nmid Y \quad \text{[case } (i)\text{]},\\
F(\beta) &= X^3 + AX(Z+\beta)^2 + B(Z+\beta)^3 - Y^2(Z+\beta) && \text{if } p|Y, p \nmid X \quad \text{[case } (ii)\text{]},\\
F(\beta) &= (X+\beta)^3 + A(X+\beta)Z^2 + BZ^3 - Y^2 Z && \text{if } p|Y, p|X \quad \text{[case } (iii)\text{]}.
\end{aligned}$$

Since $P \in \mathcal{L}$, regardless the considered case this polynomial satisfies $F(0) \equiv 0 \bmod p$. The corresponding derivatives modulo p are

$$\begin{aligned} F'(\beta) &\equiv -2(Y+\beta) \bmod p && [\text{case } (i)], \\ F'(\beta) &\equiv 2AX(Z+\beta)+3B(Z+\beta)^2 \bmod p && [\text{case } (ii)], \\ F'(\beta) &\equiv 3\beta^2+A \bmod p && [\text{case } (iii)]. \end{aligned}$$

In case (i) we have $p \nmid Y$, hence $F'(0) \equiv -2Y \not\equiv 0 \bmod p$.

In case (ii), we have $F'(0) \equiv (2AX+3BZ)Z \bmod p$. Since $p|Y$, necessarily $p \nmid Z$, so $F'(0)$ could vanish only if $\pi(P) = (3B : 0 : -2A)$, which cannot be a point of $\mathcal{E}(\mathbb{F}_p)$ since we are assuming $p \nmid X$, so $3B \not\equiv 0 \bmod p$, which implies $p \nmid B$ and

$$(3B)^3 + A(3B)(-2A)^2 + B(-2A)^3 = B(27B^2+4A^3) = B\Delta_{A,B} \not\equiv 0 \bmod p.$$

In case (iii) we have $F'(0) \equiv A \bmod p$, which cannot be zero since when $p|\gcd(X,Y)$ then the Weierstrass equation of $\mathcal{E}(\mathbb{F}_p)$ is $BZ^3 \equiv 0 \bmod p$, hence $B \equiv 0 \bmod p$, so that

$$0 \not\equiv \Delta_{A,B} \equiv 4A^3 \bmod p.$$

In each cases, $F'(0) \not\equiv 0 \bmod p$, therefore by Hensel's Lemma there is a unique $\alpha' \in \mathbb{Z}/p^e\mathbb{Z}$ such that $F(\alpha') \equiv 0 \bmod p^e$ and $\alpha' \equiv 0 \bmod p$. Thus, $\alpha = \frac{\alpha'}{p}$ seen as an integer between 0 and $p^{e-1}-1$ is the required element. □

Similarly to the curve-setting, we may distinguish between affine points and those at infinity, i.e. those lying over $\mathcal{O}_{\mathcal{E}_{A,B}(\mathbb{F}_p)}$.

Definition 3.1.4. Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be the elliptic set defined by (A,B) over $\mathbb{Z}/p^e\mathbb{Z}$. We define its *affine part* as

$$\mathcal{L}^a = \{(X:Y:Z) \in \mathcal{L} \mid \gcd(Z,p)=1\}$$

and its *part at infinity* as

$$\mathcal{L}^\infty = \{(X : Y : Z) \in \mathcal{L} \bigm| p|Z\}.$$

We refer to the points of $\mathcal{L}^a$ as *affine points* and to those of $\mathcal{L}^\infty$ as *points at infinity.*

Clearly the above definition ensures that a point $P \in \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ is affine (resp. at infinity) if and only if the projected point $\pi(P)$ is affine (resp. at infinity) in $\mathcal{E}_{A,B}(\mathbb{F}_p)$.

The affine part of an elliptic set $\mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ is entirely covered by the affine points of the elliptic curves $\{\mathcal{E}_{A+\alpha p,B+\beta p}(\mathbb{Z}/p^e\mathbb{Z})\}_{\alpha,\beta\in\{0,1,\ldots,p^{e-1}-1\}}$. To be more precise, the following lemma shows that it is a p^{e-1}-covering.

Lemma 3.1.5. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be the elliptic set and $P \in \mathcal{L}^a$ one of its affine points. For every integer $\alpha \in \{0, 1, \ldots, p^{e-1}-1\}$ there exists a unique integer $\beta \in \{0, 1, \ldots, p^{e-1}-1\}$ such that $P \in \mathcal{E}_{A+\alpha p,B+\beta p}(\mathbb{Z}/p^e\mathbb{Z})$.*

Proof. Since P is affine we may assume $P = (X : Y : 1)$. Given $\alpha \in \{0, 1, \ldots, p^{e-1} - 1\}$ we define the polynomial

$$F(\omega) = X^3 + (A + \alpha p)X + (B + \omega) - Y^2 \in \mathbb{Z}[\omega],$$

which satisfies $F(0) \equiv 0 \bmod p$ and $F'(0) = 1 \not\equiv 0 \bmod p$ by assumptions. Hence, by Hensel's Lemma there is a unique integer $0 \leq \beta' \leq p^e - 1$ such that $\beta' \equiv 0 \bmod p$ and $F(\beta') \equiv 0 \bmod p^e$, therefore $\beta = \frac{\beta'}{p}$ is the required element. □

Remark 3.1.6. On the infinity side, it is easy to verify that $\mathcal{L}^\infty$, as a set, does not depend on the given (A, B). In fact, it is equal to

$$\mathcal{L}^\infty = \{(\alpha p : 1 : \beta p)\}_{\alpha,\beta\in\{0,\ldots,p^{e-1}-1\}} \subseteq \mathbb{P}^2(\mathbb{Z}/p^e\mathbb{Z}).$$

Thus, $|\mathcal{L}^\infty| = p^{2(e-1)}$.

Unlike the affine case, not all points at infinity of $\mathcal{L}$ belong to some elliptic curve over the same base ring. In fact, given a pair $A, B \in \mathbb{Z}$ and $f_{(A,B)}$ as in Proposition 2.3.6, a point $(X : 1 : Z) \in \mathcal{L}$ belongs to $\mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ if and only if $Z = f_{(A,B)}(X)$. Therefore, the points of $\mathcal{L}^\infty$ that also belong to some elliptic curve are those of the form

$$\left\{\left(\alpha p : 1 : f_{(A,B)}(\alpha p)\right)\right\}_{\alpha \in \{0,1,\dots,p^{e-1}-1\}},$$

so in particular the family

$$\{(\alpha p^{\lceil \frac{e}{3} \rceil} : 1 : 0)\}_{\alpha \in \{0,1,\dots,p^{\lfloor \frac{2e}{3} \rfloor}-1\}}$$

belongs to every elliptic curve over $\mathbb{Z}/p^e\mathbb{Z}$, regardless of (A, B). On the contrary, a family of points that cannot belong to any elliptic curve over $\mathbb{Z}/p^e\mathbb{Z}$ is

$$\{(0 : 1 : \alpha p)\}_{\alpha \in \{1,\dots,p^{e-1}-1\}}.$$

3.2 THE OPERATION

For every pair of points $P_1, P_2 \in \mathbb{P}^2(\mathbb{Z}/p^e\mathbb{Z})$ the operation $+_{(0:1:0)}$ as defined in Section 1.2 determines a point $P_1 +_{(0:1:0)} P_2 \in \mathbb{P}^2(\mathbb{Z}/p^e\mathbb{Z})$ whenever $\pi(P_1) + \pi(P_2)$ has a non-zero second coordinate. From now on, will consider only this case.

Assumption 3.2.1 (Odd order)**.** Any elliptic set $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ is assumed to be *odd order*, namely for every $P = (X : Y : Z) \in \mathcal{L}$ we have $\mathrm{GCD}(Y, p) = 1$, i.e. $\pi(P)$ has odd order in $\mathcal{E}_{A,B}(\mathbb{F}_p)$.

Definition 3.2.2 (Elliptic loop)**.** Let $p \in \mathcal{P} \cap \mathbb{Z}_{\geq 5}$. An elliptic set $\mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ endowed with the operation $+_{(0:1:0)}$ and satisfying Assumption 3.2.1 is called *elliptic loop*.

Obviously, if the size of an elliptic curve is an odd prime, its correspondent loop is odd order.

Under the above assumption, the addition law $+_{(0:1:0)}$ has no exceptional points in $\mathcal{L}$, therefore we simply refer to it as $+$. So far we denoted *elliptic loop* a specific set, but in the next few pages we will prove that, with this $+$ operation, it is actually a loop in the standard algebraic notation.

We begin by proving that any elliptic loop endowed with this addition law is indeed a well-defined commutative magma with identity and inverses.

Proposition 3.2.3. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop. Then $(\mathcal{L}, +)$ is an abelian magma with identity $\mathcal{O} = (0 : 1 : 0)$. Moreover, every element $(X : Y : Z) \in \mathcal{L}$ has a unique inverse, namely*

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

Proof. The explicit addition law as defined in Section 1.2 is a polynomial combination of the entries of its addenda, hence it commutes with the standard reduction. Therefore for every $P_1, P_2 \in \mathcal{L}$ we have

$$\pi(P_1 + P_2) = \pi(P_1) + \pi(P_2) \in \mathcal{E}_{A,B}(\mathbb{F}_p),$$

which means that the coordinates of $\pi(P_1+P_2)$ satisfy the Weierstrass equation of $\mathcal{E}_{A,B}(\mathbb{F}_p)$, i.e. $P_1 + P_2$ is still a point of $\mathcal{L}$. Moreover, this operation is symmetric in the entries of the two addenda, hence it is commutative.

To check that $\mathcal{O}$ is the identity element, we verify that

$$(X : Y : Z) + (0 : 1 : 0) = (XY : Y^2 : YZ) = (X : Y : Z) \in \mathbb{P}^2(\mathbb{Z}/p^e\mathbb{Z}),$$

where the last equality follows from the odd order assumption. Another direct check shows that for every $P = (X : Y : Z)$ we have

$$P - P = (0 : -(A^3 + 9B^2)Z^4 - 6A^2X^2Z^2 - 6ABXZ^3 + 3AX^4 + 18BX^3Z + Y^4 : 0) = \mathcal{O},$$

which proves the existence of the inverse. As for the uniqueness, let us consider two points $P_1 = (X_1 : Y_1 : Z_1), P_2 = (X_2 : Y_2 : Z_2) \in \mathcal{L}$ satisfying

$$P_1 + P_2 = \big(S_1(X_i, Y_i, Z_i) : S_2(X_i, Y_i, Z_i) : S_3(X_i, Y_i, Z_i)\big) = \mathcal{O}.$$

Hence there exists $t \in (\mathbb{Z}/p^e\mathbb{Z})^*$ such that

$$\begin{cases} S_1(X_i, Y_i, Z_i) = S_3(X_i, Y_i, Z_i) = 0, \\ S_2(X_i, Y_i, Z_i) = t. \end{cases}$$

A direct check [Appendix B.1] shows that for every such pair P_1, P_2 we have

$$X_1Y_2 + X_2Y_1 = 0, \qquad Y_1Z_2 + Y_2Z_1 = 0.$$

Under the odd order assumption both Y_1 and Y_2 are invertible, hence the above relations imply that

$$(X_2 : Y_2 : Z_2) = \left(-\frac{Y_1}{Y_2}X_2 : -\frac{Y_1}{Y_2}Y_2 : -\frac{Y_1}{Y_2}Z_2\right) = (X_1 : -Y_1 : Z_1),$$

i.e. the unique inverse of P_1 is $(X_1 : -Y_1 : Z_1)$. □

3.3 ASSOCIATIVITY

3.3.1 Loop structure

If $\mathcal{L}$ were associative it would be a group, but this is almost never the case as we will see in Section 4.1. For the moment, we just present a small example to support this claim.

Example 3.3.1. Let $p = 5, A = 2$ and $B = 4$. The elliptic curve $\mathcal{E}_{2,4}(\mathbb{F}_5)$ has 7 points, therefore the elliptic loop $\mathcal{L}_{2,4}(\mathbb{Z}/25\mathbb{Z})$ has odd order. By considering $P = (12 : 11 : 1)$, $Q = (5 : 18 : 1)$ and $R = (15 : 8 : 1)$ we have

$$\begin{aligned} (P+Q)+R &= (5:17:1) \\ &\quad \nparallel \\ P+(Q+R) &= (15:22:1). \end{aligned}$$

Although these structures are rarely groups, a weak form of associativity holds.

Lemma 3.3.2. *Let $P, Q \in \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be any pair of points of an elliptic loop. Then*

$$P + (-P + Q) = Q.$$

Proof. We formally compute the polynomials S_1, S_2, S_3 in the coordinates of the points P and $Q = (Q_1 : Q_2 : Q_3)$, i.e.

$$(S_1 : S_2 : S_3) = P + (-P + Q).$$

A straightforward verification [Appendix B.2] shows that

$$S_1Q_2 - S_2Q_1 = 0, \qquad S_1Q_3 - S_3Q_1 = 0, \qquad S_2Q_3 - S_3Q_2 = 0,$$

which means $(S_1 : S_2 : S_3) = Q \in \mathbb{P}^2(\mathbb{Z}/p^e\mathbb{Z})$. □

We can now prove that the name *loop* is well-given.

Corollary 3.3.3. *Any elliptic loop $\mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ is an abelian algebraic loop.*

Proof. By Proposition 3.2.3 we know that $\mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ is an abelian magma with identity, therefore it is a loop as soon as it is a quasigroup. Hence, it is sufficient to show that for every $P, Q \in \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ the equation

$$P + R = Q$$

has a unique solution $R \in \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$. By Lemma 3.3.2 a solution is $R = Q - P$, and it is unique because if $R_2 \in \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ satisfies the same equation, then

$$R_2 = -P + (P + R_2) = -P + Q,$$

which implies $R = R_2$. □

Remark 3.3.4. We should mention that other weak associativity properties may be tested for commutative loops, most of them arising from non-associative algebras [62]. For instance, given $P, Q, R \in \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$, one may test

- alternativity; $$P + (P + Q) = (P + P) + Q$$
- Jordan identities; $$(P + P) + (P + Q) = P + \big(Q + (P + P)\big)$$
- Moufang identities (or Bol loop). $$\begin{cases} \big(P + (Q + R)\big) + R & = \big((P + R) + R\big) + Q \\ (P + R) + (Q + R) & = \big((P + Q) + R\big) + R \end{cases}$$

None of the above forms of associativity but the one of Lemma 3.3.2 hold (in general).

In absence of associativity, one defines the multiple of a given point P recursively: for every pair of non-negative integers $n, m \in \mathbb{Z}_{\geq 0}$, we set

$$0P = \mathcal{O}, \qquad (n + 1)P = nP + P, \qquad (-m)P = m(-P).$$

For finite loops a natural notion of order may be introduced. In fact, finiteness implies that there are different integers $n \neq m$ such that $nP = mP$, which in a loop implies $(n-m)P = \mathcal{O}$. Therefore, the following definition makes sense, i.e. the following minimum always exists.

Definition 3.3.5 ($\mathrm{ord}_{\mathcal{L}}$)**.** Let $\mathcal{L}$ be a finite loop and $P \in \mathcal{L}$. We define the *order* of P as

$$\mathrm{ord}_{\mathcal{L}}(P) = \min_{i \in \mathbb{Z}_{\geq 1}} \{iP = \mathcal{O}\}.$$

Thus, for every $P \in \mathcal{L}$ it is easy to see that $\mathrm{ord}_{\mathcal{L}}(P)$ divides every integer $i \in \mathbb{Z}$ such that $iP = \mathcal{O}$, so that for every $n, m \in \mathbb{Z}_{\geq 0}$ we have

$$nP = mP \implies n \equiv m \bmod \mathrm{ord}_{\mathcal{L}}(P).$$

3.3.2 Power associativity

A stronger and relevant associativity condition that may be investigated is the possibility of arbitrarily associating multiples of a given point.

Definition 3.3.6 (Power associativity)**.** A magma $(\mathcal{M}, +)$ is called *power associative* if the submagma generated by any element is associative.

Power associativity means that for any $P \in \mathcal{M}$ and for every pair of positive integers $n, m \in \mathbb{Z}_{\geq 0}$ we have

$$\begin{aligned}(n+m)P &= \underbrace{P + \Big(P + \ldots + \big(P + (P+P)\big)\ldots\Big)}_{(n+m)\ \text{times}} \\ &= \left(\underbrace{P + \big(\ldots + (P+P)\ldots\big)}_{n\ \text{times}}\right) + \left(\underbrace{P + \big(\ldots + (P+P)\ldots\big)}_{m\ \text{times}}\right) = nP + mP,\end{aligned}$$

which implies that multiples of P do not depend on the order we evaluate them.

We are going to show that elliptic loops are, indeed, power associative. However, this proof requires a deeper understanding of their associativity structure, which is detailed by the following theorem.

Theorem 3.3.7. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop. Let also*

$$\begin{aligned}F(x,y,z) &= x^3 + Axz^2 + Bz^3 - y^2z \in \mathbb{Z}[x,y,z], \\ \mathbb{F}(x,y,z) &= A^2z^3 - 3Ax^2z - 9Bxz^2 - 3xy^2 \in \mathbb{Z}[x,y,z],\end{aligned}$$

and for a triple $P_1, P_2, P_3 \in \mathcal{L}$, define the matrix

$$\mathbb{M} = \begin{bmatrix} F(P_1) & F(P_2) & F(P_3) \\ \mathbb{F}(P_1) & \mathbb{F}(P_2) & \mathbb{F}(P_3) \end{bmatrix}.$$

Then, the following hold.

(i) Whenever $\operatorname{rk} \mathbb{M} \leq 1$ *the triple is associative, that is $P_1 + (P_2 + P_3) = (P_1 + P_2) + P_3$.*

(ii) We have

$$\operatorname{rk} \begin{bmatrix} F(P_1) & F(P_2 + P_3) \\ \mathbb{F}(P_1) & \mathbb{F}(P_2 + P_3) \end{bmatrix} \leq \operatorname{rk} \begin{bmatrix} F(P_1) & F(P_2) & F(P_3) \\ \mathbb{F}(P_1) & \mathbb{F}(P_2) & \mathbb{F}(P_3) \end{bmatrix}.$$

Proof. For part (i) we formally compute the values $h_1, h_2, h_3, l_1, l_2, l_3 \in \mathbb{Z}/p^e\mathbb{Z}$ as functions of the entries of $P_i = (X_i : Y_i : Z_i)$ such that

$$\begin{aligned} (h_1 : h_2 : h_3) &= P_1 + (P_2 + P_3), \\ (l_1 : l_2 : l_3) &= (P_1 + P_2) + P_3. \end{aligned}$$

The above entities represent the same point in $\mathbb{P}^2(\mathbb{Z}/p^e\mathbb{Z})$ if all the following

$$c_1 = h_1 l_2 - h_2 l_1, \qquad c_2 = h_2 l_3 - h_3 l_2, \qquad c_3 = h_3 l_1 - h_1 l_3$$

vanish. A direct check [Appendix B.3] shows that all the c_j's belong to the ideal $I_2(\mathbb{M})$ generated by the 2×2-minors of $\mathbb{M}$. Thus, when the strong rank of $\mathbb{M}$ is strictly lower than 2 we have $I_2(\mathbb{M}) = (0)$ so that for every $i, j \in \{1, 2, 3\}$ we have $c_j(X_i, Y_i, Z_i) = 0$, i.e. the P_i's associate.

As for part (ii), we verify [Appendix B.3] that for both $i = 1, 2$ we have the ideal containment

$$I_i \left(\begin{bmatrix} F(P_1) & F(P_2 + P_3) \\ \mathbb{F}(P_1) & \mathbb{F}(P_2 + P_3) \end{bmatrix} \right) \subseteq I_i \left(\begin{bmatrix} F(P_1) & F(P_2) & F(P_3) \\ \mathbb{F}(P_1) & \mathbb{F}(P_2) & \mathbb{F}(P_3) \end{bmatrix} \right),$$

from which the strong rank inequality follows immediately. □

Theorem 3.3.7 provides a sufficient condition for associativity, but it is far from being necessary. In fact, by commutativity, for every $P, Q \in \mathcal{L}$ we have

$$P + (Q + P) = (P + Q) + P,$$

but, experimentally, the strong rank

$$\operatorname{rk} \begin{bmatrix} F(P) & F(Q) & F(P) \\ \mathbb{F}(P) & \mathbb{F}(Q) & \mathbb{F}(P) \end{bmatrix} = \operatorname{rk} \begin{bmatrix} F(P) & F(Q) \\ \mathbb{F}(P) & \mathbb{F}(Q) \end{bmatrix}$$

is often equal to 2 when P, Q are randomly chosen points of $\mathcal{L}$.

However, this condition is sufficient to prove that any elliptic loop is indeed power associative.

Corollary 3.3.8. *Any elliptic loop $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ is power associative.*

Proof. By part (i) of Theorem 3.3.7 it is sufficient to show that for every triple of integers $\alpha, \beta, \gamma \in \mathbb{Z}$ we have

$$\operatorname{rk}\begin{bmatrix} F(\alpha P) & F(\beta P) & F(\gamma P) \\ \mathbb{F}(\alpha P) & \mathbb{F}(\beta P) & \mathbb{F}(\gamma P) \end{bmatrix} \leq 1.$$

We prove that all the 2×2-minors of the above matrix vanish, namely we prove that for any $P \in \mathcal{L}$ and every $n, m \in \mathbb{Z}$ we have

$$\operatorname{rk}\begin{bmatrix} F(mP) & F(nP) \\ \mathbb{F}(mP) & \mathbb{F}(nP) \end{bmatrix} \leq 1. \tag{3.1}$$

Since $F(P) = F(-P)$ and $\mathbb{F}(P) = \mathbb{F}(-P)$, we may assume $n \geq m \geq 1$. We notice that when $m = n$ it is trivial, since

$$\operatorname{rk}\begin{bmatrix} F(nP) & F(nP) \\ \mathbb{F}(nP) & \mathbb{F}(nP) \end{bmatrix} \leq 1.$$

We prove by extended induction on $n \in \mathbb{Z}_{\geq 1}$ that for every positive $m \leq n$ the rank inequality (3.1) holds.

$[n = 1]$ The unique possibility is $n = m = 1$, discussed above.

$[\{1, \dots, n-1\} \to n]$ If $m = n$ it holds as above, so we may assume $n > m \geq 1$. By applying part (ii) of Theorem 3.3.7 we have

$$\operatorname{rk}\begin{bmatrix} F(mP) & F(nP) \\ \mathbb{F}(mP) & \mathbb{F}(nP) \end{bmatrix} \leq \operatorname{rk}\begin{bmatrix} F(mP) & F\big((n-1)P\big) & F(P) \\ \mathbb{F}(mP) & \mathbb{F}\big((n-1)P\big) & \mathbb{F}(P) \end{bmatrix}.$$

By inductive hypothesis we have

$$\operatorname{rk}\begin{bmatrix} F(mP) & F\big((n-1)P\big) \\ \mathbb{F}(mP) & \mathbb{F}\big((n-1)P\big) \end{bmatrix} \leq 1, \operatorname{rk}\begin{bmatrix} F(mP) & F(P) \\ \mathbb{F}(mP) & \mathbb{F}(P) \end{bmatrix} \leq 1, \operatorname{rk}\begin{bmatrix} F\big((n-1)P\big) & F(P) \\ \mathbb{F}\big((n-1)P\big) & \mathbb{F}(P) \end{bmatrix} \leq 1.$$

Thus, we obtain

$$\operatorname{rk}\begin{bmatrix} F(mP) & F\big((n-1)P\big) & F(P) \\ \mathbb{F}(mP) & \mathbb{F}\big((n-1)P\big) & \mathbb{F}(P) \end{bmatrix} \leq 1,$$

which concludes the inductive step. □

As a consequence of Corollary 3.3.8, every point of an elliptic loop is contained in a subloop that is also a group, e.g. the one it generates.

3.3.3 Shadow Curve

In this section, the odd order Assumption 3.2.1 is not needed.

Theorem 3.3.7 sheds light on the special polynomial $\mathbb{F}$, which stands behind the Weierstrass polynomial F defining the elliptic curve. Here we investigate some of its properties.

Definition 3.3.9. (Shadow polynomial) Let $F(x,y,z) = x^3 + Axz^2 + Bz^3 - y^2z \in \mathbb{Z}[x,y,z]$ be a Weierstrass polynomial. We define its *shadow polynomial* as

$$\mathbb{F}(x,y,z) = A^2z^3 - 3Ax^2z - 9Bxz^2 - 3xy^2 \in \mathbb{Z}[x,y,z].$$

The projective cubic $\mathcal{V}(\mathbb{F})$ defined by $\mathbb{F}$ over the same base ring of $\mathcal{V}(F)$ is referred to as the *shadow curve.*

As any shadow worthy of its name, the shadow curve usually intersects the original curve precisely in one point, namely the one at infinity.

Proposition 3.3.10. *Let $\mathcal{E} = \mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) = \mathcal{V}(F)$ be the elliptic curve defined by the Weierstrass polynomial F and let $P \in \mathcal{E}$ be a point of order not dividing* 3. *Then*

$$\gcd\big(\mathbb{F}(P), p\big) = 1.$$

In particular, if $\mathcal{E}$ has no 3-torsion points, then

$$\mathcal{V}(F) \cap \mathcal{V}(\mathbb{F}) = \{\mathcal{O}\}.$$

Proof. A direct computation [Appendix B.4] shows that, regardless of the addition formula used, by formally computing S_1, S_2, S_3 such that

$$(S_1 : S_2 : S_3) = 3P,$$

we have

$$S_1 \in \langle F, \mathbb{F} \rangle \subset \mathbb{Z}[x, y, z] \quad \text{and} \quad S_3 \in \langle F, \mathbb{F} \rangle \subset \mathbb{Z}[x, y, z].$$

Therefore, if a point $P \in \mathbb{P}^2(\mathbb{Z}/p^e\mathbb{Z})$ annihilates both F and $\mathbb{F}$, then $3P = \mathcal{O}$. If also $P \neq \mathcal{O}$, this implies that $\operatorname{ord}(P) = 3$.

Clearly $F(\mathcal{O}) = \mathbb{F}(\mathcal{O}) = 0$, so if $\mathcal{E}$ has no 3-torsion points, $\mathcal{O}$ is the unique point in the supports of both F and $\mathbb{F}$. □

A surprising property of these objects is that the addition law respects any linear combination of a polynomial and its shadow polynomial.

Proposition 3.3.11. *Let $\mathcal{E} = \mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) = \mathcal{V}(F)$ be the elliptic curve defined by the Weierstrass polynomial F and let $\alpha, \beta \in \mathbb{Z}$. For every pair of points $P_1, P_2 \in \mathbb{P}^2(\mathbb{Z}/p^e\mathbb{Z})$, if*

$$(\alpha F + \beta \mathbb{F})(P_1) = 0 \quad \text{and} \quad (\alpha F + \beta \mathbb{F})(P_2) = 0,$$

then, with the notation of Section 1.2, we have

$$(\alpha F + \beta \mathbb{F})(P_1 +_{(0:0:1)} P_2) = (\alpha F + \beta \mathbb{F})(P_1 +_{(0:1:0)} P_2) = 0.$$

Moreover, if $\gcd(\alpha, p) = 1$ then $+_{(0:0:1)}$ and $+_{(0:1:0)}$ are both associative and they agree on the points of $\mathcal{V}(\alpha F + \beta \mathbb{F})$.

Proof. A direct computation [Appendix B.4] shows that

$$\langle(\alpha F+\beta\mathbb{F})(P_1+_{(0:0:1)}P_2),(\alpha F+\beta\mathbb{F})(P_1+_{(0:1:0)}P_2)\rangle\subseteq\langle(\alpha F+\beta\mathbb{F})(P_1),(\alpha F+\beta\mathbb{F})(P_2)\rangle,$$

as ideals in $\mathbb{Z}/p^e\mathbb{Z}$. Thus, both $(\alpha F+\beta\mathbb{F})(P_1+_{(0:0:1)}P_2)$ and $(\alpha F+\beta\mathbb{F})(P_1+_{(0:1:0)}P_2)$ vanish if $(\alpha F+\beta\mathbb{F})(P_1)$ and $(\alpha F+\beta\mathbb{F})(P_2)$ do.

As for the "moreover" part, we straightforwardly [Appendix B.4] check that when α is invertible (i.e. we are allowed to use $\frac{1}{\alpha}$ during the computations) then both the addition laws are associative and they agree modulo $\langle(\alpha F+\beta\mathbb{F})(P_1),(\alpha F+\beta\mathbb{F})(P_2)\rangle$. □

Proposition 3.3.11 shows that $\big(\mathcal{V}(\alpha F+\beta\mathbb{F}),+\big)$ is a group whenever the operation makes sense, i.e. when it produces proper projective points. In the next section we see that it is always the case when these curves lie inside the elliptic loop defined by F.

3.3.4 Layers

By Theorem 3.3.7 the points $P\in\mathcal{L}$ with the same ratio $\frac{F(P)}{\mathbb{F}(P)}\in p(\mathbb{Z}/p\mathbb{Z})$, whenever this quotient is defined, are associative. By Proposition 3.3.11 we also know that if the sum operation for points in $\mathcal{V}(F+\beta\mathbb{F})$, then it endows this set with a group structure. The following definition exploits both these ideas for determining a new family of algebraic curves inside elliptic loops.

Definition 3.3.12 (Layer)**.** Let $p\in\mathcal{P}$ be a prime integer, $e\in\mathbb{Z}_{\geq 1}$ be a positive integer and $F\in\mathbb{Z}[x,y,z]$ be a Weierstrass polynomial. For every integer $i\in\mathbb{Z}$ we define the *i-th layer* as the plane projective curve

$$\mathbb{L}_i=\{P\in\mathbb{P}^2(\mathbb{Z}/p^e\mathbb{Z})\mid(F-ip\mathbb{F})(P)\equiv 0 \bmod p^e\}.$$

If F is the polynomial defining an elliptic loop $\mathcal{L}=\mathcal{V}(F)$, we say that $\mathbb{L}_i$ is a *layer of* $\mathcal{L}$.

Given an elliptic loop $\mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$, its zero-layer $\mathbb{L}_0=\mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ is a proper group. The following proposition shows that this is actually true for every layer.

Proposition 3.3.13. *Let $\mathcal{L}=\mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop and $i\in\mathbb{Z}$. If $\mathbb{L}_i$ is a layer of $\mathcal{L}$, then* *(i)* $\mathbb{L}_i$ *is a subloop of* $\mathcal{L}$*,*

(ii) $\mathbb{L}_i$ *is a group,*

(iii) the fibers of $\pi : \mathbb{L}_i \to \mathcal{E}_{A.B}(\mathbb{F}_p)$ *have constant size* p^{e-1}*.*

Proof. $(i - ii)$ The inclusion $\mathbb{L}_i \subseteq \mathcal{L}$ is clear, since a point $P \in \mathbb{P}^2(\mathbb{Z}/p^e\mathbb{Z})$ such that $(F - ip\mathbb{F})(P) \equiv 0 \bmod p^e$ also satisfies $F(P) \equiv 0 \bmod p$. By Proposition 3.3.11 layers are closed and associative, and the sum of two points P_1, P_2 is always defined because $\pi(P_1 + P_2)$ is a point of $\mathcal{E}_{A,B}(\mathbb{F}_p)$, thus $P_1 + P_2 \in \mathbb{P}^2(\mathbb{Z}/p^e\mathbb{Z})$. The unity of both $\mathbb{L}_i$ and $\mathcal{L}$ is $\mathcal{O}$, hence $\mathbb{L}_i$ is a subloop of $\mathcal{L}$ that is also a group itself.
(iii) Since for every $P \in \mathbb{P}^2(\mathbb{Z}/p^e\mathbb{Z})$ we have $F(P) - ip\mathbb{F}(P) \equiv F(P) \bmod p$, Hensel's Lemma applies as in Lemma 2.3.8, therefore for every $\overline{P} \in \mathcal{E}_{A.B}(\mathbb{F}_p)$ there are p^{e-1} points $P \in \mathbb{L}_i$ such that $\pi(P) = \overline{P}$. □

Proposition 3.3.13 shows that layers are large associative substructures inside elliptic loops. However, this condition is not exclusive: it may occasionally happen that a triple of points inside different layers associate, as shown by the following example.

Example 3.3.14. Let $p = 5, e = 2, A = 2$ and $B = 1$. We consider the following points inside $\mathcal{L} = \mathcal{L}_{2,1}(\mathbb{Z}/25\mathbb{Z})$:

$$P = (21 : 18 : 1), \qquad Q = (23 : 18 : 1), \qquad R = (16 : 18 : 1).$$

They associate, as

$$P + (Q + R) = (20 : 1 : 0) = (P + Q) + R.$$

Nonetheless, they belong to different layers of $\mathcal{L}$, in fact

$$P \in \mathbb{L}_3, \qquad Q \in \mathbb{L}_4, \qquad R \in \mathbb{L}_0.$$

As shown by the following proposition, in absence of 3-torsion points the affine parts of layers are a partition for the affine points of the correspondent elliptic loop.

Proposition 3.3.15. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop without points of order* 3 *and, for any of its layers $\mathbb{L}_i$, denote by $\mathbb{L}_i^a = \mathbb{L}_i \cap \mathcal{L}^a$ its affine part. Then $\mathcal{L}^a$ is given by the disjoint union*

$$\mathcal{L}^a = \bigsqcup_{0 \le i \le p^{e-1}-1} \mathbb{L}_i^a.$$

Proof. For any affine point $P \in \mathcal{L}^a$, by Proposition 3.3.10 we may define

$$n_P = \frac{F(P)}{p}\big(\mathbb{F}(P)\big)^{-1} \mod p^{e-1},$$

so that $P \in \mathbb{L}_{n_P}$. We also observe that

$$i \equiv j \bmod p^{e-1} \implies \mathbb{L}_i = \mathbb{L}_j,$$

so that

$$\mathcal{L}^a \subseteq \bigcup_{0 \le i \le p^{e-1}-1} \mathbb{L}_i^a.$$

Disjointness follows by counting: if we call $q = |\mathcal{E}_{A,B}(\mathbb{F}_p)|$, by part (iii) of Proposition 3.3.13 we find that

$$|\mathbb{L}_i^a| = p^{e-1}(q-1),$$

whereas $|\mathcal{L}| = p^{2(e-1)}q$ by Proposition 3.1.3 and $|\mathcal{L}^\infty| = p^{2(e-1)}$ by Remark 3.1.6. Thus, we have

$$|\mathcal{L}^a| = |\mathcal{L}| - |\mathcal{L}^\infty| = p^{2(e-1)}(q-1) = \sum_{i=0}^{p^{e-1}-1} |\mathbb{L}_i^a|,$$

therefore the $\mathbb{L}_i^a$'s cannot intersect. □

A different story occurs for the infinity part of layers, as they always intersect in a small group, even if particular pairs of layers are allowed to have a larger intersection, how it is exhibited by the following lemma.

Lemma 3.3.16. *Let $e \in \mathbb{Z}_{\geq 2}$ and $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop without points of order 3. Then for every $i, j \in \mathbb{Z}$ such that* $\gcd(i-j, p) = 1$ *we have*

$$\mathbb{L}_i \cap \mathbb{L}_j = \langle (p^{e-1} : 1 : 0) \rangle.$$

In particular, the intersection of the layers of $\mathcal{L}$ is

$$\bigcap_{i \in \mathbb{Z}} \mathbb{L}_i = \langle (p^{e-1} : 1 : 0) \rangle.$$

Proof. If $P \in \mathbb{L}_i \cap \mathbb{L}_j$ then by Proposition 3.3.15 it is a points at infinity, so we may write $P = (X : 1 : Z)$ with $p|X$ and $p|Z$. Moreover, it has to satisfy both the layers equations:

$$\begin{cases} F(P) \equiv ip\mathbb{F}(P) \bmod p^e, \\ F(P) \equiv jp\mathbb{F}(P) \bmod p^e, \end{cases} \implies \begin{cases} (i-j)F(P) \equiv 0 \bmod p^e, \\ (i-j)\mathbb{F}(P) \equiv 0 \bmod p^{e-1}. \end{cases}$$

Since $i - j \in (\mathbb{Z}/p^e\mathbb{Z})^*$ this implies

$$\begin{cases} Z \equiv X^3 + AXZ^2 + BZ^3 \bmod p^e, \\ 3X \equiv AZ^3 - 3AX^2Z - 9BXZ^2 \bmod p^{e-1}. \end{cases}$$

From the first equation we obtain $\mathrm{v}_p(Z) \geq \mathrm{v}_p(X)$. By means of the second equation, as $e \geq 2$, we conclude that $X \equiv 0 \bmod p^{e-1}$. Therefore, there exists $\alpha \in \mathbb{Z}$ such that $P = (\alpha p^{e-1} : 1 : 0)$, so $P \in \langle (p^{e-1} : 1 : 0) \rangle$. On the other side, all the points in $\langle (p^{e-1} : 1 : 0) \rangle$ clearly satisfy every layer equation, so $\mathbb{L}_i \cap \mathbb{L}_j = \langle (p^{e-1} : 1 : 0) \rangle$. □

Since layers intersect at infinity, they cannot fill the whole $\mathcal{L}^\infty$. In fact, we will see in the next section that there is a large group inside $\mathcal{L}^\infty$ that they never meet.

3.4 THE INFINITY LOOP

Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop. Its infinity part $\mathcal{L}^\infty$ is a subloop of $\mathcal{L}$, which is not a group in general, as shown by the following example.

Example 3.4.1. Let $p = 5, e = 6, A = 2$ and $B = 1$. In $\mathcal{L} = \mathcal{L}_{2,1}(\mathbb{Z}/15625\mathbb{Z})$ we compute

$$\big((5:1:0) + (5:1:0)\big) + (0:1:5) = (4510:1:7505),$$

while the other association order produces

$$(5:1:0) + \big((5:1:0) + (0:1:5)\big) = (7635:1:4380).$$

Thus, $\mathcal{L}^\infty$ cannot be a group. The choice $e = 6$ is not accidental, it is the smallest we might have considered to construct such an example, as we will see in Section 4.2.

Interestingly, $\mathcal{L}^\infty$ is a loop generated by two of its cyclic subgroups. The proof of this fact involves a technical result about points at infinity, which follows.

Proposition 3.4.2. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop, $\alpha, \beta \in \mathbb{Z}$ and $\epsilon \in \mathbb{Z}$ be an integer such that $1 \le \epsilon \le e-1$. For every $X_\alpha, X_\beta, Z_\alpha, Z_\beta \in p\mathbb{Z}$ the following hold.*

(i) *If $(X:1:Z) = (X_\alpha : 1 : Z_a) + (X_\beta : 1 : Z_\beta) \in \mathbb{P}^2(\mathbb{Z}/p^e\mathbb{Z})$, then*

$$(X_\alpha + \alpha p^\epsilon : 1 : Z_\alpha) + (X_\beta : 1 : Z_\beta + \beta p^\epsilon) = (X + \alpha p^\epsilon : 1 : Z + \beta p^\epsilon) \in \mathbb{P}^2(\mathbb{Z}/p^{\epsilon+2}\mathbb{Z}).$$

(ii) *Let $m = \min\{\mathrm{v}_p(X_\alpha), \mathrm{v}_p(Z_\alpha), \mathrm{v}_p(X_\beta), \mathrm{v}_p(Z_\beta)\}$. Then*

$$(X_\alpha : 1 : Z_\alpha) + (X_\beta : 1 : Z_\beta) = (X_\alpha + X_\beta : 1 : Z_\alpha + Z_\beta) \in \mathbb{P}^2(\mathbb{Z}/p^{3m}\mathbb{Z}).$$

(iii) *Let $X, Y \in p\mathbb{Z}$. Then*

$$\alpha(X:1:Z) = (\alpha X : 1 : \alpha Z) \in \mathbb{P}^2(\mathbb{Z}/p^{\mathrm{v}_p(\alpha)+2}\mathbb{Z}).$$

Proof. We explicit the operation between such points:

$$(S_1 : S_2 : S_3) = (X_1 : 1 : Z_1) + (X_2 : 1 : Z_2),$$

where

$$\begin{aligned}
S_1 &= X_1 + X_2 - AX_1^2Z_2 - 2AX_1X_2Z_1 - 2AX_1X_2Z_2 - 6BX_1Z_1Z_2 - 3BX_1Z_2^2 \\
&\quad - AX_2^2Z_1 - 3BX_2Z_1^2 - 6BX_2Z_1Z_2 + A^2Z_1^2Z_2 + A^2Z_1Z_2^2, \\
S_2 &= 1 + 3AX_1^2X_2^2 + 9BX_1^2X_2Z_2 - A^2X_1^2Z_2^2 + 9BX_1X_2^2Z_1 - 4A^2X_1X_2Z_1Z_2 \\
&\quad - 3ABX_1Z_1Z_2^2 - A^2X_2^2Z_1^2 - 3ABX_2Z_1^2Z_2 + (-A^3 - 9B^2)Z_1^2Z_2^2, \\
S_3 &= Z_1 + Z_2 + 3X_1^2X_2 + 3X_1X_2^2 + 2AX_1Z_1Z_2 + AX_1Z_2^2 + AX_2Z_1^2 + 2AX_2Z_1Z_2 \\
&\quad + 3BZ_1^2Z_2 + 3BZ_1Z_2^2.
\end{aligned}$$

(i): For every $i \in \{1, 2, 3\}$ let us define

$$\tilde{S}_i = S_i(X_\alpha, 1, Z_\alpha, X_\beta, 1, Z_\beta).$$

Since all the considered elements are divisible by p, the degree-3 terms of the above polynomials does not change by adding to their arguments a multiple of p^ϵ, i.e.

$$\begin{aligned}
S_1(X_\alpha + \alpha p^\epsilon, 1, Z_\alpha, X_\beta, 1, Z_\beta + \beta p^\epsilon) &\equiv \tilde{S}_1 + \alpha p^\epsilon \bmod p^{\epsilon+2}, \\
S_2(X_\alpha + \alpha p^\epsilon, 1, Z_\alpha, X_\beta, 1, Z_\beta + \beta p^\epsilon) &\equiv \tilde{S}_2 \bmod p^{\epsilon+2}, \\
S_3(X_\alpha + \alpha p^\epsilon, 1, Z_\alpha, X_\beta, 1, Z_\beta + \beta p^\epsilon) &\equiv \tilde{S}_3 + \beta p^\epsilon \bmod p^{\epsilon+2},
\end{aligned}$$

from which the statement follows by noting that $\tilde{S}_2 \equiv 1 \bmod p^2$ so that even its inverse modulo p^ϵ has the form $1 + kp^2$. Therefore

$$\begin{aligned}
(X_\alpha + \alpha p^\epsilon : 1 : Z_\alpha) + (X_\beta : 1 : Z_\beta + \beta p^\epsilon) &= (\tilde{S}_1 + \alpha p^\epsilon : \tilde{S}_2 : \tilde{S}_3 + \beta p^\epsilon) \\
= \left(\frac{\tilde{S}_1}{\tilde{S}_2} + \alpha p^\epsilon : 1 : \frac{\tilde{S}_3}{\tilde{S}_2} + \beta p^\epsilon \right) &= (X + \alpha p^\epsilon : 1 : Z + \beta p^\epsilon) \in \mathbb{P}^2(\mathbb{Z}/p^{\epsilon+2}\mathbb{Z}).
\end{aligned}$$

(ii): Since p^m divides $X_\alpha, Z_\alpha, X_\beta$ and Z_β, then p^{3m} divides all the degree-3 pieces of S_1, S_2

and S_3, from which we get

$$\begin{aligned}S_1(X_\alpha, 1, Z_\alpha, X_\beta, 1, Z_\beta) &\equiv X_\alpha + X_\beta \bmod p^{3m},\\ S_2(X_\alpha, 1, Z_\alpha, X_\beta, 1, Z_\beta) &\equiv 1 \bmod p^{3m},\\ S_3(X_\alpha, 1, Z_\alpha, X_\beta, 1, Z_\beta) &\equiv Z_\alpha + Z_\beta \bmod p^{3m}.\end{aligned}$$

(iii): First, we prove by induction on $\epsilon \in \mathbb{Z}_{\geq 0}$ that

$$p^\epsilon(X:1:Z) = (p^\epsilon X : 1 : p^\epsilon Z) \in \mathbb{P}^2(\mathbb{Z}/p^{\epsilon+2}\mathbb{Z}).$$

$[\epsilon = 0]$ There is nothing to prove.
$[\epsilon - 1 \to \epsilon]$ By power associativity (Corollary 3.3.8), for $\epsilon \geq 1$ we have

$$p^\epsilon(X:1:Z) = p\big(p^{\epsilon-1}(X:1:Z)\big) \in \mathbb{P}^2(\mathbb{Z}/p^{\epsilon+2}\mathbb{Z}),$$

while by inductive hypothesis there are integers $\alpha, \beta \in \mathbb{Z}$ such that

$$p^{\epsilon-1}(X:1:Z) = (p^{\epsilon-1}X + \alpha p^{\epsilon+1} : 1 : p^{\epsilon-1}Z + \beta p^{\epsilon+1}) \in \mathbb{P}^2(\mathbb{Z}/p^{\epsilon+2}\mathbb{Z}).$$

By part (i) we easily see that

$$\begin{aligned}2(p^{\epsilon-1}X + \alpha p^{\epsilon+1} : 1 : p^{\epsilon-1}Z + \beta p^{\epsilon+1}) &= (2p^{\epsilon-1}X + 2\alpha p^{\epsilon+1} : 1 : 2p^{\epsilon-1}Z + 2\beta p^{\epsilon+1}),\\ 3(p^{\epsilon-1}X + \alpha p^{\epsilon+1} : 1 : p^{\epsilon-1}Z + \beta p^{\epsilon+1}) &= (3p^{\epsilon-1}X + 3\alpha p^{\epsilon+1} : 1 : 3p^{\epsilon-1}Z + 3\beta p^{\epsilon+1}),\\ &\vdots\\ p(p^{\epsilon-1}X + \alpha p^{\epsilon+1} : 1 : p^{\epsilon-1}Z + \beta p^{\epsilon+1}) &= (p^\epsilon X : 1 : p^\epsilon Z) \in \mathbb{P}^2(\mathbb{Z}/p^{e+2}\mathbb{Z}),\end{aligned}$$

which concludes the induction step.

Since $m = \min\{\mathrm{v}_p(X), \mathrm{v}_p(Z)\} \geq 1$, then $3m \geq m+2$ so we apply part (ii) to prove that for every $\alpha' \in \mathbb{Z} \setminus p\mathbb{Z}$ we have

$$\alpha'(p^\epsilon X : 1 : p^\epsilon Z) + (p^\epsilon X : 1 : p^\epsilon Z) = (\alpha' p^\epsilon X : 1 : \alpha' p^\epsilon Z) \in \mathbb{P}^2(\mathbb{Z}/p^{\epsilon+2}\mathbb{Z}).$$

From power associativity and the above results, the main statement easily follows. In fact, by defining $\alpha' = \frac{\alpha}{p^{\mathrm{v}_p(\alpha)}}$, we have

$$\begin{aligned}\alpha(X:1:Z) = \alpha' p^{\mathrm{v}_p(\alpha)}(X:1:Z) &= \alpha'(p^{\mathrm{v}_p(\alpha)}X:1:p^{\mathrm{v}_p(\alpha)}Z),\\ &= (\alpha' p^{\mathrm{v}_p(\alpha)}X:1:\alpha' p^{\mathrm{v}_p(\alpha)}Z) \in \mathbb{P}^2(\mathbb{Z}/p^{\mathrm{v}_p(\alpha)+2}\mathbb{Z}),\end{aligned}$$

which concludes the proof. □

We may now prove the structure theorem of $\mathcal{L}^\infty$.

Theorem 3.4.3. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop. Then*

(i) $\langle (p:1:0)\rangle \cap \langle (0:1:p)\rangle = \{\mathcal{O}\}$.

(ii) $|\langle (p:1:0)\rangle| = |\langle (0:1:p)\rangle| = p^{e-1}$.

(iii) For every $P \in \mathcal{L}^\infty$ there are unique integers $\alpha, \beta \in \{0, 1, \dots, p^{e-1}-1\}$ such that

$$P = \alpha(p:1:0) + \beta(0:1:p).$$

Proof. By Part (iii) of Proposition 3.4.2 every $(X:1:Z) \in \langle (p:1:0)\rangle$ satisfies

$$Z \equiv 0 \bmod p^{\mathrm{v}_p(X)+1},$$

while for every $(X:1:Z) \in \langle (0:1:p)\rangle$ we have

$$X \equiv 0 \bmod p^{\mathrm{v}_p(Z)+1}.$$

The unique point that may satisfy them together is $\mathcal{O}$, which proves (i).

The same proposition also shows that $\alpha(p:1:0) = (X_\alpha : Y_\alpha : Z_\alpha)$ is equal to $\mathcal{O}$ in $\mathbb{P}^2(\mathbb{Z}/p^e\mathbb{Z})$ if and only if $p^{e-1}|\alpha$, so we conclude that $\mathrm{ord}_{\mathcal{L}}\big((p:1:0)\big) = p^{e-1}$. In the same way we prove that also $\mathrm{ord}_{\mathcal{L}}\big((0:1:p)\big) = p^{e-1}$, which is (ii).

Since $|\mathcal{L}^\infty| = p^{2(e-1)}$, to prove (iii) it is sufficient to demonstrate that for every $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{Z}$ we have

$$\alpha_1(p:1:0) + \beta_1(0:1:p) = \alpha_2(p:1:0) + \beta_2(0:1:p) \implies \begin{cases} \alpha_1 \equiv \alpha_2 \bmod p^{e-1}, \\ \beta_1 \equiv \beta_2 \bmod p^{e-1}. \end{cases}$$

We prove by induction on $1 \leq \epsilon \leq e-1$ that, if the above equation holds, then we have both $\alpha_1 \equiv \alpha_2 \bmod p^\epsilon$ and $\beta_1 \equiv \beta_2 \bmod p^\epsilon$.

[$\epsilon = 1$] By considering the entries of the above points modulo p^2 we have

$$\begin{cases} \alpha_1(p:1:0) + \beta_1(0:1:p) = (\alpha_1 p:1:0) + (0:1:\beta_1 p) = (\alpha_1 p:1:\beta_1 p) \in \mathbb{P}^2(\mathbb{Z}/p^2\mathbb{Z}), \\ \alpha_2(p:1:0) + \beta_2(0:1:p) = (\alpha_2 p:1:0) + (0:1:\beta_2 p) = (\alpha_2 p:1:\beta_2 p) \in \mathbb{P}^2(\mathbb{Z}/p^2\mathbb{Z}), \end{cases}$$

so if the above quantities are equal then $\alpha_1 \equiv \alpha_2 \bmod p$ and $\beta_1 \equiv \beta_2 \bmod p$.

[$\epsilon - 1 \to \epsilon$] By inductive hypothesis there are integers $\alpha, \beta \in \mathbb{Z}$ such that $\alpha_2 = \alpha_1 + \alpha p^{\epsilon-1}$ and $\beta_2 = \beta_1 + \beta p^{\epsilon-1}$. By Corollary 3.3.8 we have that $\mathcal{L}$ is power associative, so is $\mathcal{L}^\infty$. Thus, we can write

$$\begin{aligned} \alpha_2(p:1:0) + \beta_2(0:1:p) &= (\alpha_1 + \alpha p^{\epsilon-1})(p:1:0) + (\beta_1 + \beta p^{\epsilon-1})(0:1:p) \\ &= \big(\alpha_1(p:1:0) + \alpha p^{\epsilon-1}(p:1:0)\big) + \big(\beta_1(0:1:p) + \beta p^{\epsilon-1}(0:1:p)\big) \in \mathbb{P}^2(\mathbb{Z}/p^{\epsilon+1}\mathbb{Z}). \end{aligned}$$

We then apply part (iii) of Proposition 3.4.2 to write the above quantity as

$$\big(\alpha_1(p:1:0) + (\alpha p^\epsilon:1:0)\big) + \big(\beta_1(0:1:p) + (0:1:\beta p^\epsilon)\big) \in \mathbb{P}^2(\mathbb{Z}/p^{\epsilon+1}\mathbb{Z}). \tag{3.2}$$

By applying part (i) of the same proposition, if we call $(X_\alpha : 1 : Z_\alpha) = \alpha_1(p:1:0)$ and $(X_\beta : 1 : Z_\beta) = \beta_1(0:1:p)$, then

$$\begin{cases} (X_\alpha : 1 : Z_\alpha) + (\alpha p^\epsilon : 1 : 0) = (X_\alpha + \alpha p^\epsilon : 1 : Z_\alpha), \\ (X_\beta : 1 : Z_\beta) + (0:1:\beta p^\epsilon) = (X_\beta : 1 : Z_\beta + \beta p^\epsilon). \end{cases}$$

Moreover, if we define

$$(X : 1 : Z) = (X_\alpha : 1 : Z_\alpha) + (X_\beta : 1 : Z_\beta),$$

then, by applying again part (i) of Proposition 3.4.2, we have

$$(X_\alpha + \alpha p^\epsilon : 1 : Z_\alpha) + (X_\beta : 1 : Z_\beta + \beta p^\epsilon) = (X + \alpha p^\epsilon : 1 : Z + \beta p^\epsilon).$$

Therefore, Equation (3.2) becomes

$$\alpha_2(p : 1 : 0) + \beta_2(0 : 1 : p) = (X + \alpha p^\epsilon : 1 : Z + \beta p^\epsilon),$$

and since by hypothesis this is equal to $(X : 1 : Z)$, we conclude that $\alpha \equiv \beta \equiv 0 \bmod p$, which proves that $\alpha_1 \equiv \alpha_2 \bmod p^\epsilon$ and $\beta_1 \equiv \beta_2 \bmod p^\epsilon$. □

Theorem 3.4.3 shows that, as a set, $\mathcal{L}^\infty$ may be thought as the direct product of its subloops

$$\mathcal{L}^\infty \simeq \langle (p : 1 : 0) \rangle \times \langle (0 : 1 : p) \rangle,$$

but the addition of $\mathcal{L}^\infty$ is not the product-operation of these subloops.

The next lemma shows that layers can never intersect the right-hand piece of this decomposition.

Lemma 3.4.4. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop. For every layer $\mathbb{L}$ of $\mathcal{L}$ we have*

$$\mathbb{L} \cap \langle (0 : 1 : p) \rangle = \{\mathcal{O}\}.$$

Proof. By part (iii) of Proposition 3.4.2, if

$$P = (X : Y : Z) \in \langle (0 : 1 : p) \rangle,$$

then $\mathrm{v}_p(Z) \leq \mathrm{v}_p(X)$. However, for such points we have

$$\mathrm{v}_p\big(F(P)\big) = \mathrm{v}_p(Z), \qquad \mathrm{v}_p\big(\mathbb{F}(P)\big) \geq \min\{3\mathrm{v}_p(Z), \mathrm{v}_p(X)\} \geq \mathrm{v}_p(Z).$$

If P satisfies satisfies a layer equation, then there is an integer $i \in \mathbb{Z}$ such that

$$e = \mathrm{v}_p(0) = \mathrm{v}_p\big(F(P) - ip\mathbb{F}(P)\big) = \mathrm{v}_p(Z),$$

which implies $Z \equiv X \equiv 0 \bmod p^e$, i.e. $P = \mathcal{O}$. □

3.5 THE GROUP STRUCTURE OF LAYERS

From Chapter 2 we know the group structure of $\mathbb{L}_0 = \mathcal{E}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$. The following result generalizes Theorem 2.3.9 by showing that all the layers of $\mathcal{L}$ have in fact the same structure when the underlying curve is not anomalous.

Theorem 3.5.1. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop. For every $i \in \mathbb{Z}$ and layer $\mathbb{L}_i$ of $\mathcal{L}$, there is a unique $Z_i \in p(\mathbb{Z}/p^e\mathbb{Z})$ such that the following*

$$0 \to \langle (p : 1 : Z_i) \rangle \xrightarrow{\mathrm{id}} \mathbb{L}_i \xrightarrow{\pi} \mathcal{E}_{A,B}(\mathbb{F}_p) \to 0,$$

is a short exact sequence of groups. Moreover, if $\gcd(|\mathcal{E}_{A,B}(\mathbb{F}_p)|, p) = 1$ *then*

$$\mathbb{L}_i \simeq \mathbb{Z}/p^{e-1}\mathbb{Z} \oplus \mathcal{E}_{A,B}(\mathbb{F}_p).$$

Proof. We consider the polynomial

$$(F - ip\mathbb{F})(p, 1, z) \in \mathbb{Z}[z].$$

We have $(F - ip\mathbb{F})(p, 1, 0) \equiv 0 \bmod p$ and its derivative in $z = 0$ is $F'(0) \equiv -1 \not\equiv 0 \bmod p$, hence by Hensel's Lemma there exists a unique $Z_i \in \mathbb{Z}/p^e\mathbb{Z}$ such that

$$\begin{cases} Z_i \equiv 0 \bmod p, \\ (p : 1 : Z_i) \in \mathbb{L}_i. \end{cases}$$

By part (iii) of Proposition 3.3.13 we have $|\pi^{-1}(\mathcal{O})| = p^{e-1}$, hence it is sufficient to show that $\mathrm{ord}_{\mathcal{L}}\big((p : 1 : Z_i)\big) = p^{e-1}$. By part (iii) of Proposition 3.4.2 we have

$$\alpha(p : 1 : Z_i) = (\alpha p : 1 : \alpha Z_i) \in \mathbb{P}^2(\mathbb{Z}/p^{\mathrm{v}_p(\alpha)+2}\mathbb{Z}),$$

hence the minimal $\alpha \in \mathbb{Z}_{\geq 1}$ for which $\alpha(p : 1 : Z_i) = \mathcal{O} \in \mathbb{P}^2(\mathbb{Z}/p^e\mathbb{Z})$ is $\alpha = p^{e-1}$.

As for the "moreover" part, we observe that if $\gcd(|\mathcal{E}_{A,B}(\mathbb{F}_p)|, p) = 1$, then we may find $k \in \mathbb{Z}$ such that

$$\begin{cases} k \equiv 1 \bmod p^{e-1}, \\ k \equiv 0 \bmod |\mathcal{E}_{A,B}(\mathbb{F}_p)|. \end{cases}$$

Thus, the multiplication-by-k map

$$\mathbb{L}_i \xrightarrow{\cdot k} \langle (p : 1 : Z_i) \rangle$$

is a left section of the above short exact sequence, so that Splitting Theorem applies. □

3.5.1 Anomalous elliptic loops

In this section we discuss elliptic loops lying over anomalous curves. To define them, we use their size by means of Proposition 3.1.3.

Definition 3.5.2 (Anomalous loop)**.** Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop. We say that $\mathcal{L}$ is an *anomalous loop* if $|\mathcal{L}| = p^{2e-1}$.

As in the corresponding situation for elliptic curves (Section 2.3.4), two possible group structures may occur for layers of anomalous loops.

Definition 3.5.3 (Cyclic/Split)**.** Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an anomalous loop. A layer $\mathbb{L}$ of $\mathcal{L}$ is called *cyclic* if there is a group isomorphism $\mathbb{L} \simeq \mathbb{Z}/p^e\mathbb{Z}$, it is called *split* if there is a group isomorphism $\mathbb{L} \simeq \mathbb{Z}/p^{e-1}\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$.

We know by Theorem 3.5.1 that any layer of an anomalous loop is either cyclic or split. It seems that both cases appear in a highly regular manner.

Conjecture 3.5.4. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an anomalous loop. There exists an integer $m \in \mathbb{Z}$ such that for every layer $\mathbb{L}_i$ of $\mathcal{L}$, if $i \not\equiv m \bmod p$ then $\mathbb{L}_i$ is cyclic, whereas if $i \equiv m \bmod p$ then $\mathbb{L}_i$ is split.*
In particular, every anomalous loop has precisely $\mathrm{p}^{\mathrm{e}-2}$ split layers.

If the above conjecture holds, a strong link between the canonical lifts of an elliptic curve [18, 46] and the split layers of the correspondent elliptic loop seems to be prompted. However, we shall mention that no explicit relation between these objects is known.

The motivation behind such a conjecture is twofold: on the practical side, no counterexamples have been discovered in small case testing, of which an instance is given by Example 3.5.5. On the other side, there are some theoretical arguments supporting this behaviour, such as the frequency of split cases in the group structure of anomalous elliptic curves. Moreover, in the next chapter we provide a partial proof of this conjecture (Proposition 4.5.5), which appears to have good chances to be extended to the general case.

Example 3.5.5. Let $p = 7, e = 4, A = 3, B = 5$ and $\mathcal{L} = \mathcal{L}_{0,3}(\mathbb{Z}/2401\mathbb{Z})$. It may be directly verified that $|\mathcal{L}| = 823543 = 7^{2\cdot 4-1}$, therefore it is anomalous, and among the 343 layers of $\mathcal{L}$ only 49 of them, namely those of the form

$$\mathbb{L}_i, \qquad \forall i \in \{2 + 7k\}_{k\in\{1,\ldots,p^{e-2}\}},$$

are isomorphic to $\mathbb{Z}/p^{e-1} \oplus \mathbb{Z}/p\mathbb{Z}$, hence split. The remaining layers are isomorphic to $\mathbb{Z}/p^e\mathbb{Z}$, therefore cyclic, as prescribed by Conjecture 3.5.4 for $m = 2$.

3.5.2 Subgroups description

Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop whose projected curve $\mathcal{E} = \mathcal{E}_{A,B}(\mathbb{F}_p)$ has size $|\mathcal{E}| = q$. In the previous sections we have determined many large subgroups lying inside $\mathcal{L}$, such as its layers, whose size is $p^{e-1}q$, and the group at infinity, which has $p^{2(e-1)}$ elements.

As for the maximal subgroups investigation, we suspect is that this list is exhaustive.

Conjecture 3.5.6. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop without points of order 3 and $G \subseteq \mathcal{L}$ be a subloop that is a group. Then one of the following conditions hold.*

- *There is a layer $\mathbb{L}$ of $\mathcal{L}$ such that $G \subseteq \mathbb{L}$.*
- *$G \subseteq \mathcal{L}^\infty$.*

Moreover, if G is cyclic, then it is contained in a layer or there are $\alpha, \beta \in \mathbb{Z}$ with $p \nmid \beta$ such that $G \subseteq \langle(\alpha p : 1 : \beta p)\rangle$.

This conjecture simultaneously reflects two ideas: the (presumed) impossibility of finding subgroups that are “transverse” to layers and the (supposed) possibility of generating every point at infinity as a multiple of a point with p-adic valuation 1 in some of its entries.

Even in this case, there are several reasons standing behind this claim. The idea that layers shall be the maximal associativity structures is supported by practical considerations arisen from the proof of Theorem 3.3.7, which provides a sufficient condition for associativity. Although this may not be necessary, the association between different layers, appears to be, de facto, occasional: we find that such “lucky” associations (Example 3.3.14) may hardly hold simultaneously for all the points lying inside two (or more) layers. Another argument in favour of such a conjecture will be given in the next chapter by Corollary 4.5.7, where layers are proved to be maximal with respect to inclusion if $e = 2$.

The following lemma provides a partial motivation to the formulation of the final part of Conjecture 3.5.6, by showing that the case $p|\beta$ shall not lead to maximal groups.

Lemma 3.5.7. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop without points of order 3 and $P = (X : 1 : Z) \in \mathcal{L}^\infty$ a point at infinity. If $p^2|Z$, then either $p^2|X$ or there exists a layer $\mathbb{L}$ of $\mathcal{L}$ such that $P \in \mathbb{L}$.*

Proof. Let $F \in \mathbb{Z}[x, y, z]$ be the Weierstrass polynomial defining $\mathcal{L}$. If $p^2 | Z$ and $p^2 \nmid X$, then we write $P = (\alpha p : 1 : \beta p^2)$ with $\gcd(\alpha, p) = 1$, and for every integer $i \in \mathbb{Z}$ we have

$$
\begin{aligned}
(F - ip\mathbb{F})\big((X : 1 : Z)\big) &\equiv X^3 + AXZ^2 + BZ^3 - Z - ip(A^2Z^3 - 3AX^2Z - 9BXZ^2 - 3X) \\
&\equiv p^2\big((p\alpha^3 + p^3A\alpha\beta^2 + p^4B\beta^3 - ip^5A^2\beta^3 + ip^3 3A\alpha^2\beta + 9ip^4B\alpha\beta^2) + (3i\alpha - \beta)\big) \bmod p^e.
\end{aligned}
$$

If $e \leq 2$ then $P \in \langle (p : 1 : 0) \rangle$ and the statement follows from Lemma 3.3.16. Let us assume $e \geq 3$ and define the polynomial $G \in \mathbb{Z}[i]$ as

$$
G(i) = (p\alpha^3 + p^3A\alpha\beta^2 + p^4B\beta^3 - ip^5A^2\beta^3 + ip^3 3A\alpha^2\beta + 9ip^4B\alpha\beta^2) + (3i\alpha - \beta).
$$

It is easy to see that $\iota = \frac{\beta}{3\alpha}$ satisfies $G(\iota) \equiv 0 \bmod p$, as well as $G' \equiv 3\alpha \neq 0 \bmod p$, therefore by Hensel's Lemma there is a unique lift $0 \leq i \leq p^{e-2} - 1$ of ι that annihilates G modulo p^{e-2}. Therefore, we conclude that the given P lies inside the p layers $\mathbb{L}_m$ of $\mathcal{L}$ such that $0 \leq m \leq p^{e-1} - 1$ and $m \equiv i \bmod p^{e-2}$. □

We recall that 3-torsion points are often pathological for layers, as in these points layers may exceptionally intersect. In fact, the following example shows that their absence is essential for Conjecture 3.5.6.

Example 3.5.8. Let $p = 11, e = 2, A = 1, B = 7$ and let $\mathcal{L} = \mathcal{L}_{1,7}(\mathbb{Z}/121\mathbb{Z})$. We define

$$
G = \pi^{-1}\big(\{\mathcal{O}, (4 : 3 : 1), (4, 8, 1)\}\big),
$$

as the set of points lying over the rational 3-torsion points of $\mathcal{E}_{1,7}(\mathbb{F}_{11})$. Since π respects the point addition, this set is patently a closed subloop of $\mathcal{L}$. A direct check shows that every triple in G associates, hence G is a group.

However, $|G| = 363$, while layers have size 165 and the size of $\mathcal{L}^\infty$ is 121, so that G may not be contained inside any of them.

Remark 3.5.9. For some reasons that will be treated in the next chapter (Lemma 4.1.1) one might argue that for $e \geq 3$ the assumption on 3-torsion points might be omitted. As we decided to state this conjecture uniformly on e, we have not investigated this scenario.

CHAPTER 4
SMALL EXPONENTS

The results of Chapter 3 hold for every value of $e \in \mathbb{Z}_{\geq 1}$. However, one might conceive that for small values of e, stronger results hold due to the minor number of possible scenarios that may occur. In this chapter we pursue this idea, by finding results that are exclusive to some exponents, with a special focus on the small ones.

4.1 NON-GROUP GUARANTEE

In this section we certify that elliptic loops are never groups when $e \geq 3$, with few bizarre and small exceptions when $e = 2$.

Lemma 4.1.1. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop, with $e \geq 3$. Then for every affine point $P \in \mathcal{L}^a$ we have*

$$\big(P + (p:1:p)\big) + (0:1:p) \neq P + \big((p:1:p) + (0:1:p)\big).$$

Proof. It is sufficient to show that the two associations are different inside $\mathbb{P}^2(\mathbb{Z}/p^3\mathbb{Z})$. The computational verification of the following claims may be found in [Appendix C.1].

Let $P = (X : Y : 1)$ and compute

$$(S_1 : S_2 : S_3) = \big(P + (p:1:p)\big) + (0:1:p), \quad (T_1 : T_2 : T_3) = P + \big((p:1:p) + (0:1:p)\big).$$

These two points are equal inside $\mathbb{P}^2(\mathbb{Z}/p^3\mathbb{Z})$ if and only if

$$c_1 = S_1T_2 - S_2T_1, \quad c_2 = S_1T_3 - S_3T_1, \quad c_3 = S_2T_3 - S_3T_2$$

are all zero modulo p^3. It they were, also the elements of $\langle c_1, c_2, c_3 \rangle$ would vanish. In particular, since

$$54Y^3B(B-2X^3)^4p^2 \in \langle c_1, c_2, c_3\rangle,$$
$$54Y^3(96AX^{10}-3B^4+26B^3X^3-92B^2X^6+248BX^9)p^2 \in \langle c_1, c_2, c_3\rangle,$$

we would have

$$\begin{cases} Y^3B(B-2X^3)^4 \equiv 0 \bmod p, \\ Y^3(96AX^{10}-3B^4+26B^3X^3-92B^2X^6+248BX^9) \equiv 0 \bmod p. \end{cases}$$

Since we always work under the odd order Assumption 3.2.1, then $\gcd(Y,p)=1$ so the above system implies either $B \equiv 0 \bmod p$, that gives $X \not\equiv 0 \bmod p$, hence

$$A \equiv B \equiv 0 \bmod p,$$

or $B \not\equiv 0 \bmod p$, that implies $X \not\equiv 0 \bmod p$ and leads to

$$A \equiv -3X^2 \bmod p, \quad B \equiv 2X^3 \bmod p.$$

In both cases, we have $\Delta_{A,B} \equiv 0 \bmod p$, which cannot hold as $\mathcal{L}$ is an elliptic loop. □

Lemma 4.1.1 provides a concrete example of a triple that is never associative for every $e \geq 3$. When $e = 2$ the situation is slightly dissimilar, in fact there are few examples of elliptic loops that are also groups.

Definition 4.1.2 (Exceptional loops)**.** Each of the following elliptic loops

$$\mathcal{L}_{5a} = \mathcal{L}_{4,2}(\mathbb{Z}/25\mathbb{Z}), \quad \mathcal{L}_{5b} = \mathcal{L}_{4,3}(\mathbb{Z}/25\mathbb{Z}), \quad \mathcal{L}_{7a} = \mathcal{L}_{0,4}(\mathbb{Z}/49\mathbb{Z}),$$
$$\mathcal{L}_{7b} = \mathcal{L}_{0,2}(\mathbb{Z}/49\mathbb{Z}), \quad \mathcal{L}_{13a} = \mathcal{L}_{0,3}(\mathbb{Z}/169\mathbb{Z}), \quad \mathcal{L}_{13b} = \mathcal{L}_{0,10}(\mathbb{Z}/169\mathbb{Z}),$$

is referred to as *exceptional (elliptic loop).*

Proposition 4.1.3. *Exceptional loops are non-cyclic groups. More precisely, we have*

$$\mathcal{L}_{5a} \simeq \mathcal{L}_{5b} \simeq \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/15\mathbb{Z} \quad \textit{and} \quad \mathcal{L}_{7a} \simeq \mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/21\mathbb{Z},$$
$$\mathcal{L}_{7b} \simeq \mathbb{Z}/21\mathbb{Z} \oplus \mathbb{Z}/21\mathbb{Z} \quad \textit{and} \quad \mathcal{L}_{13a} \simeq \mathcal{L}_{13b} \simeq \mathbb{Z}/39\mathbb{Z} \oplus \mathbb{Z}/39\mathbb{Z}.$$

Proof. It may be straightforwardly verified [Appendix C.2]: there are 421875 ordered triples of points inside $\mathcal{L}_{5a}$ and $\mathcal{L}_{5b}$, 3176523 inside $\mathcal{L}_{7a}$, 85766121 inside $\mathcal{L}_{7b}$ and 3518743761 inside $\mathcal{L}_{13a}$ and $\mathcal{L}_{13b}$, which are all checked to associate. Therefore, the operations of the exceptional elliptic loops are associative, hence these loops are groups.

The sizes of $\mathcal{L}_{5a}, \mathcal{L}_{5b}$ and $\mathcal{L}_{7a}$ are $3p^2$ ($p = 5, 5$ and 7, respectively), while those of $\mathcal{L}_{7b}, \mathcal{L}_{13a}$ and $\mathcal{L}_{13b}$ are $9p^2$ ($p = 7, 13$ and 13, respectively). Thus, for proving the above group structures, it is sufficient to show that every element is of $3p$-torsion. We do it in [Appendix C.2] by showing that the multiplication-by-$3p$ annihilates all the points. □

Remark 4.1.4. We notice that $\mathcal{L}_{5a}$ and $\mathcal{L}_{5b}$ are actually closely related, as they lie over the elliptic curves $\mathcal{E}_{5a} = \mathcal{E}_{4,2}(\mathbb{F}_5)$ and $\mathcal{E}_{5b} = \mathcal{E}_{4,3}(\mathbb{F}_5)$, which are isomorphic via

$$\mathcal{E}_{5a} \overset{\sim}{\to} \mathcal{E}_{5b},$$
$$(X : Y : Z) \mapsto (4X : 2Y : Z).$$

The same holds for $\mathcal{L}_{13a}$ and $\mathcal{L}_{13b}$, as we have an elliptic curve isomorphism

$$\mathcal{E}_{13a} \overset{\sim}{\to} \mathcal{E}_{13b},$$
$$(X : Y : Z) \mapsto (12X : 8Y : Z).$$

The following proposition shows that the situation portrayed in Proposition 4.1.3 is unique: no other elliptic loops may be associative for any $e \geq 2$.

Proposition 4.1.5. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop with $e \geq 2$ and consider an affine point $P = (X : Y : 1) \in \mathcal{L}^a$ such that the order of $\pi(P)$ is not 3. By defining*

$P' = (X : Y + p : 1)$ *and* $R = (0 : 1 : p)$*, we have*

$$(P + P') + R \neq P + (P' + R).$$

Proof. It is sufficient to show that the two associations are different inside $\mathbb{P}^2(\mathbb{Z}/p^2\mathbb{Z})$. We compute

$$(S_1 : S_2 : S_3) = (P + P') + R, \qquad (T_1 : T_2 : T_3) = P + (P' + R),$$

which are equal inside $\mathbb{P}^2(\mathbb{Z}/p^2\mathbb{Z})$ if and only if

$$c_1 = S_1T_2 - S_2T_1, \quad c_2 = S_1T_3 - S_3T_1, \quad c_3 = S_2T_3 - S_3T_2$$

all vanish modulo p^2. If we define $F_1, F_2, G_1, G_2 \in \mathbb{Z}/p^2\mathbb{Z}$ as

$$\begin{aligned}
F_1 &= A^2 - 3AX^2 - 9BX - 3XY^2, \\
F_2 &= A^3 + 6A^2X^2 + 6ABX - 3AX^4 + 9B^2 - 18BX^3 - Y^4, \\
G_1 &= 10A^4X + 9A^3B + 2A^3Y^2 - 30A^2BX^2 + 6A^2X^5 + 6A^2X^2Y^2 + 45AB^2X + 45ABX^4 \\
&\quad + 9ABXY^2 + 54B^3 + 135B^2X^3 + 18B^2Y^2 - 9BX^3Y^2, \\
G_2 &= 2A^4 - 15A^2BX + 30A^2X^4 + 6A^2XY^2 + 9AB^2 + 90ABX^3 + 3ABY^2 - 6AX^3Y^2 \\
&\quad + 135B^2X^2 - 27BX^5 - 27BX^2Y^2.
\end{aligned}$$

we observe [Appendix C.3] that

$$c_1 = 2pY^2F_1F_2G_1, \qquad c_3 = 2pY^2F_1F_2G_2.$$

Assume by contradiction that $c_1 \equiv c_3 \equiv 0 \bmod p^2$. By the odd order Assumption 3.2.1 we have $\gcd(Y, p) = 1$, therefore one of the following conditions needs to be satisfied:

$$\text{(I)}\;\; F_1 \equiv 0 \bmod p \qquad \text{(II)}\;\; F_2 \equiv 0 \bmod p \qquad \text{(III)} \begin{cases} G_1 \equiv 0 \bmod p, \\ G_2 \equiv 0 \bmod p. \end{cases}$$

Let $F \in \mathbb{Z}[x, y, z]$ be the Weierstrass polynomial defining $\mathcal{L}$. We prove that none of the above cases may occur.

[Case I] We compute

$$(X_3 : Y_3 : Z_3) = 3P$$

and we verify [Appendix C.3] that

$$X_3, Z_3 \in \langle F(P), F_1 \rangle.$$

Thus, if F_1 vanishes modulo p, then $\pi(3P) = \mathcal{O}$, which implies that the order of $\pi(P) \neq \mathcal{O}$ divides 3, contradicting the hypothesis.

[Case II] We compute

$$(X_4 : Y_4 : Z_4) = 4P$$

and we verify [Appendix C.3] that

$$X_4, Z_4 \in \langle F(P_1), F_2 \rangle.$$

Thus, if F_2 vanishes modulo p, then $\pi(4P_1) = \mathcal{O}$, which is impossible by the odd order Assumption 3.2.1.

[Case III] We define the ideal

$$I = \langle F(P), G_1, G_2 \rangle.$$

A straight check [Appendix C.3] shows that both

$$864Y^{10}(X^3 - Y^2) \in I, \quad \text{and} \quad 288Y^8(B - 2X^3 + 2Y^2) \in I.$$

Therefore, if both the G_i's vanish modulo p, then by using again $\gcd(Y,p)=1$ we get

$$\begin{cases} X^3 - Y^2 \equiv 0 \bmod p, \\ B - 2X^3 + 2Y^2 \equiv 0 \bmod p, \\ X^3 + AX + B - Y^2 \equiv 0 \bmod p, \end{cases}$$

which implies $A = B = 0$, contradicting $\Delta_{A,B} \not\equiv 0 \bmod p$. □

Thus, we conclude that all but six elliptic loops with $e \geq 2$ are non-exceptional, in particular they are not groups.

Corollary 4.1.6. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop, with $e \geq 2$. Then $\mathcal{L}$ is a group if and only if $\mathcal{L}$ is an exceptional loop.*

Proof. By Proposition 4.1.5 the addition law on $\mathcal{L}$ may be associative only if the affine points of $\mathcal{E} = \mathcal{E}_{A,B}(\mathbb{F}_p)$ have all order 3. By Corollary 1.3.8 this may happen only if

$$\mathcal{E} \simeq \mathbb{Z}/3\mathbb{Z} \qquad \text{or} \qquad \mathcal{E} \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

By Hasse's Theorem 1.3.1 the first case may occur only for $p \in \{5,7\}$, while the joint use of Corollary 1.3.8 and Theorem 1.3.1 shows that the second case may occur only for $p \in \{7,13\}$. A direct check of these possibilities shows that the only viable curves are

$$\begin{aligned} \mathbb{Z}/3\mathbb{Z} &\rightarrow \mathcal{E}_{4,2}(\mathbb{F}_5), \mathcal{E}_{4,3}(\mathbb{F}_5), \mathcal{E}_{0,4}(\mathbb{F}_7), \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} &\rightarrow \mathcal{E}_{0,2}(\mathbb{F}_7), \mathcal{E}_{0,3}(\mathbb{F}_{13}), \mathcal{E}_{0,10}(\mathbb{F}_{13}), \end{aligned}$$

which underlie exceptional loops. On the other side, in such cases by Proposition 4.1.3 the loops are associative, hence groups. □

Remark 4.1.7. The points of order divisible by 3 are special, as we have already noticed in Proposition 3.3.10 and 3.3.15. In those points, layers may exceptionally intersect, originating a possibly strange behaviour. In fact, the cases discussed in Proposition 4.1.3 show that when there are only 3-torsion points in the underlying curve, the corresponding elliptic loop has, in a sense, a unique large layer.

4.2 THE CASE $e \leq 5$

As shown by Corollary 4.1.6, there is no hope of having associativity for almost every elliptic loop $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$, even for small exponents $e \in \mathbb{Z}_{\geq 1}$.

However, we have already observed (Proposition 2.3.7) that the infinity part tends to have a simpler behaviour when $e \leq 5$. The next proposition shows that, in such cases, $\mathcal{L}^\infty$ is a group.

Proposition 4.2.1. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop, with $e \leq 5$. Then $\mathcal{L}^\infty$ is an abelian group, generated by*

$$\mathcal{L}^\infty = \langle (p : 1 : 0) \rangle \oplus \langle (0 : 1 : p) \rangle.$$

In particular, we have a group isomorphism

$$\mathcal{L}^\infty \simeq \mathbb{Z}/p^{e-1}\mathbb{Z} \oplus \mathbb{Z}/p^{e-1}\mathbb{Z}.$$

Proof. Let $P_1, P_2, P_3 \in \mathcal{L}^\infty$, then there are integers $X_1, Z_1, X_2, Z_2, X_3, Z_3$ such that they may be written as $P_1 = (X_1 p : 1 : Z_1 p), P_2 = (X_2 p : 1 : Z_2 p)$ and $P_3 = (X_3 p : 1 : Z_3 p)$. Let us define

$$(S_1 : S_2 : S_3) = \big(P_1 + P_2\big) + P_3, \qquad (T_1 : T_2 : T_3) = P_1 + \big(P_2 + P_3\big),$$

and the commutators

$$c_1 = S_1 T_2 - S_2 T_1, \quad c_2 = S_1 T_3 - S_3 T_1, \quad c_3 = S_2 T_3 - S_3 T_2.$$

We directly verify [Appendix C.4.1] that all minimal degrees of p appearing in the above commutators are at least 5, in fact

$$c_1, c_3 \in p^5\mathbb{Z}, \quad \text{and} \quad c_2 \in p^6\mathbb{Z}.$$

Thus, we conclude

$$(S_1 : S_2 : S_3) = (T_1 : T_2 : T_3) \in \mathbb{P}^2(\mathbb{Z}/p^5\mathbb{Z}),$$

so the sum operation is associative on $\mathcal{L}^\infty$ when $e \leq 5$, i.e. it is an abelian group.

Moreover, by Theorem 3.4.3 we know that $\mathcal{L}^\infty$ is generated by $(p : 1 : 0)$ and $(0 : 1 : p)$, hence the same holds as a group. By the same theorem these two elements generate cyclic groups of order p^{e-1}, from which the claimed group isomorphism immediately follows. □

Proposition 4.2.1 shows that the infinity part is always a group when the exponent is $e \leq 5$. The following lemma shows that this condition is sharp: for $e \geq 6$ the infinity part of an elliptic loop cannot be a group, regardless the choice of the parameters.

Lemma 4.2.2. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop, with $e \geq 6$. Then*

$$\big((p : 1 : 0) + (0 : 1 : p)\big) + (0 : 1 : p) \neq (p : 1 : 0) + \big((0 : 1 : p) + (0 : 1 : p)\big).$$

Proof. It is sufficient to show that they are different inside $\mathbb{P}^2(\mathbb{Z}/p^6\mathbb{Z})$. We compute

$$\begin{aligned}(S_1 : S_2 : S_3) &= \big((p : 1 : 0) + (0 : 1 : p)\big) + (0 : 1 : p),\\ (T_1 : T_2 : T_3) &= (p : 1 : 0) + \big((0 : 1 : p) + (0 : 1 : p)\big).\end{aligned}$$

They represent the same point in $\mathbb{P}^2(\mathbb{Z}/p^6\mathbb{Z})$ if and only if

$$c_1 = S_1T_2 - S_2T_1, \quad c_2 = S_1T_3 - S_3T_1, \quad c_1 = S_2T_3 - S_3T_2$$

all vanish modulo p^6. We notice [Appendix C.4.2] that $c_2 \equiv 0 \bmod p^6$, while

$$\begin{aligned} 972p^5B^3(B-2) &\in \langle c_1, c_3\rangle, \\ 36p^5B(4A-9B^2+24B) &\in \langle c_1, c_3\rangle, \\ 6p^5A(2A+3B) &\in \langle c_1, c_3\rangle. \end{aligned}$$

Thus, if $c_1 \equiv c_3 \equiv 0 \bmod p^6$ then also

$$\begin{cases} B(B-2) \equiv 0 \bmod p, \\ B(4A-9B^2+24B) \equiv 0 \bmod p, \\ A(2A+3B) \equiv 0 \bmod p, \end{cases}$$

whose solutions are

$$A \equiv B \equiv 0 \bmod p \quad \text{and} \quad A \equiv -3, B \equiv 2 \bmod p.$$

In both cases $\Delta_{A,B} \equiv 0 \bmod p$, contradicting the fact that $\mathcal{L}$ is an elliptic loop. □

4.3 THE CASE $e \leq 3$

We have already observed (Remark 3.1.6) that the infinity part of an elliptic loop $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ never depends, set theoretically, on the chosen A and B. Here we notice that, when the exponent e is at most 3, even the addition operation on $\mathcal{L}^\infty$ is independent of (A, B), so that this group might be defined without referring to any curve.

Proposition 4.3.1. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop, with $e \leq 3$. Then for every $a, b, c, d \in \mathbb{Z}$ we have*

$$(ap : 1 : bp) + (cp : 1 : dp) = \big((a+c)p : 1 : (b+d)p\big),$$

so that the following

$$\begin{aligned}\iota : \mathcal{L}^\infty &\to \mathbb{Z}/p^{e-1}\mathbb{Z} \oplus \mathbb{Z}/p^{e-1}\mathbb{Z},\\ (X : Y : Z) &\mapsto \left(\frac{X}{pY}, \frac{Z}{pY}\right),\end{aligned}$$

is a well-defined group isomorphism.

Proof. We have $m = \min\{\mathrm{v}_p(ap), \mathrm{v}_p(bp), \mathrm{v}_p(cp), \mathrm{v}_p(dp)\} \geq 1$, hence by part (ii) of Proposition 3.4.2 we get

$$(ap : 1 : bp) + (cp : 1 : dp) = (ap + cp : 1 : bp + dp) \in \mathbb{P}^2(\mathbb{Z}/p^{3m}\mathbb{Z}),$$

even more so the same equality holds in $\mathbb{P}^2(\mathbb{Z}/p^3\mathbb{Z})$. Since every point $(X : Y : Z) \in \mathcal{L}^\infty$ has an invertible Y-value, while both X and Z are divisible by p, therefore the map ι is well-defined. The above equality proves that it is also a group morphism, as for every $P_1 = (X_1 : Y_1 : Z_1), P_2 = (X_2 : Y_2 : Z_2) \in \mathcal{L}^\infty$ we have

$$\begin{aligned}\iota(P_1 + P_2) &= \iota\left(\left(\frac{X_1}{Y_1} : 1 : \frac{Z_1}{Y_1}\right) + \left(\frac{X_2}{Y_2} : 1 : \frac{Z_2}{Y_2}\right)\right) = \iota\left(\left(\frac{X_1}{Y_1} + \frac{X_2}{Y_2} : 1 : \frac{Z_1}{Y_1} + \frac{Z_2}{Y_2}\right)\right)\\ &= \left(\frac{\frac{X_1}{Y_1} + \frac{X_2}{Y_2}}{p}, \frac{\frac{Z_1}{Y_1} + \frac{Z_2}{Y_2}}{p}\right) = \left(\frac{\frac{X_1}{Y_1}}{p}, \frac{\frac{Z_1}{Y_1}}{p}\right) + \left(\frac{\frac{X_2}{Y_2}}{p}, \frac{\frac{Z_2}{Y_2}}{p}\right) = \iota(P_1) + \iota(P_2).\end{aligned}$$

It is easily seen that its inverse is

$$\begin{aligned}\iota^{-1} : \mathbb{Z}/p^{e-1}\mathbb{Z} \oplus \mathbb{Z}/p^{e-1}\mathbb{Z} &\to \mathcal{L}^\infty,\\ (a, b) &\mapsto (ap : 1 : bp),\end{aligned}$$

then ι is a well-defined group isomorphism. □

When $e \leq 3$, by means of Proposition 4.3.1 we may write $\mathcal{L}^\infty(\mathbb{Z}/p^e\mathbb{Z})$ in place of $\mathcal{L}^\infty_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$, further shortened to $\mathcal{L}^\infty$ when the ring is understood. In such cases $\mathcal{L}^\infty$ is universal, it is the same group regardless of the underlying elliptic curve.

4.4 THE CASE $e \leq 2$

When the exponent e does not exceed 2, many forms of weak associativity hold for points in special positions. In this section we investigate them, providing examples to highlight that such formulae may not hold when $e \geq 3$.

It is worth pointing out that for $e = 1$ the results are still true but trivial since in these cases elliptic loops are groups, as seen in Chapter 2.

4.4.1 Associativity with $\mathcal{L}^\infty$

The following lemmas show that three points associate if two of them belong to $\mathcal{L}^\infty$ or one of them lies inside $< (p : 1 : 0) >$.

Lemma 4.4.1. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop, with $e \leq 2$. For every $P \in \mathcal{L}$ and $Q, R \in \mathcal{L}^\infty$, we have*

$$P + (Q + R) = (P + Q) + R.$$

Proof. Under our assumptions there are $a, b, c, d \in \mathbb{Z}$ such that

$$Q = (ap : 1 : bp), \qquad R = (cp : 1 : dp).$$

Let

$$(X_1 : Y_1 : Z_1) = P + (Q + R), \qquad (X_2 : Y_2 : Z_2) = (P + Q) + R$$

and define

$$c_1 = X_1Y_2 - X_2Y_1, \quad c_2 = X_1Z_2 - X_2Z_1, \quad c_3 = Y_1Z_2 - Y_2Z_1.$$

A formal verification [Appendix C.5] shows that all these c_i's belong to $p^2\mathbb{Z}$, which implies that $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$ are the same point inside $\mathbb{P}^2(\mathbb{Z}/p^2\mathbb{Z})$. □

Lemma 4.4.2. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop, with $e \leq 2$. For every $P, Q \in \mathcal{L}$ and $R \in < (p : 1 : 0) >$, we have*

$$P + (Q + R) = (P + Q) + R.$$

Proof. Under our assumptions there is $a \in \mathbb{Z}$ such that $R = (ap : 1 : 0)$. Let F be the Weierstrass polynomial defining $\mathcal{E}_{A,B}(\mathbb{F}_p) = \mathcal{V}(F)$, let

$$(X_1 : Y_1 : Z_1) = P + (Q + R), \qquad (X_2 : Y_2 : Z_2) = (P + Q) + R$$

and define

$$c_1 = X_1Y_2 - X_2Y_1, \quad c_2 = X_1Z_2 - X_2Z_1, \quad c_3 = Y_1Z_2 - Y_2Z_1.$$

A formal verification [Appendix C.6] shows that for every $P, Q \in \mathbb{P}^2(\mathbb{Z}/p^2\mathbb{Z})$, if we define the ideal $I_p = \langle p, F(P), F(Q)\rangle \subseteq \mathbb{Z}$, then

$$\{c_1, c_2, c_3\} \subseteq I_p^2.$$

If P, Q are points of $\mathcal{L}$, then $F(P) \equiv F(Q) \equiv 0 \bmod p$, hence I_p is the ideal generated by p in $\mathbb{Z}$, which implies that

$$c_1 \equiv c_2 \equiv c_3 \equiv 0 \bmod p^2.$$

Thus, the points $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$ are equal inside $\mathbb{P}^2(\mathbb{Z}/p^2\mathbb{Z})$. □

Lemma 4.4.1 and 4.4.2 detail some cases where parentheses are not needed. The following example displays this may not hold for $e \geq 3$, even if the hypotheses of both lemmas are simultaneously satisfied.

Example 4.4.3. Let $p = 13, e = 3, A = 0, B = 2$ and define $\mathcal{L} = \mathcal{L}_{0,2}(\mathbb{Z}/2197\mathbb{Z})$. We consider the points

$$P = (1 : 9 : 1) \in \mathcal{L}, \qquad Q = (0 : 1 : 13),\ R = (13 : 1 : 0) \in \mathcal{L}^\infty,$$

and we observe that

$$\begin{aligned}
P + (Q + R) &= (469 : 1036 : 1) \in \mathbb{P}^2(\mathbb{Z}/2197\mathbb{Z}),\\
Q + (P + R) &= (469 : 22 : 1) \in \mathbb{P}^2(\mathbb{Z}/2197\mathbb{Z}),\\
(P + Q) + R &= (469 : 2050 : 1) \in \mathbb{P}^2(\mathbb{Z}/2197\mathbb{Z})
\end{aligned}$$

are all different. However, when $e = 2$ the same operations give

$$P + (Q + R) = Q + (P + R) = (P + Q) + R = (131 : 22 : 1) \in \mathbb{P}^2(\mathbb{Z}/169\mathbb{Z}),$$

as prescribed from both Lemma 4.4.1 and 4.4.2.

We also notice that Lemma 4.4.2 does not hold by using $\langle(0 : 1 : p)\rangle$ in place of $\langle(p : 1 : 0)\rangle$, as

$$\begin{aligned}
(1 : 9 : 1) + \big((10 : 1 : 1) + (0 : 1 : 13)\big) &= (97 : 98 : 1) \in \mathbb{P}^2(\mathbb{Z}/169\mathbb{Z}),\\
(10 : 1 : 1) + \big((1 : 9 : 1) + (0 : 1 : 13) &= (149 : 85 : 1) \in \mathbb{P}^2(\mathbb{Z}/169\mathbb{Z}),\\
\big((1 : 9 : 1) + (10 : 1 : 1)\big) + (0 : 1 : 13) &= (19 : 33 : 1) \in \mathbb{P}^2(\mathbb{Z}/169\mathbb{Z})
\end{aligned}$$

are three different points.

4.4.2 A pair lying over the same point

When performing the difference between two points that lie over the same point, we may associate their parts at infinity.

Proposition 4.4.4. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop, with $e \leq 2$, and let $P_1, P_2 \in \mathcal{L}$ such that $\pi(P_1) = \pi(P_2)$. Then for every $R_1, R_2 \in \mathcal{L}^\infty$ we have*

$$(P_1 + R_1) - (P_2 + R_2) = (P_1 - P_2) + (R_1 - R_2).$$

Proof. If $P_1 = (X : Y : Z)$ then, by hypotheses, there are integers $s_x, s_y, s_z, a, b, c, d \in \mathbb{Z}$

such that

$$P_2 = (X + s_x p : Y + s_y p : Z + s_z p), \quad R_1 = (ap : 1 : bp), \quad R_2 = (cp : 1 : dp).$$

The points

$$(S_1 : S_2 : S_3) = (P_1 + R_1) - (P_2 + R_2), \quad (T_1 : T_2 : T_3) = (P_1 - P_2) + (R_1 - R_2).$$

are equal inside $\mathbb{P}^2(\mathbb{Z}/p^2\mathbb{Z})$ if and only if the commutators

$$c_1 = S_1T_2 - S_2T_1, \quad c_2 = S_1T_3 - S_3T_1, \quad c_3 = S_2T_3 - S_3T_2,$$

belong to $p^2\mathbb{Z}$, which may be straightforwardly verified [Appendix C.7]. □

Proposition 4.4.4 easily implies that any possible association of points satisfying the proposition's hypotheses produces the same final result. As an instance, since $\mathcal{L}^\infty$ is a group and $P_1 - P_2 \in \mathcal{L}^\infty$, we have

$$(P_1 - P_2) + (R_1 - R_2) = \big((P_1 - P_2) + R_1\big) - R_2 = \big((P_1 - P_2) - R_2\big) + R_1,$$

and by Lemma 3.3.2 we also get

$$(P_1 + R_1) - (P_2 + R_2) = \Big(\big((P_1 + R_1) - R_2\big) + R_2\Big) - (P_2 + R_2) = \big((P_1 + R_1) - R_2\big) - P_2.$$

In conclusion, when summing points lying over opposite points to those at infinity, the parentheses may be omitted. The following example shows that a similar result may not hold for higher exponents.

Example 4.4.5. Let $p = 11, e = 3, A = 6$ and $B = 6$. In $\mathcal{L} = \mathcal{L}_{6,6}(\mathbb{Z}/1331\mathbb{Z})$ we consider

$$P_1 = (1229 : 326 : 1), \qquad P_2 = (569 : 502 : 1),$$

which both lie over $(8:7:1) \in \mathcal{E}_{6,6}(\mathbb{Z}/11\mathbb{Z})$. Let also consider

$$R_1 = (11:1:0), \qquad R_2 = (0:1:11).$$

We have

$$\begin{aligned}
(P_1 + R_1) - (P_2 + R_2) &= (935:1:506),\\
(P_1 + P_2) - (R_1 + R_2) &= (814:1:22),\\
(P_1 - R_2) - (P_2 - R_1) &= (693:1:869),\\
\big((P_1 + R_1) - P_2\big) - R_2) &= (209:1:264),\\
\big((P_1 + R_2) - P_2\big) - R_1) &= (1177:1:143),
\end{aligned}$$

which are all distinct points in $\mathbb{P}^2(\mathbb{Z}/1331\mathbb{Z})$. However, they agree in $\mathbb{P}^2(\mathbb{Z}/121\mathbb{Z})$ as prescribed by Proposition 4.4.4, being all equal to $(88:1:22) \in \mathbb{P}^2(\mathbb{Z}/121\mathbb{Z})$.

4.4.3 A triple lying over the same point

Proposition 4.4.6. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop, with $e \leq 2$, and let $P_1, P_2, P_3 \in \mathcal{L}$ such that $\pi(P_1) = \pi(P_2) = \pi(P_3)$. Then*

$$(P_1 + P_2) - P_3 = P_1 + (P_2 - P_3).$$

Proof. By hypothesis, there are integers $X, Y, Z, s_x, s_y, s_z, t_x, t_y, t_z \in \mathbb{Z}$ such that

$$P_1 = (X:Y:Z), \quad P_2 = (X + s_x p : Y + s_y p : Z + s_z p), \quad P_3 = (X + t_x p : Y + t_y p : Z + t_z p).$$

With this notation, we compute

$$(S_1 : S_2 : S_3) = (P_1 + P_2) - P_3, \qquad (T_1 : T_2 : T_3) = P_1 + (P_2 - P_3).$$

and

$$c_1 = S_1T_2 - S_2T_1, \quad c_2 = S_1T_3 - S_3T_1, \quad c_3 = S_2T_3 - S_3T_2.$$

We explicitly check [Appendix C.8] that all the c_i's belong to the ideal $p^2\mathbb{Z}$, so that

$$(S_1 : S_2 : S_3) = (T_1 : T_2 : T_3) \in \mathbb{P}^2(\mathbb{Z}/p^2\mathbb{Z}),$$

which concludes the proof. □

Remark 4.4.7. In the setting of Proposition 4.4.6 we may avoid useless parentheses: as the result is independent of the association, it will be simply denoted by

$$P_1 + P_2 - P_3.$$

Again, the impossibility of extending such a result for larger exponents e is witnessed by the following example. It also shows that the minus sign is essential, three points lying over the same point may not associate if they belong to different layers.

Example 4.4.8. Let $p = 31, e = 3, A = 0$ and $B = 3$. In $\mathcal{L}_{0,3}(\mathbb{Z}/29791\mathbb{Z})$ we consider

$$P_1 = (45 : 22 : 1),\ P_2 = (45 : 115 : 1),\ P_3 = (14 : 29782 : 1).$$

It is easy to check that $\pi(P_1) = \pi(P_2) = \pi(P_3) = (14 : 22 : 1) \in \mathcal{E}_{0,3}(\mathbb{F}_{31})$, as well as

$$\begin{gathered} (P_1 + P_2) - P_3 = (17374 : 3029 : 1) \\ \rotatebox{90}{$\neq$} \\ P_1 + (P_2 - P_3) = (1998 : 146 : 1). \end{gathered}$$

However, for $e = 2$ the same computation gives

$$(P_1 + P_2) - P_3 = (76 : 146 : 1) = P_1 + (P_2 - P_3) \in \mathbb{P}^2(\mathbb{Z}/961\mathbb{Z}).$$

Finally, we notice that the same result does not hold by replacing $-P_3$ with P_3, as

$$(P_1 + P_2) + P_3 = (314 : 118 : 1) \neq (159 : 924 : 1) = P_1 + (P_2 + P_3) \in \mathbb{P}^2(\mathbb{Z}/961\mathbb{Z}).$$

Corollary 4.4.9. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop, with $e \leq 2$, and let $P_1, P_2 \in \mathcal{L}$ such that $P_1 + P_2 \in \mathcal{L}^\infty$. Then*

$$2(P_1 + P_2) = \big((P_1 + P_2) + P_1\big) + P_2 = (2P_1 + P_2) + P_2.$$

Proof. Since $P_1 + P_2 \in \mathcal{L}^\infty$, then $\pi(P_1) = \pi(-P_2)$ and by Proposition 4.4.4 we have

$$(P_1 + P_2) + (P_1 + P_2) = \big(P_1 + (P_1 + P_2)\big) + (P_2 + \mathcal{O}).$$

By Proposition 4.4.6 we can associate

$$\big(P_1 + (P_1 + P_2)\big) + P_2 = (2P_1 + P_2) + P_2,$$

which concludes the proof. □

Even this weak form of associativity is extremely "exclusive", neither it holds for larger values of e nor it may be extended to higher multiples of $P_1 + P_2$, i.e. for a generic $n \in \mathbb{Z}$ we may have

$$n(P_1 + P_2) \neq \Big(\dots\big((nP_1 + P_2) + P_2\big) + \dots\Big) + P_2.$$

The following example portrays both phenomena, also showing that the most "natural" association of the above points, namely $2P_1 + 2P_2$, is the unique one that may produce a different outcome.

Example 4.4.10. Let $p = 11, e = 3, A = 1$ and $B = 6$. In $\mathcal{L} = \mathcal{L}_{1,6}(\mathbb{Z}/1331\mathbb{Z})$ we consider

$$P_1 = (618 : 213 : 1), \qquad P_2 = (255 : 1096 : 1),$$

which sum to $P_1 + P_2 = (429 : 1 : 341) \in \mathcal{L}^\infty$. We check that

$$2(P_1 + P_2) = (858 : 1 : 682) \neq (495 : 1 : 77) = (2P_1 + P_2) + P_2 \in \mathbb{P}^2(\mathbb{Z}/1331\mathbb{Z}),$$

even if, when $e = 2$, we have

$$2(P_1 + P_2) = (11 : 1 : 77) = (2P_1 + P_2) + P_2 \in \mathbb{P}^2(\mathbb{Z}/121\mathbb{Z}),$$

as prescribed by Lemma 4.4.9. It is also worth pointing out that

$$2(P_1 + P_2) = (11 : 1 : 77) \neq (110 : 1 : 44) = 2P_1 + 2P_2 \in \mathbb{P}^2(\mathbb{Z}/121\mathbb{Z}).$$

Moreover, we observe that this weak associativity may not work for higher multiples even inside $\mathbb{P}^2(\mathbb{Z}/121\mathbb{Z})$, in fact

$$3(P_1 + P_2) = (77 : 1 : 55) \neq (22 : 1 : 110) = \big((3P_1 + P_2) + P_2\big) + P_2 \in \mathbb{P}^2(\mathbb{Z}/121\mathbb{Z}).$$

4.4.4 Two triples lying over two points

The following result is a weak associativity property, which will be of fundamental importance in the next section. In its statement, unnecessary parentheses are avoided by means of Remark 4.4.7.

Proposition 4.4.11. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic loop, with $e \leq 2$, and let $P_1, P_2, P_3, Q_1, Q_2, Q_3 \in \mathcal{L}$ such that $\pi(P_1) = \pi(P_2) = \pi(P_3)$ and $\pi(Q_1) = \pi(Q_2) = \pi(Q_3)$. Then*

$$(P_1 + P_2 - P_3) + (Q_1 + Q_2 - Q_3) = (P_1 + Q_1) + (P_2 + Q_2) - (P_3 + Q_3).$$

Proof. Since $\pi(P_1) = \pi(P_2) = \pi(P_3)$, there are integers $X_1, Z_1, a_1, b_1, c_1, d_1 \in \mathbb{Z}$ such that

$$P_1 = (X_1 : 1 : Z_1), \quad P_2 = (X_1 + a_1 p : 1 : Z_1 + b_1 p), \quad P_3 = (X_1 + c_1 p : 1 : Z_1 + d_1 p).$$

Similarly, since $\pi(Q_1) = \pi(Q_2) = \pi(Q_3)$, there are $X_2, Z_2, a_2, b_2, c_2, d_2 \in \mathbb{Z}$ such that

$$Q_1 = (X_2 : 1 : Z_2), \quad Q_2 = (X_2 + a_2 p : 1 : Z_2 + b_2 p), \quad Q_3 = (X_2 + c_2 p : 1 : Z_2 + d_2 p).$$

We compute

$$\begin{aligned}(S_1 : S_2 : S_3) &= (P_1 + P_2 - P_3) + (Q_1 + Q_2 - Q_3),\\ (T_1 : T_2 : T_3) &= (P_1 + Q_1) + (P_2 + Q_2) - (P_3 + Q_3),\end{aligned}$$

and we computationally check [Appendix C.9] that the three quantities

$$c_1 = S_1T_2 - S_2T_1, \quad c_2 = S_1T_3 - S_3T_1, \quad c_3 = S_2T_3 - S_3T_2$$

belong to $p^2\mathbb{Z}$, hence $(S_1 : S_2 : S_3) = (T_1 : T_2 : T_3) \in \mathbb{P}^2(\mathbb{Z}/p^2\mathbb{Z})$. □

Even in this case, the result holds only for $e \leq 2$, as shown by the following example. It contextually shows that this particular association holds only for triples of points.

Example 4.4.12. Let $p = 7, e = 3, A = 0, B = 3$ and $\mathcal{L} = \mathcal{L}_{0,3}(\mathbb{Z}/343\mathbb{Z})$. Let us consider

$$\begin{aligned}P_1 &= (143 : 122 : 1), \quad & P_2 &= (45 : 325 : 1), \quad & P_3 &= (262 : 297 : 1),\\ Q_1 &= (184 : 215 : 1), \quad & Q_2 &= (86 : 166 : 1), \quad & Q_3 &= (184 : 152 : 1),\end{aligned}$$

which satisfy

$$\begin{aligned}\pi(P_1) = \pi(P_2) = \pi(P_3) &= (3 : 3 : 1) \in \mathcal{E}_{0,3}(\mathbb{F}_7),\\ \pi(Q_1) = \pi(Q_2) = \pi(Q_3) &= (2 : 5 : 1) \in \mathcal{E}_{0,3}(\mathbb{F}_7).\end{aligned}$$

Nonetheless, we have

$$\begin{aligned}(P_1 + P_2 - P_3) + (Q_1 + Q_2 - Q_3) &= (265 : 311 : 1)\\ &\quad\;\; \nparallel\\ (P_1 + Q_1) + (P_2 + Q_2) - (P_3 + Q_3) &= (216 : 213 : 1).\end{aligned}$$

Instead, if $e = 2$ we find

$$
\begin{aligned}
(P_1 + P_2 - P_3) + (Q_1 + Q_2 - Q_3) &= (20 : 17 : 1) \\
&= (P_1 + Q_1) + (P_2 + Q_2) - (P_3 + Q_3) \in \mathbb{P}^2(\mathbb{Z}/49\mathbb{Z}).
\end{aligned}
$$

Finally, we observe that

$$
(P_2 - P_3) + (Q_2 - Q_3) = (0 : 1 : 21) \neq (7 : 1 : 35) = (P_2 + Q_2) - (P_3 + Q_3) \in \mathbb{P}^2(\mathbb{Z}/49\mathbb{Z}),
$$

which shows that a similar result does not hold for pairs in place of triples.

Remark 4.4.13. We conclude this section by highlighting a technical detail. The proofs of Lemma 4.4.1 and Proposition 4.4.4, 4.4.6 and 4.4.11 do not involve the Weierstrass polynomial of the curve. This means that the same results generically hold for points inside $\mathbb{P}^2(\mathbb{Z}/p^2\mathbb{Z})$, whenever the involved operations make sense.

4.5 THE CASE $e = 2$

In this section we focus on the smallest non-associative case of elliptic loops, i.e. those of exponent $e = 2$.

4.5.1 Rational q-torsion

Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^2\mathbb{Z})$ be an elliptic loop and $\mathcal{E} = \mathcal{E}_{A,B}(\mathbb{F}_p)$ be its underlying elliptic curve. When $\mathcal{E}$ is not anomalous, we know by Theorem 3.5.1 that every layer of $\mathcal{L}$ contains an isomorphic copy of $\mathcal{E}$. If $q = |\mathcal{E}|$, these points are referred to as (rational) q-torsion points, as their orders divide q.

Here we aim at characterizing such q-torsion points lying over the same point $P \in \mathcal{E}$.

Lemma 4.5.1. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^2\mathbb{Z})$ be an elliptic loop and let $P_1, P_2, P_3 \in \mathcal{L}$ such that $\pi(P_1) = \pi(P_2) = \pi(P_3)$. Then for every $m \in \mathbb{Z}_{\geq 0}$ we have*

$$
m(P_1 + P_2 - P_3) = mP_1 + mP_2 - mP_3.
$$

Proof. We prove it by induction on m.

$[m = 1]$ There is nothing to prove.

$[m \to m+1]$ By inductive hypothesis we have

$$(m+1)(P_1+P_2-P_3) = (P_1+P_2-P_3)+m(P_1+P_2-P_3) = (P_1+P_2-P_3)+(mP_1+mP_2-mP_3).$$

Since $\pi(mP_1) = \pi(mP_2) = \pi(mP_3)$, Proposition 4.4.11 implies

$$(P_1 + P_2 - P_3) + (mP_1 + mP_2 - mP_3) = (P_1 + mP_1) + (P_2 + mP_2) - (P_3 + mP_3),$$

which is $(m+1)P_1 + (m+1)P_2 - (m+1)P_3$, concluding the inductive step. □

Lemma 4.5.1 immediately implies that for every $m \in \mathbb{Z}_{\geq 1}$, if P_1, P_2, P_3 are m-torsion points lying over the same point $P \in \mathcal{E}$, then also $P_1 + P_2 - P_3$ is.

We may now describe q-torsion points lying over the same point. We first notice that the infinity-case is easily understood, as the unique q-torsion point over $\mathcal{O} \in \mathcal{E}$ is $\mathcal{O} \in \mathcal{L}$. On the other hand, q-torsion points lying over the same affine point $P \in \mathcal{E}^a$ may be notably detected by intersecting $\pi^{-1}(P)$ with a line, as shown by the following theorem.

Theorem 4.5.2. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^2\mathbb{Z})$ be an elliptic loop whose underlying elliptic curve $\mathcal{E} = \mathcal{E}_{A,B}(\mathbb{F}_p)$ has size $q = |\mathcal{E}|$ with $\gcd(p,q) = 1$. For every affine point $P \in \mathcal{E}^a$ let*

$$\mathcal{Q}_P = \{Q \in \mathcal{L} \mid qQ = \mathcal{O},\ \pi(Q) = P\}$$

be the q-torsion points of $\mathcal{L}$ lying over P. Then

(i) There are $P_1, \dots, P_p \in \mathcal{L}$ such that

$$\forall i \in \{1, \dots, p\} \ : \ \mathcal{Q}_P \cap \mathbb{L}_i = \{P_i\}.$$

(ii) $\{P_i - P_j\}_{1 \leq i,j \leq p}$ is a subgroup of $\mathcal{L}^\infty$ of order p.

(iii) There are $a, b, c \in \mathbb{Z}$ such that

$$\mathcal{Q}_P = \pi^{-1}(P) \cap \mathcal{V}(ax + by + cz).$$

Proof. (i): Since $\gcd(p, q) = 1$, for every layer $\mathbb{L}_i$ we have by Theorem 3.5.1 a group isomorphism $\phi_i : \mathbb{L}_i \xrightarrow{\sim} \mathcal{E} \oplus \mathbb{Z}/p\mathbb{Z}$, whose restriction to the first coordinate is the canonical projection. Thus, P_i is the unique element in $\phi_i^{-1}\big((P, 0)\big)$.

(ii): Since the P_i's lie over P, their differences lie over $\mathcal{O}$, therefore

$$G = \{P_i - P_j\}_{1 \le i,j \le p} \subseteq \mathcal{L}^\infty.$$

G is closed under point addition, since for every $1 \le i_1, j_1, i_2, j_2 \le p$ Proposition 4.4.4 gives

$$(P_{i_1} - P_{j_1}) + (P_{i_2} - P_{j_2}) = \big(P_{i_1} + (P_{i_2} - P_{j_2})\big) - P_{j_1}$$

and Lemma 4.5.1 implies that the point $P_{i_1} + P_{i_2} - P_{j_2}$ is again q-torsion and lies over P, then there exists $1 \le k \le p$ such that

$$(P_{i_1} + P_{i_2} - P_{j_2}) - P_{j_1} = P_k - P_{j_1} \in G.$$

Since $\mathcal{O} = P_1 - P_1 \in G$ and $-(P_i - P_j) = P_j - P_i \in G$, then G is a subgroup of $\mathcal{L}^\infty$.

By Proposition 4.2.1, $\mathcal{L}^\infty$ is a group of size p^2. Since the P_i's belong to different layers and are affine, they cannot be the same point, so $|G| > 1$. As for every $1 \le i, j \le p$ we have $P_i - P_i = \mathcal{O} = P_j - P_j$, not all the possible differences are distinct, which implies $|G| < p^2$. Being G a subgroup of a p-group, the unique possibility left is $|G| = p$.

(iii): From part (ii) we know that G is cyclic of prime order, hence generated by any of its non-zero elements, such as $P_2 - P_1$. Therefore

$$\mathcal{Q}_P = \{P_1, P_2, \dots, P_p\} = \{k(P_2 - P_1) + P_1\}_{k \in \{1,2,\dots,p\}}.$$

As $P_2 - P_1 \in \mathcal{L}^\infty$, there are $s, t \in \mathbb{Z}$ such that

$$(P_2 - P_1) = (sp : 1 : tp),$$

whose multiples, by Proposition 4.3.1, are

$$k(P_2 - P_1) = (ksp : 1 : ktp).$$

By defining

$$\begin{aligned}
\alpha(x,z) &= (-At)x^2 - (2As + 6Bt)xz + (-3Bs + A^2t)z^2 + s \in \mathbb{Z}[x,z],\\
\beta(x,z) &= 3sx^2 + 2Atxz + (As + 3Bt)z^2 + t \in \mathbb{Z}[x,z],
\end{aligned}$$

a direct inspection of the addition laws shows that, for every integers $X, Z \in \mathbb{Z}$, one has

$$(ksp : 1 : ktp) + (X : 1 : Z) = \big(X + k\alpha(X,Z)p : 1 : Z + k\beta(X,Z)p\big).$$

Therefore, if we define

$$P_1 = (X_1 : 1 : Z_1), \quad \alpha_1 = \alpha(X_1, Z_1), \quad \beta_1 = \beta(X_1, Z_1),$$

then for every $k \in \{1, 2, \dots, p\}$ we have

$$k(P_2 - P_1) + P_1 = \big(X_1 + k\alpha_1 p : 1 : Z_1 + k\beta_1 p\big),$$

which means that all the P_i's belong to the line in $\mathbb{P}^2(\mathbb{Z}/p^2\mathbb{Z})$ given by

$$\underbrace{-\beta_1}_{a} x + \underbrace{\big(\beta_1 X_1 - \alpha_1 Z_1\big)}_{b} y + \underbrace{\alpha_1}_{c} z \equiv 0 \bmod p^2. \tag{4.1}$$

This proves the inclusion $\mathcal{Q}_P \subseteq \pi^{-1}(P) \cap \mathcal{V}(ax + by + cz)$.

On the other side, let $(X : 1 : Z)$ a point over P satisfying the Equation (4.1). Since

$\pi(P_1) = \pi(X : 1 : Z)$, there are $s_x, s_z \in \mathbb{Z}$ such that

$$\begin{cases} X \equiv X_1 + s_x p \bmod p^2, \\ Z \equiv Z_1 + s_z p \bmod p^2, \end{cases}$$

which substituted in the above equation leads to

$$\alpha_1 s_z p \equiv \beta_1 s_x p \bmod p^2.$$

We observe that at least one between α_1 and β_1 needs to be coprime to p, otherwise every P_i would be equal to P_1. If $\gcd(\alpha_1, p) = 1$, the above equation gives

$$\begin{cases} X \equiv X_1 + s_x p \equiv X_1 + \frac{s_x}{\alpha_1}\alpha_1 p \bmod p^2, \\ Z \equiv Z_1 + s_z p \equiv Z_1 + \frac{\alpha_1 s_z p}{\alpha_1} \equiv Z_1 + \frac{s_x}{\alpha_1}\beta_1 p \bmod p^2, \end{cases}$$

therefore $(X : 1 : Z) = \frac{s_x}{\alpha_1}(P_2 - P_1) + P_1 \in \mathcal{Q}_P$. An analogous argument shows that if $\gcd(\beta_1, p) = 1$, then $(X : 1 : Z) = \frac{s_z}{\beta_1}(P_2 - P_1) + P_1 \in \mathcal{Q}_P$, proving the opposite inclusion $\pi^{-1}(P) \cap \mathcal{V}(ax + by + cz) \subseteq \mathcal{Q}_P$, from which the equality follows. □

Remark 4.5.3. We observe that the coefficients of the line determined by Theorem 4.5.2 are unique modulo p, but p^2 choices of these triples are possible inside $\mathbb{Z}/p^2\mathbb{Z}$. This is due to the definition of α_1 and β_1 in the above proof, that are easily seen to be uniquely defined only up to p-multiples.

4.5.2 Small anomalous loops

In this section we give a partial proof of Conjecture 3.5.4 in the case $e = 2$ and under an additional assumption.

Condition 4.5.4. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^2\mathbb{Z})$ be an anomalous loop. For every affine point $P \in \mathcal{E}_{A,B}(\mathbb{F}_p)$ we have*

$$|p \cdot \pi^{-1}(P)| > 1.$$

The above condition simply states that the multiplication-by-p does not map the fiber of an affine base point to a unique point at infinity.

It is needless to mention that, as Conjecture 3.5.4 implies Condition 4.5.4, neither we have found nor we expect to be there an example of an anomalous loop that does not satisfy it. As another piece of motivation, we have verified Condition 4.5.4 for every elliptic loop constructed over all the non-isomorphic anomalous elliptic curves that may be defined over $\mathbb{F}_p$, for every $p \in \mathcal{P}$ such that $p \leq 300$ [Appendix C.10].

Proposition 4.5.5. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^2\mathbb{Z})$ be an anomalous loop satisfying Condition 4.5.4. Then $\mathcal{L}$ has a unique split layer.*

Proof. Let $P = (X : 1 : Z) \in \mathcal{L}^a$ and define for every $k \in \{1, \dots, p\}$ the points

$$P_k = P + k(0 : 1 : p).$$

They all belong to different layers, as their differences lies in $\langle (0 : 1 : p) \rangle$, which has trivial intersection with any layer by Lemma 3.4.4. We also define

$$s_x = A^2Z^2 - AX^2 - 6BXZ, \qquad s_z = 2AXZ + 3BZ^2 + 1,$$

and we verify that

$$P_k = (X + ks_xp : 1 : Z + ks_zp).$$

It is easy to see that, since s_x and s_z appear only paired with p and vice versa, then for every $n \in \mathbb{Z}$ there are linear homogeneous forms $l_{n,x}, l_{n,y}, l_{n,z} \in \mathbb{Z}[x, z]$, which depends only on n and P, such that if $nP = (X_n : Y_n : Z_n)$ then

$$nP_k = \big(X_n + kl_{n,x}(s_x, s_z)p : Y_n + kl_{n,y}(s_x, s_z)p : Z_n + kl_{n,z}(s_x, s_z)p\big).$$

Since the loop is anomalous then $pP \in \mathcal{L}^\infty$, but pP also belongs to the same layer of P, therefore by Lemma 3.4.4 and Theorem 3.4.3 it lies inside $\langle (p : 1 : 0) \rangle$, as well as every pP_k. Thus, we have

$$pP = (X_p : 1 : 0) \in \mathbb{P}^2(\mathbb{Z}/p^2\mathbb{Z}), \quad \text{with } X_p \equiv 0 \bmod p,$$

which implies

$$pP_k = \big(X_p + kl_{p,x}(s_x, s_z)p : 1 + kl_{p,y}(s_x, s_z)p : 0\big) = \big(X_p + kl_{p,x}(s_x, s_z)p : 1 : 0\big).$$

Now we prove that $l_{p,x}(s_x, s_z) \not\equiv 0 \bmod p$ under Condition 4.5.4. In fact, if we had $l_{p,x}(s_x, s_z) \equiv 0 \bmod p$, then for every k we would get $pP = pP_k$. Since every P_k lies over $\pi(P)$ and by part (iii) of Proposition 3.3.13 every layer has precisely p points lying over $\pi(P)$, then the fiber of $\pi(P)$ in $\mathcal{L}$ is

$$\pi^{-1}\big(\pi(P)\big) = \{P_k + h(p : 1 : 0)\}_{1 \le k,h \le p}.$$

The addition law is associative inside layers $\big($Proposition 3.3.13-(ii)$\big)$, therefore we conclude

$$p\pi^{-1}\big(\pi(P)\big) = \{pP_k + hp(p : 1 : 0)\}_{1 \le k,h \le p} = \{pP\},$$

contradicting Condition 4.5.4.

Thus, if $l_{p,x}(s_x, s_z) \not\equiv 0 \bmod p$ we may define

$$m \equiv -\frac{X_p}{p}\big(l_{p,x}(s_x, s_z)\big)^{-1} \bmod p,$$

and we prove that $\mathbb{L}_m$ is the unique split layer of $\mathcal{L}$. Indeed, every P_k with $k \not\equiv m \bmod p$ has order p^2, since

$$pP_k = \big(X_p + kl_{p,x}(s_x, s_z)p : 1 : 0\big) = \left(\Big(\frac{X_p}{p} + kl_{p,x}(s_x, s_z)\Big)p : 1 : 0\right) \neq 0,$$

while every $P' \in \mathbb{L}_m$ has order p because it may be written for some $\alpha, \beta \in \{1, \dots, p\}$ as

$$P' = \alpha\big(P_m + \beta(p : 1 : 0)\big),$$

so that $pP' = \alpha pP_m + \beta p(p : 1 : 0) = \mathcal{O}$. □

4.5.3 Layers' maximality

In this section we prove that layers are maximal subgroups inside non-anomalous elliptic loops for the smallest non-trivial exponent. We just notice that this is a particular case of Conjecture 3.5.6.

Proposition 4.5.6. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^2\mathbb{Z})$ be an elliptic loop and $\mathbb{L}$ one of its layers. For every point $P \in \mathcal{L}$ there is a unique pair of points $(P_1, P_2) \in \mathbb{L} \times \langle (0:1:p) \rangle$ such that*

$$P = P_1 + P_2.$$

Proof. By Proposition 3.3.13-(iii) we may consider a point

$$P_{\mathbb{L}} \in \pi^{-1}\big(\pi(P)\big) \cap \mathbb{L}.$$

Since $\pi(P) = \pi(P_{\mathbb{L}})$, then $P - P_{\mathbb{L}} \in \mathcal{L}^{\infty}$ so by Theorem 3.4.3 there are $\alpha, \beta \in \{0, 1, \dots, p-1\}$ such that

$$P - P_{\mathbb{L}} = \alpha(p:1:0) + \beta(0:1:p).$$

By Lemma 4.4.2 we may associate

$$P = \big(\alpha(p:1:0) + \beta(0:1:p)\big) + P_{\mathbb{L}} = \beta(0:1:p) + \big(\alpha(p:1:0) + P_{\mathbb{L}}\big),$$

and $\alpha(p:1:0) + P_{\mathbb{L}} \in \mathbb{L}$ by Lemma 3.3.16.

An easy counting (applying Proposition 3.1.3 and 3.3.13, together with Theorem 3.4.3) gives

$$|\mathcal{L}| = p^2 |\mathcal{E}_{A,B}(\mathbb{F}_p)| = |\mathbb{L}|\ |\langle (0:1:p) \rangle| = |\mathbb{L} \times \langle (0:1:p) \rangle|,$$

from which uniqueness follows. □

From the above proposition, layers' maximality follows.

Corollary 4.5.7. *Let $\mathcal{L} = \mathcal{L}_{A,B}(\mathbb{Z}/p^2\mathbb{Z})$ be a non-exceptional elliptic loop and $\mathbb{L}$ be a layer of $\mathcal{L}$. If $G \subseteq \mathcal{L}$ is a subloop of $\mathcal{L}$ that is a group and $\mathbb{L} \subseteq G$, then $G = \mathbb{L}$.*

Proof. By Proposition 4.5.6, for every $P \in G$ we may write

$$P = \beta(p : 1 : 0) + P_{\mathbb{L}}$$

for some $\beta \in \{0, \dots, p-1\}$ and $P_{\mathbb{L}} \in \mathbb{L} \subseteq G$, so that

$$\beta(p : 1 : 0) = P - P_{\mathbb{L}} \in G.$$

If $\beta \neq 0$ then $(0 : 1 : p) \in G$, which implies by Proposition 4.5.6 that $G = \mathcal{L}$ so $\mathcal{L}$ is exceptional. Thus, we have $\beta = 0$, so $P \in \mathbb{L}$. Therefore we conclude that $G \subseteq \mathbb{L}$, from which $G = \mathbb{L}$ follows. □

This last result supports Conjecture 3.5.6, but does not prove it either in case $e = 2$, which is still open and requires further investigation.

CONCLUSIONS AND FURTHER WORK

In this work, we have defined and investigated elliptic loops as algebraic structures that enclose the behaviour of points lying above given elliptic curves over finite fields. Many objects of independent interest such as shadow curves and layers have seen the light and have been employed to study the geometry of these loops, which appears to be considerably more regular than what one could have expected.

A deeper inspection of these objects and their relation with the base curve is advised. Despite their construction in terms of the starting parameters is crystal-clear, no geometric connections among these entities are known.

Moreover, two relevant claims (Conjecture 3.5.4 and 3.5.6) arisen from the current investigation are still open and firmly demand further work to be better understood. They both seem to rely on a "lifting displacement" among layers, but a formal description of this behaviour is still considered challenging.

Furthermore, the results of this manuscript have always been presented without specializing the involved parameters, except for the exponent restraints considered in the final chapter. An intriguing line of work may consist of deriving stronger properties (e.g. associativity, substructures or discrete logarithm solution) when special values of $p, A, B \in \mathbb{Z}$ are chosen.

Finally, the choice of developing such a research on non-singular cubics is motivated by their wide interest and applications, but other types of abelian varieties might well be considered. As an instance, the case of conics is well-studied [70, Chapter VI] and had already seen cryptographical applications, such as RSA-like schemes built on Pell Hyperbolae [53, 6]. In the latter case, the group structure of these curves over $\mathbb{Z}/N\mathbb{Z}$ resembles that of elliptic ones, hinting at possible extensions of the current work to certain abelian varieties, whose addition laws display similar characteristics at infinity.

REFERENCES

[1] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen*, Math. Z. 19, pp. 207–246, 1924.

[2] M.F. Atiyah, I.G. MacDonald, *Introduction To Commutative Algebra*, Avalon Publishing, 1994.

[3] A.O.L. Atkin, F. Morain, *Elliptic Curves and Primality Proving*, Math. Comp. 61, pp. 29–68, 1993.

[4] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, F. Vercauteren, *Elliptic and Hyperelliptic Curve Cryptography: Theory and Practice*, CRC Press, 2005.

[5] H. Bass, *Algebraic K-theory*, Benjamin, 1968.

[6] E. Bellini, N. Murru, *An efficient and secure RSA-like cryptosystem exploiting Rédei rational functions over conics*, Finite Fields Appl. 39, pp. 179–194, 2016.

[7] I. Borosh, C.J. Moreno, H. Porta, *Elliptic Curves Over Finite Fields. II*, Math. Comp. 29, pp. 951–964, 1975.

[8] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24, pp. 235–265, 1997.

[9] W. Bosma, H.W. Lenstra, *Complete Systems of Two Addition Laws for Elliptic Curves*, J. Number Theory 53, pp. 229–240, 1995.

[10] W. Bosma, *Primality testing using elliptic curves*, Report 85–12, Mathematisch Instituut, Universiteit van Amsterdam, 1985.

[11] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over Q: wild 3-adic exercises*, J. Amer. Math. Soc. 14, pp. 843–939, 2001.

[12] W.C. Brown, *Matrices over commutative rings*, Marcel Dekker, 1993.

[13] J. Cassels, *Lectures on elliptic curves*, Cambridge Univ. Press, 1991.

[14] D.V. Chudnovsky, G.V. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests*, Adv. in Appl. Math. 7, pp. 385–434, 1986.

[15] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer Science &

Business Media, 2013.

[16] B. Conrad, F. Diamond, R. Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*, J. Amer. Math. Soc. 12, pp. 521–567, 1999.

[17] L. De Feo, D. Jao, J. Plût, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, IACR, 2011.

[18] M. Deuring, *Die Typen der Multiplikatoringe elliptischer Funktionenkörper*, Abh. Math. Sem. Univ. Hamburg 14, pp. 197–272, 1941.

[19] F. Diamond, *On deformation rings and Hecke rings*, Ann. of Math. (2) 144, pp. 137–166, 1996.

[20] S.D. Galbraith, *Elliptic Curve Paillier Schemes*, J. Cryptology 15, 2001.

[21] S. Goldwasser, J. Kilian, *Almost all primes can be quickly certified*, Proc. 18th Annual ACM Symp. on Theory of Computing, pp. 316–329, 1986.

[22] R. Gupta, M.R. Murty, *Cyclicity and generation of points mod p on elliptic curves*, Invent. Math. 101, pp. 225–235, 1990.

[23] H. Hasse, *Zur Theorie der abstrakten elliptischen Funktionenkörper*, J. Reine Angew. Math., 1936.

[24] T.L. Heath, *Diophantus of Alexandria: A Study in the History of Greek Algebra*, Cambridge University Press, 1910.

[25] K. Hensel, *Über eine neue Begründung der Theorie der algebraischen Zahlen*, Jahresber. Dtsch. Math.-Ver. 6, pp. 83–88, 1897.

[26] D. Husemöller, *Elliptic Curves*, Grad. Texts in Math. 111, Springer-Verlag, New York, 1987.

[27] N. Jacobson, *Basic Algebra I*, Dover Publications, 2009.

[28] N. Jacobson, *Basic Algebra II*, Dover Publications, 2009.

[29] D. Johnson, A. Menezes, S. Vanstone, *The Elliptic Curve Digital Signature Algorithm (ECDSA)*, Int. J. Inf. Secur., pp. 36–63, 2001.

[30] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. 109, pp. 221–229, 1992.

[31] S. Kamienny, B. Mazur, *Rational torsion of prime order in elliptic curves over number fields*, Astérisque 228, pp. 81–100, 1995.

[32] N. Koblitz, *Elliptic curve cryptosystems*, Math. Comp. 48, pp. 203–209, 1987.

[33] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Grad. Texts in Math. 97, Springer-Verlag, 1993.

[34] D.R. Kohel, I.E. Shparlinski, *On Exponential Sums and Group Generators for Elliptic Curves over Finite Fields*, Lecture Notes in Comput. Sci. 1838, pp. 395–404, 2000.

[35] K. Koyama, U.M. Maurer, T. Okamoto, S.A. Vanstone, *New Public-Key Schemes Based on Elliptic Curves over the Ring Z_n*, Advances in Cryptology, pp. 252–266, 1991.

[36] N. Kunihiro, K. Koyama, *Equivalence of Counting the Number of Points on Elliptic Curve over the Ring Z_n and Factoring n*, Advances in Cryptology, 1998.

[37] S. Lang, *Algebra*, Springer Science & Business Media, 2005.

[38] S. Lang, *Algebraic Number Theory*, Springer-Verlag, 1986.

[39] H. Lange, W. Ruppert, *Complete systems of addition laws on abelian varieties*, Invent. Math. 79, pp. 603–610, 1985.

[40] H. Lange, W. Ruppert, *Addition Laws on Elliptic Curves in Arbitrary Characteristics*, J. Algebra 107, pp. 106–116, 1987.

[41] C. Lara-Nino, A. Díaz-Pérez, M. Morales-Sandoval, *Elliptic Curve Lightweight Cryptography: a Survey*, IEEE Access, 2018.

[42] H.W. Lenstra, *Elliptic curves and number-theoretic algorithms*, Proc. of the International Congress of Mathematicians, pp. 99–120, 1986.

[43] H.W. Lenstra, *Factoring integers with elliptic curves*, Ann. of Math. (2) 126, pp. 649–673, 1987.

[44] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge University Press, 1997.

[45] A. Lozano-Robledo, *Elliptic Curves, Modular Forms, and Their L-functions*, American Mathematical Soc., 2011.

[46] J. Lubin, J.P. Serre, J. Tate, *Elliptic curves and formal groups*, American Mathematical Soc., 2011. Notes available on https://web.ma.utexas.edu/users/voloch/lst.html, 1964.

[47] S. Mac Lane, *Homology*, Springer-Verlag, 1994.

[48] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math.-Paris, 47, pp. 33–186, 1977.

[49] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. 44, pp. 129–162, 1978.

[50] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. 124, pp. 437–449, 1996.

[51] V.S. Miller, *Use of elliptic curves in cryptography*, Advances in Cryptology, pp. 417–426, 1985.

[52] L.J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Camb. Phil. Soc. 21, pp. 179–192, 1922.

[53] S. Padhye, *A public key cryptosystem based on Pell equation*, IACR 191, 2006.

[54] H.G. Rück, *A Note on Elliptic Curves Over Finite Fields*, Math. Comp. 49, pp. 301–304, 1987.

[55] H.G. Rück, *On the discrete logarithm in the divisor class group of curves*, Math. Comp. 68, pp. 805–806, 1999.

[56] T. Satoh, K. Araki, *Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves*, Comm. Math. Univ. St. Pauli 47(1), pp. 81–92, 1998.

[57] T. Satoh, K. Araki, *Errata to the paper: Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves (published in Comm. Math. Univ. St. Pauli, 47(1), pp. 81–92, 1998)*, Comm. Math. Univ. St. Pauli 48, pp. 211–213, 1999.

[58] R. Schoof, *Counting points on elliptic curves over finite fields*, J. Theor. Nombr. Bordx. 7, pp. 219–254, 1995.

[59] R. Schoof, *Elliptic Curves over Finite Fields and the Computation of Square Roots mod p*, Math. Comp. 44, pp. 483–494, 1985.

[60] R. Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory 46, pp. 183–211, 1987.

[61] I.A. Semaev, *Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p*, Math. Comp. 67, pp. 353–356, 1998.

[62] R.D. Schafer, *An introduction to nonassociative algebras*, Academic Press, 1966.

[63] C.P. Schnorr, *Efficient signature generation by smart cards*, J. Cryptology 4, pp. 161–174, 1991.

[64] I.E. Shparlinski, *Pseudorandom number generators from elliptic curves* Contemporary

Mathematics 477, pp. 121-142, 2009.

[65] I.E. Shparlinski, J.F. Voloch, *Generators of elliptic curves over finite fields*, Bull. Inst. Math. Acad. Sin. (N.S.) 9, pp. 657–670, 2014.

[66] J.H. Silverman, *Lifting and Elliptic Curve Discrete Logarithms*, SAC, pp. 82–102, 2008.

[67] J.H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, 1986.

[68] N. Smart, *The discrete logarithm on elliptic curves of trace one*, J. Cryptology 12, pp. 193–196, 1999.

[69] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) 141, pp. 553–572, 1995.

[70] O. Veblen, J.W. Young, *Projective Geometry. I* Boston Ginn and Co., 1918.

[71] S.G. Vlădut, *On the Cyclicity of Elliptic Curves over Finite Field Extensions*, Finite Fields Appl. 5, pp. 354–363, 1999.

[72] J.F. Voloch, *A note on elliptic curves over finite fields*, Bull. Soc. Math. France 116, pp. 455-458, 1988.

[73] J.F. Voloch, *The discrete logarithm problem on elliptic curves and descents*, preprint available at `https://web.ma.utexas.edu/users/voloch/oldpreprint.html`.

[74] L.C. Washington, *Elliptic curves, number theory and cryptography*, Chapman & Hall / CRC, 2008.

[75] W.C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. 2, pp. 521–560, 1969.

[76] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. of Math. (2) 142, pp. 443–551, 1995.

[77] NASA Advanced Supercomputing Division, *NAS Technical Report - NAS-03-012*, 2003.

APPENDICES

The following appendices are devoted to verifying some tedious computations involved in proofs from the current work, in order not to pointlessly weighing down the reading.

Only exact (i.e. without any approximations) and directly verifiable statements are presented, they are just overly heavy to be performed directly.

These tasks are accomplished by exploiting the Magma software [8]. The bulk of the code is intended to produce the reported output in a working Magma environment supporting or compatible with *Magma V2.24-8*.

The code is designed to perform the prescribed computations within few minutes on a personal computer, with the only exceptions of Appendix C.9, which is memory intensive, and Appendix C.2, which is highly time-consuming. A server is advised to run such parts: our results have been obtained on the *Noether1* server of University of Trento, running *Magma V2.22-5*.

The expected outputs and the running time, if critical, have been included to assist the verification process.

APPENDIX A
ADDITION LAWS

Here we verify the computations involved in the proof of Proposition 2.2.11. We begin with the definition of the involved objects.

```
S< A,B, x1,y1,z1, x2,y2,z2, x3,y3,z3 > := PolynomialRing(Integers(),11);
J := ideal< S | y1^2*z1 - x1^3 - A*x1*z1^2 - B*z1^3,
                y2^2*z2 - x2^3 - A*x2*z2^2 - B*z2^3,
                y3^2*z3 - x3^3 - A*x3*z3^2 - B*z3^3 >;
```

We define the two addition laws $+_{(0:0:1)}$ and $+_{(0:1:0)}$.

```
// (0:0:1)
function AL1(A,B, x1,y1,z1, x2,y2,z2)
    local X1,Y1,Z1;
    X1 := ( (x1*y2 - x2*y1)*(y1*z2 + y2*z1) + (x1*z2 - x2*z1)*y1*y2 - A*(x1*z2 +
     x2*z1)*(x1*z2 - x2*z1) - 3*B*(x1*z2 -x2*z1)*z1*z2 );
    Y1 := ( -3*x1*x2*(x1*y2 - x2*y1) - y1*y2*(y1*z2 - y2*z1) - A*(x1*y2 - x2*y1)
   *z1*z2 + A*(x1*z2 + x2*z1)*(y1*z2 - y2*z1) + 3*B*(y1*z2 - y2*z1)*z1*z2 );
    Z1 := ( 3*x1*x2*(x1*z2 - x2*z1) - (y1*z2 + y2*z1)*(y1*z2 - y2*z1) + A*(x1*z2
     - x2*z1)*z1*z2 );
    return X1,Y1,Z1;
end function;


// (0:1:0)
function AL2(A,B, x1,y1,z1, x2,y2,z2)
    local X2,Y2,Z2;
    X2 := ( y1*y2*(x1*y2 + x2*y1) - A*x1*x2*(y1*z2 + y2*z1) - A*(x1*y2 + x2*y1)
   *(x1*z2 + x2*z1) - 3*B*(x1*y2 + x2*y1)*z1*z2 - 3*B*(x1*z2 + x2*z1)*(y1*z2 +
   y2*z1) + A^2 *(y1*z2 + y2*z1)*z1*z2 );
    Y2 := ( y1^2*y2^2 + 3*A*x1^2*x2^2 + 9*B*x1*x2*(x1*z2 + x2*z1) - A^2*x1*z2*(
   x1*z2 + 2*x2*z1) - A^2*x2*z1*(2*x1*z2 + x2*z1) - 3*A*B*z1*z2*(x1*z2 + x2*z1)
```

```
     - (A^3 + 9*B^2)*z1^2*z2^2 );
    Z2 := ( 3*x1*x2*(x1*y2 + x2*y1) + y1*y2*(y1*z2 + y2*z1) + A*(x1*y2 + x2*y1)*
   z1*z2 + A*(x1*z2 + x2*z1)*(y1*z2 + y2*z1) + 3*B*(y1*z2 + y2*z1)*z1*z2 );
    return X2,Y2,Z2;
end function;
```

The following functions are used to check if two triples $(X1, Y1, Z1)$ and $(X2, Y2, Z2)$ agree in $\mathbb{P}^2(S/J)$, i.e. to test whether $[X, Y],\ [X, Z],\ [Y, Z] \in J$.

```
function Comm(V,W)
    return V[1]*W[2] - V[2]*W[1];
end function;


function ProjAgree(X1,Y1,Z1, X2,Y2,Z2)
    if Comm([X1,Y1],[X2,Y2]) in J and Comm([X1,Z1],[X2,Z2]) in J and Comm([Y1,Z1
   ],[Y2,Z2]) in J then
        return true;
    else
        return false;
    end if;
end function;
```

A.1 DEFINITION

We show that the + operation is well-defined, i.e. that $+_{(0:0:1)}$ agrees with $+_{(0:1:0)}$.

```
X1,Y1,Z1 := AL1(A,B, x1,y1,z1, x2,y2,z2);
X2,Y2,Z2 := AL2(A,B, x1,y1,z1, x2,y2,z2);
ProjAgree(X1,Y1,Z1, X2,Y2,Z2);
> true
```

A.2 GROUP

We check that all the group conditions are satisfied.

[Closure]

```
X1,Y1,Z1 := AL1(A,B, x1,y1,z1, x2,y2,z2);
X2,Y2,Z2 := AL2(A,B, x1,y1,z1, x2,y2,z2);

Y1^2*Z1 - X1^3 - A*X1*Z1^2 - B*Z1^3 in J;
> true
Y2^2*Z2 - X2^3 - A*X2*Z2^2 - B*Z2^3 in J;
> true
```

[Commutativity]

```
X1a,Y1a,Z1a := AL1(A,B, x1,y1,z1, x2,y2,z2);
X1b,Y1b,Z1b := AL1(A,B, x2,y2,z2, x1,y1,z1);

X2a,Y2a,Z2a := AL2(A,B, x1,y1,z1, x2,y2,z2);
X2b,Y2b,Z2b := AL2(A,B, x2,y2,z2, x1,y1,z1);

ProjAgree(X1a,Y1a,Z1a, X1b,Y1b,Z1b);
> true
ProjAgree(X2a,Y2a,Z2a, X2b,Y2b,Z2b);
> true
```

[Associativity]

```
// I.
X1A,Y1A,Z1A := AL1(A,B, x1,y1,z1, x2,y2,z2);
AssX1A, AssY1A, AssZ1A := AL1(A,B, X1A,Y1A,Z1A, x3,y3,z3);

X2A,Y2A,Z2A := AL2(A,B, x1,y1,z1, x2,y2,z2);
AssX2A, AssY2A, AssZ2A := AL2(A,B, X2A,Y2A,Z2A, x3,y3,z3);

// II.
X1B,Y1B,Z1B := AL1(A,B, x2,y2,z2, x3,y3,z3);
AssX1B, AssY1B, AssZ1B := AL1(A,B, x1,y1,z1, X1B,Y1B,Z1B);

X2B,Y2B,Z2B := AL2(A,B, x2,y2,z2, x3,y3,z3);
```

```
AssX2B, AssY2B, AssZ2B := AL2(A,B, x1,y1,z1, X2B,Y2B,Z2B);


ProjAgree(AssX1A,AssY1A,AssZ1A, AssX1B,AssY1B,AssZ1B);
> true
ProjAgree(AssX2A,AssY2A,AssZ2A, AssX2B,AssY2B,AssZ2B);
> true
```

[Identity]

```
x10,y10,z10 := AL1(A,B, x1,y1,z1, 0,1,0);
x20,y20,z20 := AL2(A,B, x1,y1,z1, 0,1,0);


ProjAgree(x1,y1,z1, x10,y10,z10);
> true
ProjAgree(x1,y1,z1, x20,y20,z20);
> true
```

[Inverse]

```
x1e,y1e,z1e := AL1(A,B, x1,y1,z1, x1,-y1,z1);
x2e,y2e,z2e := AL2(A,B, x1,y1,z1, x1,-y1,z1);


ProjAgree(x1e,y1e,z1e, 0,1,0);
> true
ProjAgree(x2e,y2e,z2e, 0,1,0);
> true
```

APPENDIX B
LOOP PROPERTIES

In this appendix we expand on the computations of Chapter 3. First, we define the points sum and the commutator functions.

```
function Sum(A,B, x1,y1,z1, x2,y2,z2)
    local X2,Y2,Z2;
    X2 := ( y1*y2*(x1*y2 + x2*y1) - A*x1*x2*(y1*z2 + y2*z1) - A*(x1*y2 + x2*y1)
    *(x1*z2 + x2*z1) - 3*B*(x1*y2 + x2*y1)*z1*z2 - 3*B*(x1*z2 + x2*z1)*(y1*z2 +
    y2*z1) + A^2 *(y1*z2 + y2*z1)*z1*z2 );
    Y2 := ( y1^2*y2^2 + 3*A*x1^2*x2^2 + 9*B*x1*x2*(x1*z2 + x2*z1) - A^2*x1*z2*(
    x1*z2 + 2*x2*z1) - A^2*x2*z1*(2*x1*z2 + x2*z1) - 3*A*B*z1*z2*(x1*z2 + x2*z1)
     - (A^3 + 9*B^2)*z1^2*z2^2 );
    Z2 := ( 3*x1*x2*(x1*y2 + x2*y1) + y1*y2*(y1*z2 + y2*z1) + A*(x1*y2 + x2*y1)*
    z1*z2 + A*(x1*z2 + x2*z1)*(y1*z2 + y2*z1) + 3*B*(y1*z2 + y2*z1)*z1*z2 );
    return X2,Y2,Z2;
end function;


function Comm(V,W)
    return V[1]*W[2] - V[2]*W[1];
end function;
```

B.1 INVERSE

Here we verify that in any elliptic loop the inverse element is unique, as stated in Proposition 3.2.3.

```
Z< t > := FunctionField(Integers());
S< A,B, x1,y1,z1, x2,y2,z2 > := PolynomialRing(Z,8);


X,Y,Z := Sum(A,B, x1,y1,z1, x2,y2,z2);
I := ideal< S | [X,Y-t,Z] >;
```

```
x1*y2+x2*y1 in I;
> true
z1*y2+z2*y1 in I;
> true
```

B.2 WEAK ASSOCIATIVITY

Here we prove the weak associtativity property of Lemma 3.3.2.

```
S< A,B, x1,y1,z1, x2,y2,z2 > := PolynomialRing(Integers(),8);
P := [x1,y1,z1]; Q := [x2,y2,z2];

X,Y,Z := Sum(A,B, Q[1],Q[2],Q[3], P[1],-P[2],P[3]); // Q - P
QmP := [X,Y,Z];

X,Y,Z := Sum(A,B, P[1],P[2],P[3], QmP[1],QmP[2],QmP[3]); // P + (Q - P)
Su := [X,Y,Z];

(Su[1] div Q[1]) eq (Su[2] div Q[2]);
> true
(Su[1] div Q[1]) eq (Su[3] div Q[3]);
> true
```

B.3 ASSOCIATIVITY

In this part we perform the computationally heavy check involved in the proof of Theorem 3.3.7. We begin by verifying that the commutators c_i belong to the ideal generated by the 2×2-minors.

```
S< x1,y1,z1, x2,y2,z2, x3,y3,z3, A,B > := PolynomialRing(Integers(),11);
// Notice: Here A,B are considered as last variables to speed up the following
    computations. The same check may result infeasible with a personal computer
    when other variables orders are considered.
```

```
SXYZ< X,Y,Z > := PolynomialRing(S,3);

F := X^3 + A*X*Z^2 + B*Z^3 - Y^2*Z;
G := A^2*Z^3 - 3*A*X^2*Z - 9*B*X*Z^2 - 3*X*Y^2;

X1,Y1,Z1 := Sum(A,B, x1,y1,z1, x2,y2,z2); // P+Q
X1,Y1,Z1 := Sum(A,B, X1,Y1,Z1, x3,y3,z3); // (P+Q)+R

X2,Y2,Z2 := Sum(A,B, x2,y2,z2, x3,y3,z3); // Q+R
X2,Y2,Z2 := Sum(A,B, x1,y1,z1, X2,Y2,Z2); // P+(Q+R)

c1 := Comm([X1,Y1],[X2,Y2]);
c2 := Comm([X1,Z1],[X2,Z2]);
c3 := Comm([Y1,Z1],[Y2,Z2]);

Minor1 := Comm( [ Evaluate(F,[x1,y1,z1]), Evaluate(F,[x2,y2,z2]) ],
                [ Evaluate(G,[x1,y1,z1]), Evaluate(G,[x2,y2,z2]) ] );
Minor2 := Comm( [ Evaluate(F,[x1,y1,z1]), Evaluate(F,[x3,y3,z3]) ],
                [ Evaluate(G,[x1,y1,z1]), Evaluate(G,[x3,y3,z3]) ] );
Minor3 := Comm( [ Evaluate(F,[x2,y2,z2]), Evaluate(F,[x3,y3,z3]) ],
                [ Evaluate(G,[x2,y2,z2]), Evaluate(G,[x3,y3,z3]) ] );

I := ideal< S | [Minor1,Minor2,Minor3] >;

c1 in I;
> true
c2 in I;
> true
c3 in I;
> true
```

Now we verify the part (ii), i.e. we check that the minors ideal of order 1 and 2 of the left-hand side matrix are contained in those of the right-hand side one.

```
P := [x1,y1,z1];
Q1 := [x2,y2,z2];
Q2 := [x3,y3,z3];
Xt,Yt,Zt := Sum(A,B, Q1[1],Q1[2],Q1[3], Q2[1],Q2[2],Q2[3]); // P+Q
Q1Q2 := [Xt,Yt,Zt];
```

[1 × 1 minors, i.e. entries]

We prove a stronger statement, i.e. we show that $F(Q_1 + Q_2) \in \langle F(Q_1), F(Q_2)\rangle$ and $G(Q_1 + Q_2) \in \langle G(Q_1), G(Q_2)\rangle$. This is not sterile virtuosity: with a personal computer, directly checking the whole ideal containment would be unfeasible.

```
g1 := Evaluate(F,Q1Q2);
g2 := Evaluate(G,Q1Q2);
IF := ideal< S | [Evaluate(F,Q1), Evaluate(F,Q2)] >;
IG := ideal< S | [Evaluate(G,Q1), Evaluate(G,Q2)] >;


g1 in IF;
> true
g2 in IG;
> true
```

[2 × 2 minors]

```
Minor1 := Comm( [ Evaluate(F,P), Evaluate(F,Q1) ],
                [ Evaluate(G,P), Evaluate(G,Q1) ] );
Minor2 := Comm( [ Evaluate(F,P), Evaluate(F,Q2) ],
                [ Evaluate(G,P), Evaluate(G,Q2) ] );
Minor3 := Comm( [ Evaluate(F,Q1), Evaluate(F,Q2) ],
                [ Evaluate(G,Q1), Evaluate(G,Q2) ] );


g := Comm( [ Evaluate(F,P), Evaluate(F,Q1Q2) ],
           [ Evaluate(G,P), Evaluate(G,Q1Q2) ] );
```

```
g in ideal< S | [Minor1,Minor2,Minor3] >;
> true
```

B.4 SHADOW CURVE

This part is devoted to verifying the computational part of Section 3.3.3. They both make use of the addition laws introduced in Section 1.2.

```
// (0:0:1)
function AL1(A,B, x1,y1,z1, x2,y2,z2)
    local X1,Y1,Z1;
    X1 := ( (x1*y2 - x2*y1)*(y1*z2 + y2*z1) + (x1*z2 - x2*z1)*y1*y2 - A*(x1*z2 +
     x2*z1)*(x1*z2 - x2*z1) - 3*B*(x1*z2 -x2*z1)*z1*z2 );
    Y1 := ( -3*x1*x2*(x1*y2 - x2*y1) - y1*y2*(y1*z2 - y2*z1) - A*(x1*y2 - x2*y1)
    *z1*z2 + A*(x1*z2 + x2*z1)*(y1*z2 - y2*z1) + 3*B*(y1*z2 - y2*z1)*z1*z2 );
    Z1 := ( 3*x1*x2*(x1*z2 - x2*z1) - (y1*z2 + y2*z1)*(y1*z2 - y2*z1) + A*(x1*z2
     - x2*z1)*z1*z2 );
    return X1,Y1,Z1;
end function;

// (0:1:0)
function AL2(A,B, x1,y1,z1, x2,y2,z2)
    local X2,Y2,Z2;
    X2 := ( y1*y2*(x1*y2 + x2*y1) - A*x1*x2*(y1*z2 + y2*z1) - A*(x1*y2 + x2*y1)
    *(x1*z2 + x2*z1) - 3*B*(x1*y2 + x2*y1)*z1*z2 - 3*B*(x1*z2 + x2*z1)*(y1*z2 +
    y2*z1) + A^2 *(y1*z2 + y2*z1)*z1*z2 );
    Y2 := ( y1^2*y2^2 + 3*A*x1^2*x2^2 + 9*B*x1*x2*(x1*z2 + x2*z1) - A^2*x1*z2*(
    x1*z2 + 2*x2*z1) - A^2*x2*z1*(2*x1*z2 + x2*z1) - 3*A*B*z1*z2*(x1*z2 + x2*z1)
     - (A^3 + 9*B^2)*z1^2*z2^2 );
    Z2 := ( 3*x1*x2*(x1*y2 + x2*y1) + y1*y2*(y1*z2 + y2*z1) + A*(x1*y2 + x2*y1)*
    z1*z2 + A*(x1*z2 + x2*z1)*(y1*z2 + y2*z1) + 3*B*(y1*z2 + y2*z1)*z1*z2 );
    return X2,Y2,Z2;
```

```
end function;
```

First, we perform the computational tasks required by Proposition 3.3.10.

```
S<A,B, x,y,z> := PolynomialRing(Integers(),5);

F := x^3 + A*x*z^2 + B*z^3 - y^2*z;
G := A^2*z^3 - 3*A*x^2*z - 9*B*x*z^2 - 3*x*y^2;
I := ideal< S | [F,G] >;

// The addition laws that are non-exceptional for point doubling are those
    corresponding to points with non-zero y coordinate. Hence, only AL1 will be
    used for evaluating 2P.
X2,Y2,Z2 := AL2(A,B, x,y,z, x,y,z);

// (S1:S2:S3) = (2P) + P  -  version a
S1a,S2a,S3a := AL1(A,B, x,y,z, X2,Y2,Z2);
// (S1:S2:S3) = (2P) + P  -  version b
S1b,S2b,S3b := AL2(A,B, x,y,z, X2,Y2,Z2);

S1a in I and S3a in I;
> true
S1b in I and S3b in I;
> true
```

Then, the verification employed by Proposition 3.3.11. First, for general (i.e. possibly not invertible) integers $\alpha \in \mathbb{Z}$.

```
S< A,B, x1,y1,z1, x2,y2,z2, a,b > := PolynomialRing(Integers(),10);
SXYZ< X,Y,Z > := PolynomialRing(S,3);

F := X^3 + A*X*Z^2 + B*Z^3 - Y^2*Z;
G := A^2*Z^3 - 3*A*X^2*Z - 9*B*X*Z^2 - 3*X*Y^2;
```

```
P := [x1,y1,z1];
Q := [x2,y2,z2];

PQx,PQy,PQz := AL1(A,B, x1,y1,z1, x2,y2,z2);
PQ1 := [PQx,PQy,PQz];
PQx,PQy,PQz := AL2(A,B, x1,y1,z1, x2,y2,z2);
PQ2 := [PQx,PQy,PQz];

I := ideal< S | [Evaluate(a*F-b*G,P),Evaluate(a*F-b*G,Q)] >;
J := ideal< S | [Evaluate(a*F-b*G,PQ1),Evaluate(a*F-b*G,PQ2)] >;

J subset I;
> true
```

As for the “moreover” part, we consider $\alpha \in \mathbb{Z}$ invertible.

```
PreS<a> := FunctionField(Integers(), 1);
S< x1,y1,z1, x2,y2,z2, x3,y3,z3, b, A,B > := PolynomialRing(PreS,12);
SXYZ< X,Y,Z > := PolynomialRing(S,3);
F := X^3 + A*X*Z^2 + B*Z^3 - Y^2*Z;
G := A^2*Z^3 - 3*A*X^2*Z - 9*B*X*Z^2 - 3*X*Y^2;

P := [x1,y1,z1]; Q := [x2,y2,z2]; R := [x3,y3,z3];
J := ideal< S | [Evaluate(a*F-b*G,P), Evaluate(a*F-b*G,Q), Evaluate(a*F-b*G,R)]
   >;

function Comm(V,W)
    return V[1]*W[2] - V[2]*W[1];
end function;

function ProjAgree(X1,Y1,Z1, X2,Y2,Z2)
        if Comm([X1,Y1],[X2,Y2]) in J and Comm([X1,Z1],[X2,Z2]) in J and Comm([
   Y1,Z1],[Y2,Z2]) in J then
```

```
                return true;
        else
                return false;
        end if;
end function;

X1,Y1,Z1 := AL1(A,B, x1,y1,z1, x2,y2,z2);
X2,Y2,Z2 := AL2(A,B, x1,y1,z1, x2,y2,z2);

ProjAgree(X1,Y1,Z1, X2,Y2,Z2);
> true

AssX1A, AssY1A, AssZ1A := AL1(A,B, X1,Y1,Z1, x3,y3,z3);
AssX2A, AssY2A, AssZ2A := AL2(A,B, X1,Y1,Z1, x3,y3,z3);

tmpX1, tmpY1, tmpZ1 := AL1(A,B, x2,y2,z2, x3,y3,z3);
tmpX2, tmpY2, tmpZ2 := AL2(A,B, x2,y2,z2, x3,y3,z3);

AssX1B, AssY1B, AssZ1B := AL1(A,B, x1,y1,z1, tmpX1,tmpY1,tmpZ1);
AssX2B, AssY2B, AssZ2B := AL2(A,B, x1,y1,z1, tmpX2,tmpY2,tmpZ2);

ProjAgree(AssX1A,AssY1A,AssZ1A, AssX1B,AssY1B,AssZ1B);
> true
ProjAgree(AssX2A,AssY2A,AssZ2A, AssX2B,AssY2B,AssZ2B);
> true
```

APPENDIX C
SMALL EXPONENTS

Here we perform the computations involved in Chapter 4. We recall the `Sum` function, which will be used all along this appendix. For our convenience, unlike the addition laws employed in previous appendices, now this function returns triples.

```
function Sum(A,B, x1,y1,z1, x2,y2,z2)
  local X2,Y2,Z2;
  X2 := ( y1*y2*(x1*y2 + x2*y1) - A*x1*x2*(y1*z2 + y2*z1) - A*(x1*y2 + x2*y1)
  *(x1*z2 + x2*z1) - 3*B*(x1*y2 + x2*y1)*z1*z2 - 3*B*(x1*z2 + x2*z1)*(y1*z2 +
  y2*z1) + A^2 *(y1*z2 + y2*z1)*z1*z2 );
  Y2 := ( y1^2*y2^2 + 3*A*x1^2*x2^2 + 9*B*x1*x2*(x1*z2 + x2*z1) - A^2*x1*z2*(
  x1*z2 + 2*x2*z1) - A^2*x2*z1*(2*x1*z2 + x2*z1) - 3*A*B*z1*z2*(x1*z2 + x2*z1)
   - (A^3 + 9*B^2)*z1^2*z2^2 );
  Z2 := ( 3*x1*x2*(x1*y2 + x2*y1) + y1*y2*(y1*z2 + y2*z1) + A*(x1*y2 + x2*y1)*
  z1*z2 + A*(x1*z2 + x2*z1)*(y1*z2 + y2*z1) + 3*B*(y1*z2 + y2*z1)*z1*z2 );
  return [X2,Y2,Z2];
end function;
```

C.1 NON-ASSOCIATIVITY FOR $e \geq 3$

This section is devoted to perform the calculations used by Lemma 4.1.1.

```
S< p, A,B, X,Y > := PolynomialRing(Integers(), 5);


P1 := [X,Y,1];
P2 := [p,1,p];
P3 := [0,1,p];


P12 := Sum( A,B, P1[1],P1[2],P1[3], P2[1],P2[2],P2[3] );
SS := Sum( A,B, P12[1],P12[2],P12[3], P3[1],P3[2],P3[3] );
```

```
P23 := Sum( A,B, P2[1],P2[2],P2[3], P3[1],P3[2],P3[3] );
TT := Sum( A,B, P1[1],P1[2],P1[3], P23[1],P23[2],P23[3] );

c1 := SS[1]*TT[2] - SS[2]*TT[1];
c2 := SS[1]*TT[3] - SS[3]*TT[1];
c3 := SS[2]*TT[3] - SS[3]*TT[2];

c1 := &+[m : m in Terms(c1) | Degree(m,p) lt 3];
c2 := &+[m : m in Terms(c2) | Degree(m,p) lt 3];
c3 := &+[m : m in Terms(c3) | Degree(m,p) lt 3];

I := ideal< S | c1,c2,c3 >;

54*Y^3*B*(B-2*X^3)^4*p^2 in I;
> true
54*Y^3*(96*A*X^10 - 3*B^4 + 26*B^3*X^3 - 92*B^2*X^6 + 248*B*X^9)*p^2 in I;
> true
```

C.2 ELLIPTIC GROUPS

In this section we check that anomalous elliptic loops are non-cyclic groups, as claimed by Proposition 4.1.3. The larger cases of these computation ($p = 13$) may last for several days on a personal laptop.

```
Parameters := [ [5,4,2], [5,4,3], [7,0,4], [7,0,2], [13,0,3], [13,0,10] ];
for par in Parameters do
    p := par[1];
    A := par[2];
    B := par[3];
    Laff := [ [X,Y,1] : X,Y in [0..p^2-1] | (-Y^2 + X^3 + A*X + B) mod p eq 0 ];
    Linf := [ [a*p,1,b*p] : a,b in [0..p-1] ];
    L := Laff cat Linf;
    res := true;
    time for P,Q,R in L do
        PQ := Sum(A,B, P[1],P[2],P[3], Q[1],Q[2],Q[3]);
        PQRa := Sum(A,B, PQ[1],PQ[2],PQ[3], R[1],R[2],R[3]);
        QR := Sum(A,B, Q[1],Q[2],Q[3], R[1],R[2],R[3]);
        PQRb := Sum(A,B, P[1],P[2],P[3], QR[1],QR[2],QR[3]);

        c1 := (PQRa[1]*PQRb[2] - PQRa[2]*PQRb[1]) mod p^2;
        c2 := (PQRa[1]*PQRb[3] - PQRa[3]*PQRb[1]) mod p^2;
        c3 := (PQRa[2]*PQRb[3] - PQRa[3]*PQRb[2]) mod p^2;

        if not( c1 eq 0 and c2 eq 0 and c3 eq 0) then
            res := false;
            break P;
        end if;
    end for;
    par, res;
end for;
> Time: 22.470
> [ 5, 4, 2 ]
> true
> Time: 22.700
> [ 5, 4, 3 ]
> true
> Time: 151.830
> [ 7, 0, 4 ]
> true
> Time: 4018.330
> [7, 0, 2]
> true
> Time: 190043.830
> [13, 0, 3]
> true
> Time: 201058.250
> [13, 0, 10]
> true
```

Now we prove these groups are not cyclic by proving that, every point of $\mathcal{L}_{A,B}(\mathbb{Z}/p^2\mathbb{Z})$ is of $(3p)$-torsion.

```
Parameters := [ [5,4,2], [5,4,3], [7,0,4], [7,0,2], [13,0,3], [13,0,10] ];
for par in Parameters do
    p := par[1];
    A := par[2];
    B := par[3];
    Laff := [ [X,Y,1] : X,Y in [0..p^2-1] | (-Y^2 + X^3 + A*X + B) mod p eq 0 ];
    Linf := [ [a*p,1,b*p] : a,b in [0..p-1] ];
    L := Laff cat Linf;
    res := true;
    for P in L do
        sum := P;
        for i in [2..3*p] do
            sum := Sum(A,B, P[1],P[2],P[3], sum[1] mod p^2,sum[2] mod p^2,sum[3]
     mod p^2);
        end for;

        if not( sum[1] mod p^2 eq 0 and sum[3] mod p^2 eq 0 ) then
            res := false;
            break P;
        end if;
    end for;
    par, res;
end for;
> [ 5, 4, 2 ]
> true
> [ 5, 4, 3 ]
> true
> [ 7, 0, 4 ]
> true
> [7, 0, 2]
> true
> [13, 0, 3]
> true
> [13, 0, 10]
> true
```

C.3 CONDITIONED NON-ASSOCIATIVITY FOR $e \geq 2$

In this section we detail the computations of Proposition 4.1.5.

```
S< p, A,B, X,Y > := PolynomialRing(Integers(), 5);

P1 := [X,Y,1];
P2 := [X,Y+p,1];
P3 := [0,1,p];

P12 := Sum( A,B, P1[1],P1[2],P1[3], P2[1],P2[2],P2[3] );
SS := Sum( A,B, P12[1],P12[2],P12[3], P3[1],P3[2],P3[3] );

P23 := Sum( A,B, P2[1],P2[2],P2[3], P3[1],P3[2],P3[3] );
TT := Sum( A,B, P1[1],P1[2],P1[3], P23[1],P23[2],P23[3] );

c1 := SS[1]*TT[2] - SS[2]*TT[1];
c3 := SS[2]*TT[3] - SS[3]*TT[2];

c1 := &+[m : m in Terms(c1) | Degree(m,p) lt 2];
c3 := &+[m : m in Terms(c3) | Degree(m,p) lt 2];
```

```
F1 := A^2 - 3*A*X^2 - 9*B*X - 3*X*Y^2;
F2 := A^3 + 6*A^2*X^2 + 6*A*B*X - 3*A*X^4 + 9*B^2 - 18*B*X^3 - Y^4;
G1 := 10*A^4*X + 9*A^3*B + 2*A^3*Y^2 - 30*A^2*B*X^2 + 6*A^2*X^5 + 6*A^2*X^2*Y^2
    + 45*A*B^2*X + 45*A*B*X^4 + 9*A*B*X*Y^2 + 54*B^3 + 135*B^2*X^3 + 18*B^2*Y^2
    - 9*B*X^3*Y^2;
G2 := 2*A^4 - 15*A^2*B*X + 30*A^2*X^4 + 6*A^2*X*Y^2 + 9*A*B^2 + 90*A*B*X^3 + 3*A
    *B*Y^2 - 6*A*X^3*Y^2 + 135*B^2*X^2 - 27*B*X^5 - 27*B*X^2*Y^2;

c1 eq 2*p*Y^2*F1*F2*G1;
> true
c3 eq 2*p*Y^2*F1*F2*G2;
> true

ExtS<x,y,z> := PolynomialRing(S,3);
F := x^3+A*x*z^2+B*z^3-y^2*z;

// Case I

dP1 := Sum( A,B, P1[1],P1[2],P1[3], P1[1],P1[2],P1[3] );
tP1 := Sum( A,B, dP1[1],dP1[2],dP1[3], P1[1],P1[2],P1[3] );
tP1 := [ &+[m : m in Terms(tP1[i]) | Degree(m,p) lt 2] : i in [1..3]];

I3 := ideal< S | Evaluate(F,P1), F1 >;

tP1[1] in I3;
> true
tP1[3] in I3;
> true

// Case II
```

```
dP1 := Sum( A,B, P1[1],P1[2],P1[3], P1[1],P1[2],P1[3] );
qP1 := Sum( A,B, dP1[1],dP1[2],dP1[3], dP1[1],dP1[2],dP1[3] );
qP1 := [ &+[m : m in Terms(qP1[i]) | Degree(m,p) lt 2] : i in [1..3]];

I4 := ideal< S | Evaluate(F,P1), F2 >;

qP1[1] in I4;
> true
qP1[3] in I4;
> true

// Case III

I := ideal<S | Evaluate(F,P1), G1, G2 >;

864*(X^3*Y^10 - Y^12) in I;
> true
288*(B*Y^8 - 2*X^3*Y^8 + 2*Y^10) in I;
> true
```

C.4 INFINITY PART

In this section we deal with the computations of Proposition 4.2.1 and Lemma 4.2.2.

C.4.1 Group if $e \leq 5$

In this part we prove that, when $e \leq 5$, the infinity part of an elliptic loop is associative, hence a group, as stated by Proposition 4.2.1.

```
S< p, A,B, x1,z1, x2,z2, x3,z3 > := PolynomialRing(Integers(),9);

P1 := [x1*p,1,z1*p];
P2 := [x2*p,1,z2*p];
P3 := [x3*p,1,z3*p];
```

```
P12 := Sum(A,B, P1[1],P1[2],P1[3], P2[1],P2[2],P2[3]);
SS := Sum(A,B, P12[1],P12[2],P12[3], P3[1],P3[2],P3[3]);

P23 := Sum(A,B, P2[1],P2[2],P2[3], P3[1],P3[2],P3[3]);
TT := Sum(A,B, P1[1],P1[2],P1[3], P23[1],P23[2],P23[3]);

c1 := SS[1]*TT[2] - SS[2]*TT[1];
c2 := SS[1]*TT[3] - SS[3]*TT[1];
c3 := SS[2]*TT[3] - SS[3]*TT[2];

Min([Degree(X,p) : X in Monomials(c1)]) eq 5;
> true
Min([Degree(X,p) : X in Monomials(c2)]) eq 6;
> true
Min([Degree(X,p) : X in Monomials(c3)]) eq 5;
> true
```

C.4.2 Non-group if $e \geq 6$

We continue by specializing, in the above setting, the points $P_1 = (p : 1 : 0)$ and $P_2 = P_3 = (0 : 1 : p)$, to perform the computations involved in Lemma 4.2.2.

```
c1ev := Evaluate(c1,[p, A,B, 1,0, 0,1, 0,1]);
c2ev := Evaluate(c2,[p, A,B, 1,0, 0,1, 0,1]);
c3ev := Evaluate(c3,[p, A,B, 1,0, 0,1, 0,1]);

IsEmpty( [m : m in Terms(c2ev) | Degree(m,p) lt 6] );
> true

c1ev := &+[m : m in Terms(c1ev) | Degree(m,p) lt 6];
c3ev := &+[m : m in Terms(c3ev) | Degree(m,p) lt 6];
```

```
I := ideal< S | c1ev,c3ev >;

972*p^5*B^3*(B-2) in I;
> true
36*p^5*B*(4*A-9*B^2+24*B) in I;
> true
6*p^5*A*(2*A+3*B) in I;
> true
```

C.5 TWO POINTS AT INFINITY

In this part we verify the inclusion stated in the proof of Lemma 4.4.1.

```
S< p, A,B, x1,y1,z1, a,b,c,d > := PolynomialRing(Integers(), 10);
P := [x1,y1,z1];
Q := [a*p,1,b*p];
R := [c*p,1,d*p];

Ip := ideal<S | p >;

QR := Sum( A,B, Q[1],Q[2],Q[3], R[1],R[2],R[3] );
Ass1 := Sum( A,B, P[1],P[2],P[3], QR[1],QR[2],QR[3] );

PQ := Sum( A,B, P[1],P[2],P[3], Q[1],Q[2],Q[3] );
Ass2 := Sum( A,B, PQ[1],PQ[2],PQ[3], R[1],R[2],R[3] );

c1 := Ass1[1]*Ass2[2]-Ass1[2]*Ass2[1];
c2 := Ass1[1]*Ass2[3]-Ass1[3]*Ass2[1];
c3 := Ass1[2]*Ass2[3]-Ass1[3]*Ass2[2];

c1 in Ip^2 and c2 in Ip^2 and c3 in Ip^2;
> true
```

C.6 WELL-BEHAVING INFINITY

Here we check the containment employed while proving Lemma 4.4.2.

```
S< p, A,B, x1,y1,z1, x2,y2,z2, a > := PolynomialRing(Integers(), 10);
P := [x1,y1,z1];
Q := [x2,y2,z2];
R := [a*p,1,0];

F1 := x1^3+A*x1*z1^2+B*z1^3-y1^2*z1;
F2 := x2^3+A*x2*z2^2+B*z2^3-y2^2*z2;
Ip := ideal<S | p, F1, F2 >;

QR := Sum( A,B, Q[1],Q[2],Q[3], R[1],R[2],R[3] );
Ass1 := Sum( A,B, P[1],P[2],P[3], QR[1],QR[2],QR[3] );

PQ := Sum( A,B, P[1],P[2],P[3], Q[1],Q[2],Q[3] );
Ass2 := Sum( A,B, PQ[1],PQ[2],PQ[3], R[1],R[2],R[3] );

c1 := Ass1[1]*Ass2[2]-Ass1[2]*Ass2[1];
c2 := Ass1[1]*Ass2[3]-Ass1[3]*Ass2[1];
c3 := Ass1[2]*Ass2[3]-Ass1[3]*Ass2[2];

c1 in Ip^2 and c2 in Ip^2 and c3 in Ip^2;
> true
```

C.7 TWO POINTS INSIDE $\pi^{-1}(\overline{P})$

In this part we verify the computational tasks required by Proposition 4.4.4.

```
S< p, A,B, x,y,z, sx,sy,sz, a,b,c,d > := PolynomialRing(Integers(), 13);
P1 := [x,y,z];
P2 := [x+sx*p,-y+sy*p,z+sz*p];
R1 := [a*p,1,b*p];
R2 := [c*p,1,d*p];
```

```
F := x^3+A*x*z^2+B*z^3-y^2*z;
Ip := ideal< S | p >;

P1P2 := Sum( A,B, P1[1],P1[2],P1[3], P2[1],P2[2],P2[3] );
R1R2 := Sum( A,B, R1[1],R1[2],R1[3], R2[1],R2[2],R2[3] );

SS := Sum( A,B, P1P2[1],P1P2[2],P1P2[3], R1R2[1],R1R2[2],R1R2[3] );

P1R1 := Sum( A,B, P1[1],P1[2],P1[3], R1[1],R1[2],R1[3] );
P2R2 := Sum( A,B, P2[1],P2[2],P2[3], R2[1],R2[2],R2[3] );

TT := Sum( A,B, P1R1[1],P1R1[2],P1R1[3], P2R2[1],P2R2[2],P2R2[3] );

// Cast into the quotient now to speed up computations
SS := [(S/Ip^2)!SS[i] : i in [1..3]];
TT := [(S/Ip^2)!TT[i] : i in [1..3]];

c1 := SS[1]*TT[2]-SS[2]*TT[1];
c2 := SS[1]*TT[3]-SS[3]*TT[1];
c3 := SS[2]*TT[3]-SS[3]*TT[2];

c1 eq 0 and c2 eq 0 and c3 eq 0;
> true
```

C.8 THREE POINTS INSIDE $\pi^{-1}(\overline{P})$

In this section we detail the proof of Proposition 4.4.6.

```
S< p, A,B, x1,y1,z1, sx,sy,sz, tx,ty,tz > := PolynomialRing(Integers(), 12);
P1 := [x1,y1,z1];
P2 := [x1+sx*p,y1+sy*p,z1+sz*p];
P3 := [x1+tx*p,-y1+ty*p,z1+tz*p];
```

```
Ip := ideal< S | p >;

P1P2 := Sum( A,B, P1[1],P1[2],P1[3], P2[1],P2[2],P2[3] );
SS := Sum( A,B, P1P2[1],P1P2[2],P1P2[3], P3[1],P3[2],P3[3] );

P2P3 := Sum( A,B, P2[1],P2[2],P2[3], P3[1],P3[2],P3[3] );
TT := Sum( A,B, P1[1],P1[2],P1[3], P2P3[1],P2P3[2],P2P3[3] );

// Cast into the quotient now to speed up computations
SS := [(S/Ip^2)!SS[i] : i in [1..3]];
TT := [(S/Ip^2)!TT[i] : i in [1..3]];

c1 := SS[1]*TT[2]-SS[2]*TT[1];
c2 := SS[1]*TT[3]-SS[3]*TT[1];
c3 := SS[2]*TT[3]-SS[3]*TT[2];

c1 eq 0 and c2 eq 0 and c3 eq 0;
> true
```

C.9 THREE POINTS INSIDE $\pi^{-1}(\overline{P})$ AND THREE INSIDE $\pi^{-1}(\overline{Q})$

This part is devoted to complete the proof of Proposition 4.4.11. Despite the introduction of many implementation strategies aiming at reducing space consumption, this task is still heavily memory intensive, therefore a server is advised for running it.

First, we create the objects involved in the computation.

```
S< p, x1,z1, x2,z2, a1,b1, c1,d1, a2,b2, c2,d2, A,B > := PolynomialRing(Integers
    (), 15);
P1 := [x1,1,z1];
P2 := [x1+a1*p,1,z1+b1*p];
P3 := [x1+c1*p,1,z1+d1*p];
```

```
Q1 := [x2,1,z2];
Q2 := [x2+a2*p,1,z2+b2*p];
Q3 := [x2+c2*p,1,z2+d2*p];
```

Here we perform the first association:

$$SS = (P_1 + P_2 - P_3) + (Q_1 + Q_2 - Q_3).$$

```
// We perform the difference first. This heuristically speeds up the final
    computation.
P23 := Sum( A,B, P2[1],P2[2],P2[3], P3[1],-P3[2],P3[3] );
P123 := Sum( A,B, P1[1],P1[2],P1[3], P23[1],P23[2],P23[3] );

Q23 := Sum( A,B, Q2[1],Q2[2],Q2[3], Q3[1],-Q3[2],Q3[3] );
Q123 := Sum( A,B, Q1[1],Q1[2],Q1[3], Q23[1],Q23[2],Q23[3] );

// leave out p^2 terms to speed up the following operations

P123 := [ &+[m : m in Terms(P123[i]) | Degree(m,p) lt 2] : i in [1..3] ];
Q123 := [ &+[m : m in Terms(Q123[i]) | Degree(m,p) lt 2] : i in [1..3] ];

time SS := Sum( A,B, P123[1],P123[2],P123[3], Q123[1],Q123[2],Q123[3] );
> Time: 175.830
```

Now we perform the second association:

$$TT = (P_1 + Q_1) + (P_2 + Q_2) - (P_3 + Q_3).$$

```
X1 := Sum( A,B, P1[1],P1[2],P1[3], Q1[1],Q1[2],Q1[3] );
X2 := Sum( A,B, P2[1],P2[2],P2[3], Q2[1],Q2[2],Q2[3] );
X3 := Sum( A,B, P3[1],P3[2],P3[3], Q3[1],Q3[2],Q3[3] );

// leave out p^2 terms to speed up the following operations
```

```
X1 := [ &+[m : m in Terms(X1[i]) | Degree(m,p) lt 2] : i in [1..3] ];
X2 := [ &+[m : m in Terms(X2[i]) | Degree(m,p) lt 2] : i in [1..3] ];
X3 := [ &+[m : m in Terms(X3[i]) | Degree(m,p) lt 2] : i in [1..3] ];

// again, we perform the difference first, to shorten computational time
X2X3 := Sum( A,B, X2[1],X2[2],X2[3], X3[1],-X3[2],X3[3] );

// leave out p^2 terms to speed up the following operations

X2X3 := [ &+[m : m in Terms(X2X3[i]) | Degree(m,p) lt 2] : i in [1..3] ];

time TT := Sum( A,B, X1[1],X1[2],X1[3], X2X3[1],X2X3[2],X2X3[3] );
> Time: 1136.010
```

The following is the heavy part. Let $SS = (S_1 : S_2 : S_3)$ and $TT = (T_1 : T_2 : T_3)$, we want to verify that

$$S_1T_2 - S_2T_1 = S_1T_3 - S_3T_1 = S_2T_3 - S_3T_2 = 0.$$

To speed up the multiplications, which involve huge polynomials, we cancel the p^2-terms before computing them, as follows:

$$\left.\begin{aligned} S_1 &= S_1^o + S_1^p p \\ S_2 &= S_2^o + S_2^p p \\ T_1 &= T_1^o + T_1^p p \\ T_2 &= T_2^o + T_2^p p \end{aligned}\right\} \to \quad S_1T_2 - S_2T_1 = \left| \begin{aligned} & S_1^oT_2^o - S_2^oT_1^o \\ & + (S_1^oT_2^p + S_1^pT_2^o - S_2^oT_1^p - S_2^pT_1^o)p \\ & + (S_1^pT_2^p - S_2^pT_1^p)p^2 \quad \leftarrow \text{do not compute} \end{aligned}\right.$$

In fact, we prove that

$$S_1^oT_2^o - S_2^oT_1^o = S_1^oT_2^p + S_1^pT_2^o - S_2^oT_1^p - S_2^pT_1^o = 0.$$

The same strategy is applied on $S_1T_3 - S_3T_1$ and $S_2T_3 - S_3T_2$.

```
SS := [ &+[m : m in Terms(SS[i]) | Degree(m,p) lt 2] : i in [1..3] ];
TT := [ &+[m : m in Terms(TT[i]) | Degree(m,p) lt 2] : i in [1..3] ];

ppart1 := [ &+[(m div p) : m in Terms(SS[i]) | Degree(m,p) eq 1] : i in [1..3]
   ];
opart1 := [ SS[i] - p*ppart1[i] : i in [1..3] ];

ppart2 := [ &+[(m div p) : m in Terms(TT[i]) | Degree(m,p) eq 1] : i in [1..3]
   ];
opart2 := [ TT[i] - p*ppart2[i] : i in [1..3] ];

// We verify that the opart of the commutators are 0

opart1[1]*opart2[2]-opart1[2]*opart2[1] eq 0;
> true
opart1[1]*opart2[3]-opart1[3]*opart2[1] eq 0;
> true
opart1[2]*opart2[3]-opart1[3]*opart2[2] eq 0;
> true

// Now the heavy part

time c1 := ppart1[1]*opart2[3] + ppart2[3]*opart1[1] - ppart2[1]*opart1[3] -
   ppart1[3]*opart2[1];
> Time: 14647.680
c1 eq 0;
> true

time c2 := ppart1[1]*opart2[2] + ppart2[2]*opart1[1] - ppart2[1]*opart1[2] -
   ppart1[2]*opart2[1];
> Time: 11185.280
```

```
c2 eq 0;
> true


time c3 := ppart1[2]*opart2[3] + ppart2[3]*opart1[2] - ppart2[2]*opart1[3] -
   ppart1[3]*opart2[2];
> Time: 10902.050
c3 eq 0;
> true
```

C.10 CONDITION VERIFICATION FOR $p \leq 300$

We conclude this appendix by computationally verifying Condition 4.5.4 for every prime $p \leq 300$. Actually, we show that no intensive research is needed: for any pseudorandomly chosen $P \in \mathcal{L}^a$, we always find $pP \neq p\big(P + (0 : 1 : p)\big)$. This procedure lasts roughly fifteen minutes.

```
function AnomalousCurves(p)
        local l, toAdd;
        l := [];
        for A,B in [0..p-1] do
                b,E := IsEllipticCurve([GF(p)!A,B]);
                if b and #E eq p then
                        toAdd := true;
                        for C in l do
                                if IsIsomorphic(C,E) then
                                        toAdd := false;
                                end if;
                        end for;
                        if toAdd then
                                l cat:= [E];
                        end if;
                end if;
        end for;
        return l;
end function;


Z := Integers();


time for p in PrimesInInterval(5,300) do
        Zp2 := Integers(p^2);
        for E in AnomalousCurves(p) do
                A := Z!Coefficients(E)[4];
                B := Z!Coefficients(E)[5];
                for P in Points(E) do
                        if P ne E![0,1,0] then
                                sP := Sum(A,B,Z!P[1],Z!P[2],Z!P[3],0,1,p);
                                psP := [Zp2!Z!P[1],Zp2!Z!P[2],Zp2!Z!P[3]];
                                pP := [Zp2!Z!P[1],Zp2!Z!P[2],Zp2!Z!P[3]];
                                for i in [2..p] do
                                        pP := Sum(A,B,Z!P[1],Z!P[2],Z!P[3],pP
    [1],pP[2],pP[3]);
                                        sP := Sum(A,B,sP[1],sP[2],sP[3],psP[1],
    psP[2],psP[3]);
                                end for;
                                if ( pP[1]*sP[2]-pP[2]*pP[1] eq 0 and pP[1]*sP
    [3]-pP[3]*pP[1] eq 0 and pP[2]*sP[3]-pP[3]*pP[2] eq 0 ) then
                                    E,P;
                                    break P;
                                end if;
                        end if;
                end for;
        end for;
end for;
> Time: 847.750
```

APPENDIX D
OTHER WORKS

A Ph.D. in mathematics is intended, by the author, as a period where facing research-level problems from different fields, testing yourself against thrilling challenges that keep reminding you how moving this discipline is.

Since the present essay constitutes the author's doctoral thesis, it needs to collect at least a short reference to other journeys made in the past years, even if not related to the main subject of this work, which is what this appendix is devoted to.

The first mention undoubtedly needs to be granted to a substantial work[1] where a symmetric tensor decomposition algorithm is provided by exploiting properties of apolar duality and Hankel operators. In this paper, we have improved the best known symbolic algorithm for recovering Waring decomposition of symmetric tensors by means of simple symmetric pieces, as far as we have employed the same ideas to address more general types of decomposition, such as the tangential and the cactus ones.

A second credit is given to the description[2] of first degree prime ideals in biquadratic extensions, which shows great potential for further generalizations and applications to the general number field sieve toolkit.

On the cryptographic side, a new ECDLP-based scheme has been proposed[3] for designing a blockchain model in which users do not need to trust either the protocol proposers.

Finally, two surveys[4][5] have seen light to systematize the knowledge about the modern notions of proof-of-work and distributed computing techniques.

[1] A. Bernardi, D. Taufer, *Waring, tangential and cactus decompositions*, to appear, accepted in JMPA, Preprint available at `https://arxiv.org/abs/1812.02612`.

[2] M. Sala, G. Santilli, D. Taufer, *First-Degree Prime Ideals of Biquadratic Fields dividing prescribed Principal Ideals*, Preprint available at `https://arxiv.org/abs/1908.00383`.

[3] A. Meneghetti, M. Sala, D. Taufer, *A new ECDLP-based PoW model*, CEUR Proceedings, Vol. 2580, 2020.

[4] A. Meneghetti, M. Sala, D. Taufer, *A survey on PoW-based consensus*, AETiC, Vol. 4, No. 1, 2020.

[5] A. Meneghetti, T. Parise, M. Sala, D. Taufer, *A survey on efficient parallelization of blockchain-based smart contracts*, AETiC, Vol. 3, No. 5, 2019.