Research Article

Massimiliano Sala and Daniele Taufer*

Group structure of elliptic curves over $\mathbb{Z}/N\mathbb{Z}$

https://doi.org/10.1515/jmc-2023-0025
received September 05, 2023; accepted October 18, 2023

Abstract: We characterize the possible groups $E(\mathbb{Z}/N\mathbb{Z})$ arising from elliptic curves over $\mathbb{Z}/N\mathbb{Z}$ in terms of the groups $E(\mathbb{F}_p)$, with p varying among the prime divisors of N. This classification is achieved by showing that the infinity part of any elliptic curves over $\mathbb{Z}/p^e\mathbb{Z}$ is a $\mathbb{Z}/p^e\mathbb{Z}$-torsor, of which a generator is exhibited. As a first consequence, when $E(\mathbb{Z}/N\mathbb{Z})$ is a p-group, we provide an explicit and sharp bound on its rank. As a second consequence, when $N = p^e$ is a prime power and the projected curve $E(\mathbb{F}_p)$ has trace one, we provide an isomorphism attack to the elliptic curve discrete logarithm problem, which works only by means of finite ring arithmetic.

Keywords: group structure, elliptic curves, ECDLP

MSC 2020: 11T71, 13B25, 14H52

1 Introduction

Elliptic curves have been providing number theory with a fertile field of intense research for the last century, from theoretic [1–4], algorithmic [5,6], and applied [7–10] sides. In their basic definition, these objects consist of non-singular plane projective cubics, defined as the zero-set of a Weierstrass polynomial over a given base field. It is well known that these curves are actually abelian varieties with the chord-tangent sum [11–13]. The study of the group structure arising from this operation has attracted huge attention, and its grasp has proven to be remarkably challenging. Beyond its indisputable algebraic interest, the security of cryptographic protocols based on these curves relies upon the nature of their addition operation; hence, the investigation of these groups has received impetus in the last few decades.

When the underlying field is finite, any group that may be realized as the point group of an elliptic curve is known [14,15]. Nevertheless, both their distribution [16] and their efficient explicit description [17] are lines of open research. We refer to the study by Sala and Taufer [18] for an overview of the known classification of groups arising from curves with a Weierstrass model.

Elliptic curves may also be defined over rings, among which $\mathbb{Z}/N\mathbb{Z}$ is a significant instance both from a theoretical perspective [19] and for cryptographic applications [20,21]. In this study, we are mainly interested in their algebraic, especially groupal, properties: we classify all the possible groups arising from elliptic curves over any residue ring $\mathbb{Z}/N\mathbb{Z}$ in terms of their projected components modulo the prime divisors of N. More precisely, if p is a prime integer and $v_p(N)$ is the p-adic valuation of N, the Chinese reminder theorem provides a group isomorphism:

$$E(\mathbb{Z}/N\mathbb{Z}) \simeq \bigoplus_{p|N} E(\mathbb{Z}/p^{v_p(N)}\mathbb{Z}),$$

*** Corresponding author: Daniele Taufer,** KU Leuven, Numerical Analysis and Applied Mathematics (NUMA), Celestijnenlaan 200a, 3001 Leuven, Belgium, e-mail: daniele.taufer@kuleuven.be
Massimiliano Sala: Department of Mathematics, University of Trento, Via Sommarive 14, 38123 Povo, Italy, e-mail: massimiliano.sala@unitn.it
ORCID: Massimiliano Sala 0000-0002-7266-5146; Daniele Taufer 0000-0003-3402-4863

whose components are known [12,19] to split as:

$$E(\mathbb{Z}/p^{v_p(N)}\mathbb{Z}) = H \oplus E(\mathbb{F}_p).$$

The subgroup at infinity H, given by the kernel of the canonical projection, is known to be a p-group, since $|H| = p^{v_p(N)-1}$ [19]. However, the structure of this group was only recently determined in terms of 0-layers of elliptic loops [22].

In this work, we provide a complete classification result based only on the arithmetic of curves over $\mathbb{Z}/N\mathbb{Z}$. In particular, we prove the following group isomorphism:

$$E(\mathbb{Z}/N\mathbb{Z}) \simeq \bigoplus_{\substack{p|N \\ |E(\mathbb{F}_p)|\neq p}} E(\mathbb{F}_p) \oplus \mathbb{Z}/p^{v_p(N)-1}\mathbb{Z} \oplus \bigoplus_{\substack{p|N \\ |E(\mathbb{F}_p)|=p}} G_p,$$

where every G_p may be either $\mathbb{Z}/p^{v_p(N)}\mathbb{Z}$ (*cyclic* case) or $\mathbb{F}_p \oplus \mathbb{Z}/p^{v_p(N)-1}\mathbb{Z}$ (*split* case). This result is obtained by proving that the infinity part of $E(\mathbb{Z}/p^e\mathbb{Z})$ is a $\mathbb{Z}/p^e\mathbb{Z}$-torsor, which is far from holding over generic local rings [23]. By proving it, we refine the case $t = 0$ of [22, Proposition 10.3], as we explicitly exhibit a generator of this cyclic subgroup.

From the aforementioned classification, we derive some consequences. First, we give an explicit bound on the rank of $E(\mathbb{Z}/N\mathbb{Z})$ when the points of such curve form a p-group. This bound is sharp and depends only on p, determining as a corollary infinitely many groups that cannot arise from such curves. The proof of this bound also provides a systematic way for generating such p-curves of admissible ranks. Second, we exhibit a polynomial-time isomorphism attack to the elliptic curve discrete logarithm problem (ECDLP) over anomalous curves. Although similar attacks have already appeared [24,25], we find this approach noteworthy as its correctness and execution may be elaborated with only finite ring arithmetic, which makes it slightly more elementary.

This article is organized as follows. In Section 2, we recall some known results and definitions, including the group structure of elliptic curves over finite fields and the definition of such curves over rings. In Section 3, the group structure of elliptic curves over $\mathbb{Z}/N\mathbb{Z}$ is investigated and we derive our main result (Theorem 2). Consequently, in Section 4, we present a bound to the rank of p-groups that may arise from elliptic curves over $\mathbb{Z}/N\mathbb{Z}$. An isomorphism attack to the ECDLP over anomalous curves is described in Section 5. Finally, conclusions and further work are discussed in Section 6.

2 Preliminaries

In this study, R always denotes a commutative ring with unity and R^* is the set of its invertible elements. We use capital letters X, Y, and Z to denote the elements of R, while lowercase ones are variables in $R[x, y, z]$.

Definition 1. (Primitivity) A finite collection $\{X_i\}_{i\in\{0,\dots,n\}} \subseteq R^{n+1}$ is called *primitive* if the ideal $(\{X_i\}_{i\in\{0,\dots,n\}})_R$ is R itself.

2.1 Elliptic curves over finite fields

The trace t of any elliptic curve over a finite field $\mathbb{F}_q$ is constrained by the Hasse bound [11, Theorem V.1.1], i.e.,

$$t = q + 1 - |E(\mathbb{F}_q)|$$

is bounded by

$$-2\sqrt{q} \le t \le 2\sqrt{q}.$$

Not every possible integer t in the aforementioned interval occurs as the trace of an elliptic curve over $\mathbb{F}_q$, as detailed in [26, Theorem 4.1]. However, the same theorem shows that every such t may be achieved if q is a

pure prime, i.e., the Hasse interval over prime fields is full. From this work, a complete characterization of the possible point groups for elliptic curves over finite fields has seen the light, independently discovered by two authors [14,15].

By virtue of these works, we know all the possible groups arising from elliptic curves over finite fields, which we will use in Section 3 to characterize those of curves over $\mathbb{Z}/N\mathbb{Z}$.

2.2 Strong rank

To deal with matrices over commutative rings, it is worth introducing a stronger notion of matrix rank.

Definition 2. (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 $I_t(A) = (0)$.

Definition 3. (Strong rank) Let $n, m \in \mathbb{Z}_{\geq 1}$ and $A \in M_{n,m}(R)$. We define the *strong rank* of A as:

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

This notion of rank is easily shown to be never lower than the usual notion of rank over rings [27, Chapter 4]. The convenience of using this rank relies on the following result.

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

(*i*) $\mathrm{rk}(A) = 1$.
(*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 $\mathrm{rk}(A) = 1$, 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 column combinations. Since v_1 is primitive, there are $\alpha_1, \ldots, \alpha_n \in R$ with

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

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. Thus, for every $i, j \in \{1, \ldots, n\}$, we have $v_{1i}v_{2j} = v_{1j}v_{2i}$, then

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

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 $\mathrm{rk}(A) = 1$. □

2.3 Elliptic curves over rings

Let n be a non-negative integer. The projective n-space over R is defined in order to respect projections on any non-zero quotient of R, as follows.

Definition 4. (Projective n-space) The *projective n-space* over R is the set of orbits of primitive tuples in R^{n+1} under the action of elements $u \in R^*$ given by:

$$u(X_0, \ldots, X_n) = (uX_0, \ldots, uX_n).$$

It is denoted by $\mathbb{P}^n(R)$, while $(X_0 : \cdots : X_n) \in \mathbb{P}^n(R)$ represents the orbit of $(X_0, \ldots, X_n) \in R^{n+1}$.

An elliptic curve over R may be defined [19] to properly extend a family of elliptic curves over $R/\mathfrak{m}$, for $\mathfrak{m}$ ranging among all the maximal ideals of R, provided that this ring satisfies the following condition.

Condition I [19] For every pair $n, m \in \mathbb{Z}_{\geq 1}$ 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.

In this work, we will only deal with elliptic curves that may be defined via their short Weierstrass equation, which is not restrictive when $6 \in R^*$.

Definition 5. (Elliptic curve over R) Let R be a commutative ring with unity satisfying Condition I and let $A, B \in R$ such that

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

The *elliptic curve* $E_{A,B}(R)$ is defined as:

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

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

On these curves, a sum operation may be explicitly defined on an open covering of $E_{A,B}(R) \times E_{A,B}(R)$ by means of $(2, 2)$-bidegree polynomials [28,29]. This operation extends the usual point addition with respect to projections, i.e., for every proper ideal $I \subsetneq R$, we have a well defined group homomorphism:

$$\pi : E_{A,B}(R) \twoheadrightarrow E_{A,B}(R/I).$$

We recall for convenience the two addition laws we use in this work: the sum of $P_1 = (X_1 : Y_1 : Z_1)$ and $P_2 = (X_2 : Y_2 : Z_2)$ is given by any primitive linear combination of $(S_1 : S_2 : S_3)$ and $(T_1 : T_2 : T_3)$, where[1]

$$\begin{aligned}
S_1 &= (X_1Y_2 - X_2Y_1)(Y_1Z_2 + Y_2Z_1) + (X_1Z_2 - X_2Z_1)Y_1Y_2 - A(X_1Z_2 - X_2Z_1)(X_1Z_2 + X_2Z_1) - 3B(X_1Z_2 - X_2Z_1)Z_1Z_2, \\
S_2 &= -3X_1X_2(X_1Y_2 - X_2Y_1) - Y_1Y_2(Y_1Z_2 - Y_2Z_1) - A(X_1Y_2 - X_2Y_1)Z_1Z_2 + A(Y_1Z_2 - Y_2Z_1)(X_1Z_2 + X_2Z_1) \\
&\quad + 3B(Y_1Z_2 - Y_2Z_1)Z_1Z_2, \\
S_3 &= 3X_1X_2(X_1Z_2 - X_2Z_1) - (Y_1Z_2 - Y_2Z_1)(Y_1Z_2 + Y_2Z_1) + A(X_1Z_2 - X_2Z_1)Z_1Z_2
\end{aligned}$$

and

1 Addition laws corresponding to $(0 : 0 : 1)$ and $(0 : 1 : 0)$ as in [28, Theorem 2].

$$T_1 = Y_1Y_2(X_1Y_2 + X_2Y_1) - AX_1X_2(Y_1Z_2 + Y_2Z_1) - A(X_1Y_2 + X_2Y_1)(X_1Z_2 + X_2Z_1) - 3B(X_1Y_2 + X_2Y_1)Z_1Z_2 - 3B(X_1Z_2 + X_2Z_1)(Y_1Z_2 + Y_2Z_1) + A^2(Y_1Z_2 + Y_2Z_1)Z_1Z_2,$$

$$T_2 = Y_1^2Y_2^2 + 3AX_1^2X_2^2 + 9BX_1X_2(X_1Z_2 + X_2Z_1) - A^2X_1Z_2(X_1Z_2 + 2X_2Z_1) - A^2X_2Z_1(2X_1Z_2 + X_2Z_1) - 3ABZ_1Z_2(X_1Z_2 + X_2Z_1) - (A^3 + 9B^2)Z_1^2Z_2^2,$$

$$T_3 = 3X_1X_2(X_1Y_2 + X_2Y_1) + Y_1Y_2(Y_1Z_2 + Y_2Z_1) + A(X_1Y_2 + X_2Y_1)Z_1Z_2 + A(X_1Z_2 + X_2Z_1)(Y_1Z_2 + Y_2Z_1) + 3B(Y_1Z_2 + Y_2Z_1)Z_1Z_2.$$

A compact and efficient way for computing the latter addition law may be found in [22, Lemma 2.1]. Similar concise formulas over any characteristics were established in [23, Proposition 3.2].

3 Elliptic curves over $\mathbb{Z}/N\mathbb{Z}$

Let $N \in \mathbb{Z}_{\geq 2}$ be an integer. Hereafter, we consider elliptic curves defined over the ring $R = \mathbb{Z}/N\mathbb{Z}$, which satisfies Condition I. More generally, in the study by Lenstra [19], this condition has been proved to hold for every ring with a finite number of maximal ideals. Here, we show that $\mathbb{Z}/N\mathbb{Z}$ underlies a condition even stronger than Condition I.

Lemma 2. *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 I.*

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

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

is primitive over $\mathbb{Z}/p\mathbb{Z}$. By the Chinese reminder theorem, we may find integers $\beta_1, ..., \beta_m \in \mathbb{Z}$ solving, for every prime divisor p of N, the congruence system:

$$\beta_i \equiv \alpha_i^{(p)} \bmod p.$$

Therefore, $\sum_{i=1}^{m} \beta_i c_i$ is easily seen to be a primitive combination of the columns of A. □

We now recall how the group of points of an elliptic curve over $\mathbb{Z}/N\mathbb{Z}$ can be described by the curve projections over the p-components of this ring, with p ranging among the prime divisors of N.

Proposition 1. [12, Corollary 2.32] *Let N_1 and N_2 be coprime integers and let $A, B \in \mathbb{Z}$ such that $\Delta_{A,B} \in (\mathbb{Z}/N_1N_2\mathbb{Z})^*$. Then, the canonical projections induce a group isomorphism:*

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

Thus, it is sufficient to study the structure of elliptic curves $E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ for any prime p and positive integer e, which is the main goal of this section. We begin by noting that the points $P \in E = E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ of such curves have prescribed representatives:

– If $P \in E^a$, then there are $X, Y \in \mathbb{Z}/p^e\mathbb{Z}$ such that

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

– If $P \in E^\infty$, then there are $X, Z \in p(\mathbb{Z}/p^e\mathbb{Z})$ such that

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

The size of these curves is known, as reported in the next lemma.

Lemma 3. [19, Section 4] *Let p be a prime, $e \in \mathbb{Z}_{\geq 1}$, and*

$$\pi : E_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) \to E_{A,B}(\mathbb{F}_p)$$

be the canonical projection. Then, for every $P \in E_{A,B}(\mathbb{F}_p)$, we have

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

In particular:

- *The size of the curve is $|E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})| = p^{e-1}|E_{A,B}(\mathbb{F}_p)|$,*
- $\ker\pi$ *is a subgroup of $E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$, whose size is p^{e-1}.*

The coordinates of points at infinity satisfy the following relation, which we prove by adapting the idea of expansion around O [11, Chapter IV].

Proposition 2. *Let p be a prime, $e \in \mathbb{Z}_{\geq 1}$, and $E = E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$. There is a polynomial $\mathsf{f} \in \mathbb{Z}[x]$ of degree at most $e-1$ such that for every $P \in E^\infty$, there is $X \in p(\mathbb{Z}/p^e\mathbb{Z})$ satisfying*

$$P = (X : 1 : \mathsf{f}(X)).$$

Moreover, we have

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

Proof. Since $P \in E^\infty$, it may be represented in the form $(X : 1 : Z)$, with $X, Z \in p(\mathbb{Z}/p^e\mathbb{Z})$ that satisfy

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

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

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

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 $F_0(x, z)$, which contains only 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 exist $M \in \mathbb{Z}_{\geq 0}$ and $g \in \mathbb{Z}[x, z]$ such that

$$F_M(x, z) = \mathsf{f}(x) + g(x, z),$$

with $g \in (x, z)^{e_{\mathbb{Z}[x,z]}}$ and $\deg(\mathsf{f}) < e$. Since both X and Z are divisible by p, then

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

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

$$F_3 = x^3 + Ax^7 + Bx^9 + (\text{terms of degree } \geq 11),$$

which proves the moreover part. □

Remark 1. Although finite local rings are complete with respect to the topology induced by their maximal ideal, they may well not be domains (e.g., $\mathbb{Z}/N\mathbb{Z}$). For this reason, we found it appropriate to explicitly compute f instead of considering the truncation to the correct exponent of the classical series [11, Chapter IV].

To simplify the exposition, for any $X \in \mathbb{Z}/p^e\mathbb{Z}$ and any positive integer t we write $p^t|X$ or $X \equiv 0 \bmod p^t$ in place of the more precise $X \in p^t(\mathbb{Z}/p^e\mathbb{Z})$. In the same spirit, we assign a p-adic valuation to any $X \in \mathbb{Z}/p^e\mathbb{Z}$ by writing

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

From Proposition 2, it is possible to derive a description of the first-order approximation of the sum of two points at infinity.

Proposition 3. *Let p be a prime, $e \in \mathbb{Z}_{\geq 1}$, $E = E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$, and $\mathsf{f} \in \mathbb{Z}[x]$ be the polynomial arising from E as in Proposition 2. Let also*

$$P_1 = (X_1 : 1 : \mathsf{f}(X_1)) \quad \text{and} \quad P_2 = (X_2 : 1 : \mathsf{f}(X_2)) \in E^\infty,$$

with $e_1 = v_p(X_1)$ and $e_2 = v_p(X_2)$. Then,

$$P_1 + P_2 = (X_3 : 1 : \mathsf{f}(X_3)), \quad \text{where } X_3 \equiv X_1 + X_2 \bmod p^{5\min\{e_1,e_2\}}.$$

Proof. As π is a group homomorphism, $P_1 + P_2$ lies in E^∞, which implies that these points are never exceptional for the addition law $+_{(0:1:0)}$ corresponding to $(0 : 1 : 0)$ [28, Theorem 2]. A straightforward computation with $+_{(0:1:0)}$ shows that, modulo monomials in X_1 and X_2 of total degree at least 5 (i.e., modulo $p^{5\min\{e_1,e_2\}}$), we have

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

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

We can now prove that the infinity group is cyclic, which provides a structure theorem for elliptic curves over $\mathbb{Z}/N\mathbb{Z}$.

Theorem 1. *Let p be a prime, $e \in \mathbb{Z}_{\geq 1}$, and $\mathsf{f} \in \mathbb{Z}[x]$ be the polynomial arising from $E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ as in Proposition 2. Then,*

$$0 \to \langle (p : 1 : \mathsf{f}(p)) \rangle \overset{\iota}{\hookrightarrow} E_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) \overset{\pi}{\to} E_{A,B}(\mathbb{F}_p) \to 0,$$

is a short exact sequence of groups.

Proof. We know that the canonical projection $\pi : E_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) \twoheadrightarrow E_{A,B}(\mathbb{F}_p)$ is a surjective group homomorphism and that $|\ker\pi| = p^{e-1}$ by Lemma 3. Thus, it is sufficient to prove that $P = (p : 1 : \mathsf{f}(p)) \in \ker\pi$ has order p^{e-1}. Since P lies over $O \in E_{A,B}(\mathbb{F}_p)$, then its order is a power of p ($\ker\pi$ is a p-group). We prove by induction on $0 \leq \varepsilon \leq e - 1$ that

$$p^\varepsilon P = (X : 1 : \mathsf{f}(X)) \quad \text{with} \quad v_p(X) = \varepsilon + 1.$$

In particular, the minimal ε such that $X \equiv 0 \bmod p^e$ is $\varepsilon = e - 1$.

[$\varepsilon = 0$] It is trivially seen that

$$p^0 P = (p : 1 : \mathsf{f}(p)) \quad \text{and} \quad v_p(p) = 1.$$

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

$$p^{\varepsilon+1}P = p(p^\varepsilon P) = p(X : 1 : \mathsf{f}(X)) \quad \text{and} \quad v_p(X) = \varepsilon + 1.$$

By Proposition 3 and induction on $\alpha \in \{1, \ldots, p - 1\}$, we have

$$(X : 1 : \mathsf{f}(X)) + (\alpha X : 1 : \mathsf{f}(\alpha X)) = (X_2 : 1 : \mathsf{f}(X_2)),$$

with

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

Thus, by specializing the aforementioned result for $\alpha = p - 1$, the p-adic valuation of the first component of $p(X : 1 : \mathsf{f}(X))$ is proved to be $v_p(X) + 1 = \varepsilon + 2$. □

The aforementioned theorem shows that the infinity part of any elliptic curve over $\mathbb{Z}/p^e\mathbb{Z}$ is a $\mathbb{Z}/p^e\mathbb{Z}$-torsor with respect to the standard multiplication action. This agrees with [22, Proposition 10.3], and it is sufficient to determine the group structure of these curves when their projection is not anomalous.

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

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

Proof. It is sufficient to show that the short exact sequence of Theorem 1 splits, which by the splitting lemma amounts to proving that it is left split. Since $q = |E_{A,B}(\mathbb{F}_p)| \neq p$ is in the Hasse bound of p, then $(p, q) = 1$, which implies the existence of a $k \in \mathbb{Z}$ satisfying

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

By Theorem 1, we have $E^{\infty}_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) = \pi^{-1}(O) = \langle (p : 1 : \mathsf{f}(p)) \rangle$. Thus, since $k \equiv 0 \bmod q$, the map

$$E_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) \xrightarrow{\cdot k} \langle (p : 1 : \mathsf{f}(p)) \rangle$$

is a well defined group homomorphism. Moreover, since $k \equiv 1 \bmod p^{e-1}$, the cyclic group $\langle (p : 1 : \mathsf{f}(p)) \rangle$ is fixed under this map; hence, the multiplication-by-k is a left section for the considered sequence. □

Despite forming a cyclic group, the algebra of points at infinity may be rather involved [23]. However, when e is small, an explicit group isomorphism may also be exhibited. The key point is the simplified description of X_3 as $X_1 + X_2$ given by Proposition 3, when the exponent of p does not exceed 5. We also remark that in the more general setting of elliptic loops, 5 is the exponent threshold for associativity of the projective part [22, Lemma 8.3, 8.4].

Proposition 4. *Let p be a prime, $1 \leq e \leq 5$ be an integer, $E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic curve, and $q = |E_{A,B}(\mathbb{F}_p)|$ be the size of its projected curve. Then,*

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

is a well defined group homomorphism. 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 projective representative of P. Moreover, as π is a group homomorphism, we have

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

Hence, by Proposition 2, we have $qP = (X : 1 : \mathsf{f}(X))$ with $X \in p(\mathbb{Z}/p^e\mathbb{Z})$. Therefore, $\frac{(qP)_x}{(qP)_y} \in p(\mathbb{Z}/p^e\mathbb{Z})$, which is canonically isomorphic to $\mathbb{Z}/p^{e-1}\mathbb{Z}$. Thus, Φ is a well defined map between groups having, by Lemma 3, the same size. It also respects the sum, as for every pair $P_1, P_2 \in E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$, we compute

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

and since $e \leq 5 \min\{v_p((qP_1)_x), v_p((qP_2)_x)\}$, then by Proposition 3, we have

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

As for the moreover part, it is sufficient to prove that $\ker\Phi = \{O\}$ when $q \neq p$. Let $\Phi(P) = (O, 0)$, then there exists $X \in p(\mathbb{Z}/p^e\mathbb{Z})$ such that $P = (X : 1 : \mathrm{f}(X))$ and

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

Since q lies in the Hasse interval of p, then $q \neq p$ implies $(p, q) = 1$, and we conclude that $X \equiv 0 \bmod p^e$; hence, the kernel of Φ is trivial. □

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

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

or split, i.e.,

$$E_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) \simeq \mathbb{F}_p \oplus \mathbb{Z}/p^{e-1}\mathbb{Z}. \tag{Split}$$

Even if the cyclic case occurs over $\mathbb{Z}/p^e\mathbb{Z}$ with an overwhelming probability of $\frac{p-1}{p}$ [25], both may take place. For instance, one may check that

$$E_{7,3}(\mathbb{Z}/13^2\mathbb{Z}) \simeq \langle(0 : 61 : 1)\rangle, \quad \text{while } E_{1,6}(\mathbb{Z}/13^2\mathbb{Z}) \simeq \langle(2 : 4 : 1)\rangle \oplus \langle(13 : 1 : 0)\rangle.$$

The aforementioned discussion leads to the classification theorem.

Theorem 2. *Let N be a positive integer and let A and B be integers such that $\Delta_{A,B}$ is coprime to N. Then, we have*

$$E_{A,B}(\mathbb{Z}/N\mathbb{Z}) \simeq \bigoplus_{\substack{p|N \\ |E_{A,B}(\mathbb{F}_p)|\neq p}} E_{A,B}(\mathbb{F}_p) \oplus \mathbb{Z}/p^{v_p(N)-1}\mathbb{Z} \oplus \bigoplus_{\substack{p|N \\ |E_{A,B}(\mathbb{F}_p)|=p}} G_p,$$

where every G_p may be either $\mathbb{Z}/p^{v_p(N)}\mathbb{Z}$ or $\mathbb{F}_p \oplus \mathbb{Z}/p^{v_p(N)-1}\mathbb{Z}$.

Proof. By Proposition 1, we know that

$$E_{A,B}(\mathbb{Z}/N\mathbb{Z}) \simeq \bigoplus_{p|N} E_{A,B}(\mathbb{Z}/p^{v_p(N)}\mathbb{Z}).$$

By Corollary 1, for every p such that $E_{A,B}(\mathbb{F}_p)$ is not anomalous, we have

$$E_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) \simeq E_{A,B}(\mathbb{F}_p) \oplus \mathbb{Z}/p^{v_p(N)-1}\mathbb{Z}.$$

On the other side, we have seen that

$$G_p = \mathbb{F}_p \oplus \mathbb{Z}/p^{v_p(N)-1}\mathbb{Z} \quad \text{or} \quad G_p = \mathbb{Z}/p^{v_p(N)}\mathbb{Z}$$

may both occur as group structure of $E_{A,B}(\mathbb{Z}/p^{v_p(N)}\mathbb{Z})$ when $E_{A,B}(\mathbb{F}_p)$ is anomalous, which completes the study cases. □

Remark 2. Given a finite collection of elliptic curves $\{E_{A_l,B_l}(R_l)\}_{1\leq l\leq k}$, we may define an elliptic curve over their product ring $\prod_{l=1}^k R_l$ with the componentwise operation, and by [19, Section 4], we have

$$E_{(A_1,\dots,A_k),(B_1,\dots,B_k)}\left(\prod_{l=1}^k R_l\right) \simeq \prod_{l=1}^k E_{A_l,B_l}(R_l).$$

Thus, Theorem 2 provides the group structures of every elliptic curve defined over a ring isomorphic to a finite product of integer residue rings.

Remark 3. We note that Theorem 1 heavily relies on the behavior of elliptic curves over $\mathbb{Z}/p^e\mathbb{Z}$. Let us consider another local ring, namely, $R = \mathbb{F}_5[x]/(x^4)$, and let ε be a generator of its maximal ideal. Again, we have a canonical projection:

$$R \to \mathbb{F}_5, \quad X_0 + X_1\varepsilon + X_2\varepsilon^2 + X_3\varepsilon^3 \mapsto X_0,$$

so we have an elliptic curve $E_{1,2}(R)$ defined as in Section 2.3, together with a canonical projection onto $E_{1,2}(\mathbb{F}_5)$.

This curve may appear similar to $E_{1,2}(\mathbb{Z}/5^4\mathbb{Z})$ at first glance, but one can directly verify that the point group of $E_{1,2}(R)$ is given by:

$$\langle(2\varepsilon^3 + \varepsilon : 1 : \varepsilon^3)\rangle \oplus \langle(3\varepsilon^3 + 3\varepsilon^2 + 2\varepsilon : 1 : 3\varepsilon^3)\rangle \oplus \langle(\varepsilon^3 + \varepsilon + 3 : \varepsilon^3 + 3\varepsilon^2 + 4\varepsilon + 3 : 1)\rangle,$$

so that $E_{1,2}(R) \simeq \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/35\mathbb{Z}$. This is due to the different structure of the infinity parts, as $E^{\infty}_{1,2}(R) \simeq (\mathbb{Z}/5\mathbb{Z})^{\oplus 3}$, while $E^{\infty}_{1,2}(\mathbb{Z}/5^4\mathbb{Z}) \simeq \mathbb{Z}/5^3\mathbb{Z}$ as prescribed by our previous results. A detailed study of the latter type of rings may be found in the study by Invernizzi and Taufer [23].

4 Rank of p-groups from elliptic curves

We know that groups arising from elliptic curves defined over finite fields have prescribed constraints [14,15], e.g., their rank cannot exceed 2. This restriction can be relaxed for curves defined over $\mathbb{Z}/N\mathbb{Z}$, as their rank may be arbitrarily large, but it may still be bounded in terms of the number of primes inside a Hasse interval.

Definition 6. ($\mathcal{H}_p$) Given an integer $p \in \mathbb{Z}$, we define

$$\mathcal{H}_p = |\{q \in \mathbb{Z} | q \text{ is prime and } p + 1 - 2\sqrt{p} \le q \le p + 1 + 2\sqrt{p}\}|.$$

The following result provides a sharp bound on the rank that elliptic curves over $\mathbb{Z}/N\mathbb{Z}$ may have if their point group are p-groups, which, in particular, shows that there are infinitely many groups that cannot arise as a point group for an elliptic curve over an integer residue ring.

Proposition 5. *Let $p \ge 5$ be a prime, $N \in \mathbb{Z}_{\ge 2}$, and $E = E_{A,B}(\mathbb{Z}/N\mathbb{Z})$ be an elliptic curve that is a p-group. Then, by defining*

$$\chi_p = \begin{cases} 2, & \text{if there is a prime } q \text{ such that } E_{A,B}(\mathbb{F}_q) \simeq \mathbb{F}_p \oplus \mathbb{F}_p, \\ 0, & \text{otherwise,} \end{cases}$$

we have

$$\mathrm{rk}(E) \le \mathcal{H}_p + \chi_p + 1.$$

Proof. By Theorem 2, we have

$$E \simeq \bigoplus_{\substack{q|N \\ |E_{A,B}(\mathbb{F}_q)| \neq q}} E_{A,B}(\mathbb{F}_q) \oplus \mathbb{Z}/q^{v_q(N)-1}\mathbb{Z} \oplus \bigoplus_{\substack{q|N \\ |E_{A,B}(\mathbb{F}_q)| = q}} G_q,$$

where every G_q may be either $\mathbb{Z}/q^{v_q(N)}\mathbb{Z}$ or $\mathbb{F}_q \oplus \mathbb{Z}/q^{v_q(N)-1}\mathbb{Z}$. It is easy to see that G_q is a p-group only if $q = p$; hence, we have

$$\mathrm{rk} \bigoplus_{\substack{q|N \\ |E_{A,B}(\mathbb{F}_q)| = q}} G_q \le 2.$$

Similarly, we note that $\mathbb{Z}/q^{v_q(N)-1}\mathbb{Z}$ is a p-group only if $q = p$, but $E_{A,B}(\mathbb{F}_p)$ is a p-group if and only if $|E_{A,B}(\mathbb{F}_p)| = p$. Thus, we have

$$\bigoplus_{\substack{q|N \\ |E_{A,B}(\mathbb{F}_q)|\neq q}} E_{A,B}(\mathbb{F}_q) \oplus \mathbb{Z}/q^{v_q(N)-1}\mathbb{Z} \simeq \bigoplus_{\substack{q|N \\ q\neq p}} E_{A,B}(\mathbb{F}_q).$$

Moreover, since the rank of $E_{A,B}(\mathbb{F}_q)$ is at most 2 [12, Theorem 4.1], then it is a p-group only if

$$\text{either} \quad E_{A,B}(\mathbb{F}_q) \simeq \mathbb{F}_p \quad \text{or} \quad E_{A,B}(\mathbb{F}_q) \simeq \mathbb{F}_p \oplus \mathbb{F}_p.$$

Since the Hasse bound over a prime field is full, then $E_{A,B}(\mathbb{F}_q)$ may be isomorphic to $\mathbb{F}_p$ for every prime q inside the Hasse interval of p.

On the other side, by [12, Prop.4.16], we know that $E_{A,B}(\mathbb{F}_q) \simeq \mathbb{F}_p \oplus \mathbb{F}_p$ may occur only if

$$q \in \{p^2 + 1, p^2 \pm p + 1, p^2 \pm 2p + 1\}.$$

However, both p and q are odd primes; hence, only $q = p^2 \pm p + 1$ may occur. Furthermore, since $p > 3$, it is easy to see that either $3|p^2 + p + 1$ or $3|p^2 - p + 1$; therefore, only one of them can be prime. We conclude that there is at most one prime q such that $E_{A,B}(\mathbb{F}_q) \simeq \mathbb{F}_p \oplus \mathbb{F}_p$, so that

$$\operatorname{rk} \bigoplus_{\substack{q|N \\ q\neq p}} E_{A,B}(\mathbb{F}_q) \leq (\mathcal{H}_p - 1) + \chi_p.$$

Collecting the aforementioned rank bounds, the statement follows. □

Example 1. Let $p = 11$. None of $11^2 \pm 11 + 1$ is prime, then we have $\chi_{11} = 0$; therefore, by Proposition 5, regardless of $N \in \mathbb{Z}_{\geq 2}$, the rank of any elliptic curve over $\mathbb{Z}/N\mathbb{Z}$ that is a 11-group is bounded by $\mathcal{H}_{11} + 1 = 5$. We also note that this bound is sharp, as

$$E_{167707,21664}(\mathbb{Z}/187187\mathbb{Z}) \simeq \mathbb{F}_{11} \oplus \mathbb{F}_{11} \oplus \mathbb{F}_{11} \oplus \mathbb{F}_{11} \oplus \mathbb{F}_{11}.$$

Example 2. Let $p = 13$. We note that $13^2 - 13 + 1 = 157$ is prime and

$$E_{0,15}(\mathbb{F}_{157}) \simeq \mathbb{F}_{13} \oplus \mathbb{F}_{13}.$$

Therefore, we have $\chi_{13} = 2$. By means of Proposition 5, we know that any elliptic curve over $\mathbb{Z}/N\mathbb{Z}$ that is a 13-group has rank-bounded by $\mathcal{H}_{13} + 3 = 8$. We note again that this bound is sharp, as

$$E_{63707931,239467091}(\mathbb{Z}/659902243\mathbb{Z}) \simeq (\mathbb{F}_{13})^{\oplus 8}.$$

5 Another isomorphism attack to anomalous ECDLP

Given an additive group G and a base element $g \in G$, the discrete logarithm problem (DLP) on G consists of computing for any given $h \in G$ a positive integer N, if existent, such that $h = N \cdot g = g + g + \cdots + g$. When G is the point group of an elliptic curve (ECDLP), this problem is known to be computationally feasible only in special cases, such as the anomalous ones [24,25,30].

From the knowledge of the group structure provided by Theorem 1, we have another way of efficiently solving the ECDLP on anomalous curves using any cyclic curve that projects onto it.

Proposition 6. *Let p be a prime, $e \in \mathbb{Z}_{\geq 2}$, and $E = E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic curve, whose point group is cyclic of order p^e. Then, the map*

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

is a well defined surjective group homomorphism, whose kernel is

$$\ker\Theta = \langle (p : 1 : \mathsf{f}(p)) \rangle.$$

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

$$p^{e-1}P = (X : 1 : \mathsf{f}(X)), \quad \text{with } v_p(X) \geq e - 1.$$

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

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

where the last equality follows from Proposition 3, 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 homomorphism. Moreover, from the aforementioned equation, it follows that

$$\ker\Theta = \{mp \quad G | m \in \mathbb{Z}\} = \langle (p : 1 : \mathsf{f}(p)) \rangle.$$

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

From the aforementioned proposition, the discrete logarithm over anomalous curves may be immediately recovered.

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

$$\Theta \circ \pi^{-1} : E_{A,B}(\mathbb{F}_p) \to \mathbb{F}_p$$

is a well defined group isomorphism.

Proof. By Theorem 1, the projection π induces a group isomorphism $E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})/\langle (p : 1 : \mathsf{f}(p)) \rangle \simeq E(\mathbb{F}_p)$, whereas the map Θ arisen from Proposition 6 induces a group isomorphism $E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})/\langle (p : 1 : \mathsf{f}(p)) \rangle \simeq \mathbb{F}_p$. By composing those isomorphisms, the result follows. □

Finding any lift of a given point is computationally costless; therefore, the complexity of the isomorphism attack given by Corollary 2 only depends on the cost of computing Θ, which is $O(\log p)$. This approach is not faster than previously known attacks to the same family of curves [24,25,30], but it has the advantage of involving only finite precision objects.

Example 3. Let us consider an anomalous curve as constructed in the study by Leprévost et al. [31]:

$$p = 730750818665451459112596905638433048232067471723,$$
$$A = 425706413842211054102700238164133538302169176474,$$
$$B = 203362936548826936673264444982866339953265530166.$$

We consider on $E_{A,B}(\mathbb{F}_p)$ the points

$$P = (1 : 310536468939899693718962354338996655381367569020 : 1),$$
$$Q = (3 : 382927830531564410197403195539563768199438545 15 : 1).$$

To find their discrete logarithm, it is sufficient to compute any lifts, such as

$$P^{\uparrow} = (1 : P_y + \alpha p : 1), \quad Q^{\uparrow} = (3 : Q_y + \beta p : 1) \in E_{A,B}(\mathbb{Z}/p^2\mathbb{Z}),$$

where

$$\alpha = \frac{1 + A + B - P_y^2}{2pP_y} \bmod p^2, \quad \text{and} \quad \beta = \frac{27 + 3A + B - Q_y^2}{2pQ_y} \bmod p^2,$$

and to apply them, the group homomorphism Θ of Proposition 6:

$$\Theta(P^{\uparrow}) = 343088892565802863386490109374548044078624360215,$$
$$\Theta(Q^{\uparrow}) = 47097471200108454043339865392198374166198744 9793.$$

This way we obtain the discrete logarithm N such that $Q = N \cdot P$ as:

$$N = \frac{\Theta(Q^{\uparrow})}{\Theta(P^{\uparrow})} \bmod p = 113690975836469390483838646646828917131453128585.$$

We remark that such a discrete logarithm would be infeasible to be computed with generic logarithm techniques, as one can directly verify that the `Log` routine of Magma [32] does not terminate in a reasonable time.

6 Conclusions and open problems

In this work, we have provided the classification of groups arising from elliptic curves over $\mathbb{Z}/N\mathbb{Z}$ and exploited it to obtain a bound for their rank and an attack on the ECDLP over anomalous elliptic curves.

The key ingredient is Theorem 1, which might still hold for more general classes of rings, even though the kernel generator may be less explicit. Finding other instances or even classifying all the rings over which the infinity group is cyclic is still an open line of research.

From a cryptographic perspective, Theorem 1 shows that the difficulty of the ECDLP depends on the difficulty of the same problem over the base field and in the group of points at infinity. Whenever these two groups are linked (as in the case of the anomalous curves), the discrete logarithm on one group may be read from the other.

Finally, in this work, we only considered genus-1 curves for their theoretical and historical relevance, but it is reasonable to ask which other abelian varieties admit such an extension to $\mathbb{Z}/N\mathbb{Z}$ and, when it is the case, if analogous group decompositions over these rings hold.

Acknowledgement: This work has been accepted for presentation at CIFRIS23, the Congress of the Italian association of cryptography “De Componendis Cifris.”

Funding information: MS acknowledges the support from Ripple’s University Blockchain Research Initiative. DT was supported in part by the European Union’s H2020 Programme under grant agreement number ERC-669891, and in part by the Research Foundation – Flanders (FWO), project 12ZZC23N, and travel grant V425623N.

Author contributions: All authors have accepted responsibility for the entire content of this manuscript and approved its submission.

Conflict of interest: Prof. Massimiliano Sala is the Editor-in-Chief of the Journal of Mathematical Cryptology but was not involved in the review process of this article.

References

[1] Breuil C, Conrad B, Diamond F, Taylor R. On the modularity of elliptic curves over Q: wild 3-adic exercises. J Amer Math Soc. 2001;14:843–939.
[2] Merel L. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. Invent Math. 1996;124:437–49.
[3] Mordell LJ. On the rational solutions of the indeterminate equations of the third and fourth degrees. Proc Camb Phil Soc. 1922;21:179–92.
[4] Wiles A. Modular elliptic curves and Fermat’s last theorem. Ann Math. 1995;142:443–551.

[5] Bosma W. Primality testing using elliptic curves. Math Instituut, Univ Amsterdam, volume Tech Rep. 1985. p. 85–12.
[6] Schoof R. Elliptic curves over finite fields and the computation of square roots mod p. Math Comp. 1985;44:483–94.
[7] Johnson D, Menezes A, Vanstone S. The Elliptic Curve Digital Signature Algorithm (ECDSA). Int J Inf Secur. 2001;1:36–63.
[8] Koblitz N. Elliptic curve cryptosystems. Math Comp. 1987;48:203–9.
[9] Miller VS. Use of elliptic curves in cryptography. Adv Cryptol. 1985;218:417–26.
[10] Shparlinski IE. Pseudorandom number generators from elliptic curves. Contemp Math. 2009;477:121–42.
[11] Silverman JH. The arithmetic of elliptic curves, Springer-Verlag, 1986.
[12] Washington LC. Elliptic curves, number theory and cryptography. London: Chapman & Hall/CRC; 2008.
[13] Husemöller D. Elliptic curves. Graduate Texts in Mathematics. Vol. 111. Berlin: Springer-Verlag; 1987.
[14] Rück HG. A note on elliptic curves over finite fields. Math Comp. 1987;49:301–4.
[15] Voloch JF. A note on elliptic curves over finite fields. Bull Soc Math France. 1988;116:455–8.
[16] Banks WD, Pappalardi F, Shparlinski IE. On group structures realized by elliptic curves over arbitrary finite fields. Experiment Math. 2012;21:11–25.
[17] Kohel DR, Shparlinski IE. On exponential sums and group generators for elliptic curves over finite fields. Lecture Notes Comput Sci. 2000;21:395–404.
[18] Sala M, Taufer D. A survey on the group of points arising from elliptic curves with a Weierstrass model over a ring. Int J Group Theory. 2023;12:177–96.
[19] Lenstra HW. Elliptic curves and number-theoretic algorithms. Proceedings of the International Congress of Mathematicians; 1986. p. 99–120.
[20] Lenstra HW. Factoring integers with elliptic curves. Ann Math. 1987;126:649–73.
[21] Koyama K, Maurer UM, Okamoto T, Vanstone SA. New public-key schemes based on elliptic curves over the ring Z_n. Adv Cryptol. 1991;576:252–66.
[22] Sala M, Taufer D. Elliptic loops. J Pure Appl Algebra. 2023;227(12):107417.
[23] Invernizzi R, Taufer D. Multiplication polynomials for elliptic curves over finite local rings. In ACM's International Conference Proceedings Series (ISSAC 2023); 2023. p. 335–44.
[24] Satoh T, Araki K. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. Comm Math Univ Sancti Pauli. 1998;47:81–92.
[25] Smart N. The discrete logarithm on elliptic curves of trace one. J Cryptology. 1999;12:193–6.
[26] Waterhouse WC. Abelian varieties over finite fields. Ann. Sci. École Norm. Sup. 1969;4:521–60.
[27] Brown WC. Matrices over commutative rings. New York: Marcel Dekker; 1986.
[28] Bosma W, Lenstra HW. Complete systems of two addition laws for elliptic curves. J Number Theory. 1995;53:229–40.
[29] Lange H, Ruppert W. Complete systems of addition laws on abelian varieties. Invent Math. 1985;79:603–10.
[30] Semaev IA. Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p. Math Comp. 1998;67:353–6.
[31] Leprévost F, Monnerat J, Varrette S, Vaudenay S. Generating anomalous elliptic curves. Inform Process Lett. 2005;93:225–30.
[32] Bosma W, Cannon J, Playoust C. The Magma algebra system. I. The user language. J Symbolic Comput. 1997;24:235–65.