http://ijgt.ui.ac.ir

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. 12 No. 3 (2023), pp. 177-196.

www.ui.ac.ir

A SURVEY ON THE GROUP OF POINTS ARISING FROM ELLIPTIC CURVES WITH A WEIERSTRASS MODEL OVER A RING

MASSIMILIANO SALA AND DANIELE TAUFER*

Abstract. We survey the known group structures arising from elliptic curves defined by Weierstrass models over commutative rings with unity and satisfying a technical condition. For every considered base ring, the groups that may arise depending on the curve coefficients are recalled. When a complete classification is still out of reach, partial results about the group structure and relevant subgroups are provided. Several examples of elliptic curves over the inspected rings are presented, and open questions regarding the structure of their points are highlighted.

1. Introduction

Elliptic curves are ubiquitous objects in several fields such as number theory, arithmetic geometry and computational algebra (see [72, 4, 41], among others). Their main interest lies in the group structure of their points, making them the abelian varieties of smallest dimension.

Determining the structure of groups arising from such curves is a long-standing problem in mathematics, which still presents many open questions and bustling research lines. This question is intimately related to the precise determination of their rational points, as they prescribe the curve structure in all but small sporadic cases [42]. Thus, it is not surprising that the solution to such a problem heavily depends on the algebraic structure underlying the curve, as changing the base ring radically modifies the group of points.

Beyond their theoretical interest, the group structure of elliptic curves is crucial for the concrete adoption of such objects. In a cryptography purview, elliptic curves over fields have always been

Communicated by Patrizia Longobardi.

MSC(2010): Primary: 20E34; Secondary: 14H52.

Keywords: Elliptic curves, group of points, effective addition law.

Article Type: Ischia Group Theory 2020/2021.

Received: 23 December 2021, Accepted: 08 June 2022.

*Corresponding author.

http://dx.doi.org/10.22108/IJGT.2022.131984.1769 .

playing a prominent role [31, 35, 51], and they are recently rising further attention for their application to cryptocurrency design [47, 48]. Nevertheless, these objects have also been inspected and employed over different rings. As a few instances, cryptosystems based on elliptic curves defined over $\mathbb{Z}/N\mathbb{Z}$ [49], as well as those based on other finite rings [5] have been investigated.

In this work we provide a detailed overview of the structure of groups arising from elliptic curves over commutative rings with unity, presenting the known classification results and the main open questions regarding this subject. To ensure a definition of an effective addition law on such objects, we only require a technical condition on the linear algebra over the base ring. This way we deal with smooth projective curves admitting a Weierstrass model, whose group operation may be effectively outlined.

When the base ring is not a field, many unexpected phenomena may be observed, especially in presence of non-invertible elements or zero-divisors. These cases enrich the panorama of possible groups arising from these curves, which are expected to aid the research in several areas of algebra. Numerous examples are provided to highlight the use of the presented results for the group computation.

1.1. **Paper organization.** The basic definitions and preliminary results are collected in Section 2, which constitute the minimal requirements for the elliptic curves construction. Afterwards, the groups arising from elliptic curves over fields are discussed, as follows.

- In Section 3, the unique isomorphism class of complex curves is recalled.
- In Section 4, the two groups that may arise from real curves are described.
- In Section 5, the more varied cases of curves defined over number fields are discussed. A complete classification is still unknown even for number fields of small degree, such as $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}$ itself.
- In Section 6, elliptic curves over finite fields are treated, whose complete classification has been achieved in the 80's. These results are necessary for explaining the statements of sections 7 and 10.
- In Section 7, the curves defined over the field $\mathbb{Q}_p$ of p-adic numbers are examined.
- In Section 8, further results about other fields such as function fields $\mathbb{F}_q(T)$ and composite fields $\mathbb{Q}(d^\infty)$ are recalled.

Subsequently, elliptic curves over more general rings are surveyed, as follows.

- In Section 9, elliptic curves defined over rings of integers of number fields are presented.
- In Section 10, the complete classification of elliptic curves over $\mathbb{Z}/N\mathbb{Z}$ is presented.
- In Section 11, other rings are considered, such as $\mathbb{F}_q[x]/(x^k)$ and arbitrary products of suitable rings.

Finally, in Section 12 the information about the considered groups is systematized, and open problems are summarized.

1.2. **Notation.** Given a positive integer $m \in \mathbb{Z}_{>0}$, we denote by C_m the cyclic group of order m.

http://dx.doi.org/10.22108/IJGT.2022.131984.1769

Given a prime power $q = p^e \in \mathbb{Z}$, we will refer to the finite field of q elements by $\mathbb{F}_q$. When a primitive element $\alpha \in \mathbb{F}_q$ needs to be considered, the defining irreducible polynomial $f \in \mathbb{F}_p[x]$ will be specified.

Given an integer $N \in \mathbb{Z}$ and a prime p, will denote by $\mathrm{v}_p(N)$ the p-adic valuation of N, namely the exponent of p appearing in the prime factorization of N. Furthermore, we will denote by $\mathbb{Q}_p$ the field of p-adic numbers and by $\mathbb{Z}_p$ the ring of p-adic integers.

2. Basics

2.1. **The base ring.** Generalized elliptic curves may be defined over arbitrary base schemes S as proper smooth curves with geometrically connected genus-1 fibers, with a prescribed zero section. A theorem of Abel shows that such a definition always leads to a unique structure of commutative group-scheme over this curve [25, Theorem 2.1.2]. In particular, for every commutative ring R one can construct elliptic curves over the spectrum of R. However, with the latter definition we are not guaranteed we can embed the curve in a proper projective plane over S, and the resultant point-addition law may sometimes be only formal.

As in this work we are mostly interested in objects whose operations may be explicitly exhibited, we will restrict our attention to elliptic curves defined over commutative rings R with unity, such that R satisfies a technical condition [40, Section 3], which we now recall.

Definition 2.1 (Primitivity)**.** *A finite collection $\{x_i\}_{1\leq i\leq n} \subseteq R$ is called* primitive *if the ideal $\langle\{x_i\}_{1\leq i\leq n}\rangle$ it generates in R is equal to R itself.*

The following is the condition we will always require on the base rings we consider for defining elliptic curves, in order to prevent their addition law from having exceptional points.

Condition 2.2 (Suitable rings [40])**.** *Let R be a commutative ring with unity. For every rectangular matrix M over R, if the elements of M are primitive and every (2×2)-minor of M vanishes, then there exists an R-linear combination of the rows that is primitive.*

The above condition is trivially satisfied for every field: in this case, a tuple is primitive if and only if it contains a non-zero element, so an R-linear combination that evinces a primitive vector simply consists of selecting any row of M containing a non-zero element.

More generally, we also know that Condition 2.2 is satisfied whenever the ring R has finitely many maximal ideals [40, Section 3], thus in particular it holds for every finite ring. Moreover, we also know that when R is Dedekind, Condition 2.2 is equivalent to having a trivial class group. The above fact rules out a few interesting rings over which one might envision to construct elliptic curves, such as that of the following example.

http://dx.doi.org/10.22108/IJGT.2022.131984.1769

Example 2.3. *Let $K = \mathbb{Q}(\sqrt{-5})$ and let $R = \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ be its ring of integers, namely $R = \mathbb{Z}[\sqrt{-5}]$. We shall prove that such R does not satisfy Condition 2.2. Let us consider the matrix*

$$M = \begin{pmatrix} 2 & 1-\sqrt{-5} \\ 1+\sqrt{-5} & 3 \end{pmatrix}.$$

This matrix has primitive entries and its unique (2×2)-minor vanishes. However, for every $r_1, r_2 \in R$ the ideal

$$I_{r_1,r_2} = \langle 2r_1 + (1+\sqrt{5})r_2, (1-\sqrt{5})r_1 + 3r_2 \rangle \subseteq R$$

is always proper, as one can verify explicitly by showing the following implication:

$$\langle 2, 1+\sqrt{5} \rangle \subseteq I_{r_1,r_2} \implies \langle 2, 1+\sqrt{5} \rangle = I_{r_1,r_2}.$$

Hence, there may be no primitive R-linear combinations among the rows of M.

2.2. **The projective plane.** To discuss the group structure of smooth, plane and projective curves, we first need to recall some facts about the projective plane over a given ring.

Given a positive integer $n \in \mathbb{Z}_{\geq 1}$, it is easy to see that the group R^* of invertible elements of R acts on the primitive $(n+1)$-tuples of R via the component-wise multiplication

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

Definition 2.4 (Projective n-space)**.** *The* projective n-space over R*, denoted by $\mathbb{P}^n(R)$, is defined as the set of orbits of primitive tuples of R^{n+1} under the action (2.1). Whenever $n = 2$, it is called* projective plane*. Finally, we will denote by $(x_0 : \cdots : x_n) \in \mathbb{P}^n(R)$ the orbit of $(x_0, \dots, x_n) \in R^{n+1}$.*

Definition 2.5 (Affine and at infinity points)**.** *A point $(x_0 : \cdots : x_n) \in \mathbb{P}^n(R)$ is called* affine *if $x_n \in R^*$, while it is said to lie* at infinity *otherwise. When $n = 2$, the point at infinity $\mathcal{O} = (0 : 1 : 0)$ is simply called* zero*.*

When R is a field, the projective plane simply amounts to non-zero triples modulo non-zero multiples, i.e. its affine points are $\{(x_0 : x_1 : 1)\}_{x_0,x_1 \in R}$, while those at infinity are either $\{(x_0 : 1 : 0)\}_{x_0 \in R}$ or $(1 : 0 : 0)$. However, when the underlying ring has zero-divisors or non-invertible elements, it may have extremely different shapes, as in the following example.

Example 2.6. *Let $N \in \mathbb{Z}$ and consider $R = \mathbb{Z}/N\mathbb{Z}$.*

When $|N| > 1$ this ring is finite, hence it underlies Condition 2.2. Its invertible elements are integers coprime to N, and the primitive elements of R^n are the n-tuples of elements $(x_0, \dots, x_n)$ such that $\gcd(x_0, \dots, x_n, N) = 1$. It may also be proved [8, Section 10.3.2] *that the size of this projective space is*

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

Over such rings, the affine points may always be presented as $\{(x_0 : \cdots : x_{n-1} : 1)\}_{x_i \in R}$, but there are points at infinity with non-zero last coordinate, whenever N is composite.

http://dx.doi.org/10.22108/IJGT.2022.131984.1769

Let us now consider $N = 0$, i.e. $R = \mathbb{Z}$. Since it is a Dedekind principal ideal domain, then Condition 2.2 still holds. Its units are only ± 1, then its affine part is $\{(x_0 : \cdots : x_n)\}_{x_i \in \mathbb{Z}, x_n > 0}$, while the points at infinity are those having the last entry equal to 0.

The remaining cases $N = \pm 1$ are trivial, since R would be the zero-ring so $\mathbb{P}^n(R) = \{(0 : \cdots : 0)\}$.

2.3. **Elliptic curves.** In this work, we are interested in dealing with smooth plane projective curves defined by a Weierstrass equation, which over fields are proved to precisely correspond to smooth curves of genus one with a specified base point [62, Section III.3].

Definition 2.7 (Elliptic curve over R)**.** *Let R be a ring satisfying Condition 2.2 and $a_1, \dots, a_6 \in R$. If the projective set*

$$\{(X : Y : Z) \in \mathbb{P}^2(R) \mid Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\}$$

defines a smooth curve, then it is called elliptic curve *and it will be denoted by $E_{a_1,\dots,a_6}(R)$. If also*

$$a_1 = a_2 = a_3 = 0,$$

we will simply denote it by $E_{a_4,a_6}(R)$. Whenever the coefficients $\{a_i\}_i$ are understood or irrelevant, we shorten the notation as $E(R)$.

It is well-known that the smoothness of such a curve depends on the invertibility of its discriminant $\Delta_{a_1,\dots,a_6}$ [62, Section III.1]. When $6 \in R^*$, every elliptic curves may be written in the form $E_{A,B}(R)$ for some $A, B \in R$ satisfying

$$\Delta_{A,B} = -16(4A^3 + 27B^2) \in R^*.$$

An interested reader may find the remaining cases in [62, Appendix A].

We highlight that the considered assumptions on the base ring are necessary conditions for defining elliptic curves with efficient addition laws, but they are not sufficient to ensure the existence of such objects.

Example 2.8. *Let us consider $R = \mathbb{Z}$. Although it respects the conditions we posed on the underlying ring, no elliptic curves may be defined over such a ring. In fact, should such a curve exists, its Weierstrass equation would also define an elliptic curve over $\mathbb{Q}$ with good reduction at every prime. This is known to be not possible [67], as it may also be verified explicitly [55].*

Actually, we also know that no abelian varieties may exist over $\mathbb{Z}$, as it was proved independently by Fontaine [17] and Abrashkin [1].

2.4. **The group structure.** Elliptic curves constitute the genus-1 abelian varieties, those with dimension 1. In fact, it is known that when they are defined over a field an addition law may be defined on them [62, Section III.2], making $\mathcal{O}$ the identity element and imposing that whenever P_1, P_2, P_3 are aligned points on such a curve, then $P_1 + P_2 + P_3 = \mathcal{O}$. This operation may be explicitly described in terms of the coordinates of the given points on an open covering of the considered curve [3, **?**, 38].

http://dx.doi.org/10.22108/IJGT.2022.131984.1769

This addition law may also be extended to rings underlying Condition 2.2 as follows. Given two points $P_1 = (X_1 : Y_1 : Z_1)$ and $P_2 = (X_2 : Y_2 : Z_2)$ of $E(R)$, we define

$$V_1 = (X_3^{(1)}, Y_3^{(1)}, Z_3^{(1)}) \quad \text{and} \quad V_2 = (X_3^{(2)}, Y_3^{(2)}, Z_3^{(2)}),$$

where the above quantities are the polynomial relations in the entries of P_1 and P_2 defined in [3, Section 4], modulo the following corrections [2] to two minor typos:

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

The point $P_1+P_2 = (X_3 : Y_3 : Z_3)$ is defined as any primitive R-combination (X_3, Y_3, Z_3) of V_1 and V_2. In [40, Section 3] an algorithmic approach for computing this primitive vector is presented, and this operation is proved to provide $E(R)$ with an abelian group structure. Finally, we remark that if $E(R)$ has no points of order 2, then we simply have $P_1 + P_2 = (X_3^{(2)} : Y_3^{(2)} : Z_3^{(2)})$.

Example 2.9. *Let us consider $E = E_{0,1}(\mathbb{Z}/35\mathbb{Z})$ and $P = (20 : 21 : 15) \in E$. To perform $P + \mathcal{O}$, we compute*

$$(X_3^{(1)}, Y_3^{(1)}, Z_3^{(1)}) = (20, 0, 5), \quad (X_3^{(2)}, Y_3^{(2)}, Z_3^{(2)}) = (0, 21, 0).$$

We notice that none of the above triples is primitive, so they do not define points in $\mathbb{P}^2(\mathbb{Z}/35\mathbb{Z})$. However, for every $\alpha \in \mathbb{Z}$ such that $5 \nmid \alpha$, their combination

$$\left(X_3^{(1)}, Y_3^{(1)}, Z_3^{(1)}\right) + \alpha \cdot \left(X_3^{(2)}, Y_3^{(2)}, Z_3^{(2)}\right) = (20, 21\alpha, 15)$$

is primitive, and all these points correspond to $P = P + \mathcal{O}$ in $\mathbb{P}^2(\mathbb{Z}/35\mathbb{Z})$, since

$$(20, 21\alpha, 15) = (15 + 21\alpha) \cdot (20, 21, 15),$$

and $15 + 21\alpha \in (\mathbb{Z}/35\mathbb{Z})^*$.

3. Elliptic curves defined over $\mathbb{C}$

When an elliptic curve is defined over the complex field, its group structure is independent of the coefficients of its defining Weierstrass equation.

Given a lattice $\Lambda \subset \mathbb{C}$, the Weierstrass $\wp$-function relative to Λ is defined by

$$\wp_\Lambda : \mathbb{C} \to \mathbb{C} \cup \{\pm\infty\}, \quad z \mapsto \frac{1}{z^2} + \sum_{w \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

For every lattice Λ, the function $\wp_\Lambda$ is an even elliptic function, which converges absolutely and uniformly on every compact subset of $\mathbb{C} \setminus \Lambda$ [62, Theorem VI.3.1].

The well-known uniformization theorem identifies elliptic curves with complex tori, showing that for every elliptic curve $E(\mathbb{C}) = E/\mathbb{C}$ there exists a lattice $\Lambda \subset \mathbb{C}$ such that the map

$$\phi_\Lambda : \mathbb{C}/\Lambda \to E(\mathbb{C}), \quad z \to \left(\wp_\Lambda(z) : \wp'_\Lambda(z) : 1\right)$$

http://dx.doi.org/10.22108/IJGT.2022.131984.1769

is a complex analytic isomorphism of Lie groups [62, Section VI.5]. Thus, the group structure of elliptic curves over $\mathbb{C}$ is always

$$E(\mathbb{C}) \simeq \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}.$$

The above isomorphism implies that the torsion subgroup of $E(\mathbb{C})$ is isomorphic to

$$E(\mathbb{C})_{\text{tors}} \simeq \mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z},$$

and in particular the m-torsion points will be

$$E(\mathbb{C})[m] \simeq \mathrm{C}_m \times \mathrm{C}_m.$$

We also recall that the above results over $\mathbb{C}$ may be extended to every field of characteristic 0 by means of the Lefschetz Principle [62, Section VI.6].

Example 3.1. *Let $R = \overline{\mathbb{Q}}$ be the algebraic closure of the rationals, namely the field obtained from $\mathbb{Q}$ by adding the roots of any non-zero polynomial in $\mathbb{Z}[x]$. Under the canonical embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ every elliptic curve $E(\overline{\mathbb{Q}})$ is mapped into $E(\mathbb{C})$. Since $\overline{\mathbb{Q}}$ is algebraically closed, then the two torsion subgroups coincide, namely*

$$E(\overline{\mathbb{Q}})_{\text{tors}} \simeq \mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z}.$$

As an instance, let $\rho = e^{\frac{2\pi i}{3}}$ be a primitive 3-root of unity and consider the elliptic curve $E_{0,-\frac{1}{4}}(\overline{\mathbb{Q}})$, which lies inside the image of $\phi_{\mathbb{Z}+\rho\mathbb{Z}}$. One can explicitly verify that its 3-torsion subgroup is

$$E_{0,-\frac{1}{4}}(\overline{\mathbb{Q}})[3] = \left\langle \left(0 : \frac{i}{2} : 1\right) \right\rangle \oplus \left\langle \left(\rho : \frac{\sqrt{3}}{2} : 1\right) \right\rangle \simeq \mathrm{C}_3 \times \mathrm{C}_3.$$

4. **Elliptic curves defined over $\mathbb{R}$**

When the underlying ring is the field of reals $\mathbb{R}$, the group structure of $E(\mathbb{R})$ only depends on its discriminant Δ_E, in fact we have [61, Corollary V.2.3.1]

$$E(\mathbb{R}) \simeq \begin{cases} \mathbb{R}/\mathbb{Z} & \text{if } \Delta_E < 0, \\ \mathbb{R}/\mathbb{Z} \times \mathrm{C}_2 & \text{if } \Delta_E > 0. \end{cases}$$

This distinction reflects the topology of the curve: expressing $E_{A,B}(\mathbb{R})$ via its Weierstrass minimal model, when $\Delta_{A,B} < 0$ this curve has only one connected component, which is symmetric with respect to the affine x-axis given by $\{(x : 0 : 1)\}_{x\in\mathbb{R}}$. Hence, it may have only one intersection with that line, which implies that the points of order 2 are $\{\mathcal{O}, (r : 0 : 1)\}$, where $r \in \mathbb{R}$ is the unique real solution of the equation $x^3 + Ax + B = 0$. On the other side, when $\Delta_{A,B} > 0$ there are $r_1, r_2, r_3 \in \mathbb{R}$ such that $x^3 + Ax + B = (x - r_1)(x - r_2)(x - r_3)$, hence the points of order 2 in $E_{A,B}(\mathbb{R})$ are $\{\mathcal{O}, (r_1 : 0 : 1), (r_2 : 0 : 1), (r_3 : 0 : 1)\}$, which may occur because $E_{A,B}(\mathbb{R})$ has two connected components.

http://dx.doi.org/10.22108/IJGT.2022.131984.1769

Example 4.1. *Let us consider the elliptic curve* $E_{0,-\frac{1}{4}}(\mathbb{R})$ *with the same Weierstrass coefficients as that of Example* 3.1*, but defined over the real numbers. Since* $\Delta_{0,-\frac{1}{4}} = 27 < 0$*, this curve has one connected component which lies in the affine semiplane* $x \geq -\frac{1}{\sqrt[3]{4}}$*. Its points of order* 3 *form a subgroup of* $\mathrm{C}_3 \times \mathrm{C}_3$*, but since* $\mathbb{R}$ *is not algebraically closed it may be trivial. Indeed, it has no affine points of order* 3*, as its* 3*-torsion points are those computed in Example* 3.1*, which have complex entries.*

On the other side, the curve $E_{-\frac{1}{4},0}(\mathbb{R})$ *has discriminant* $\Delta_{-\frac{1}{4},0} = 1 > 0$*, it has three* 2*-torsion points and two connected components, lying respectively in the affine regions* $-\frac{1}{2} \leq x \leq 0$ *and* $x \geq \frac{1}{2}$*. Thus, its group of points is* $\mathbb{R}/\mathbb{Z} \times \mathrm{C}_2$*, with the* C_2 *part generated by* $(-\frac{1}{2} : 0 : 1)$*.*

5. Elliptic curves defined over number fields

5.1. **Elliptic curves over** $\mathbb{Q}$**.** When the curve is defined over the rationals, Mordell proved that its group of points is finitely generated [52], namely

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\mathrm{tors}} \times \mathbb{Z}^r,$$

where r is the rank of E and $E(\mathbb{Q})_{\mathrm{tors}}$ is its (finite) torsion subgroup. The latter is completely understood, as there are 15 possibilities by means of a theorem of Mazur [44, 45]:

$$E(\mathbb{Q})_{\mathrm{tors}} \simeq \begin{cases} \mathrm{C}_n & 1 \leq n \leq 10, \text{ or } n = 12, \\ \mathrm{C}_2 \times \mathrm{C}_{2n} & 1 \leq n \leq 4. \end{cases}$$

These torsion points may be effectively computed, since the Nagell-Lutz theorem [43] shows that when $(X : Y : 1) \in E(\mathbb{Q})_{\mathrm{tors}}$, then

$$x, y \in \mathbb{Z} \quad \text{and} \quad y = 0 \text{ or } y^2 \mid \Delta_E,$$

where Δ_E is the discriminant of the curve.

Instead, the possible ranks r are far from being understood: while it is often conjectured that such rank is unbounded, the largest known computable rank is 20 [15], even though an instance of elliptic curve with rank at least 28 [14] has been presented. Under the GRH, the latter rank was proved to be precisely 28 [29].

Example 5.1. *Let us consider the elliptic curve* $E_{7,0}(\mathbb{Q})$*. By means of Nagell-Lutz theorem, for computing its torsion part we only need to test the points* $(X : Y : 1) \in \mathbb{P}^2(\mathbb{Q})$ *with*

$$Y = 0 \quad \text{or} \quad Y^2 \mid \Delta_{7,0} = -2^6 7^3.$$

Let us assume $Y \neq 0$ *(then also* $X \neq 0$*). From the affine Weierstrass equation* $Y^2 = X(X^2 + 7)$ *we see that* Y *is even but neither* X *nor* Y *can be a power of* 2*. Moreover,* X *and* $X^2 + 7$ *have different parity but they multiply to a divisor of* $\Delta_{7,0}$*, and* $X^2 + 7$ *cannot be a power of* 7*. This implies that* $X = 7^b$ *for some* $0 \leq b \leq 3$*, but none of those cases lead a rational solution for* Y*. Hence, we conclude*

$$E_{7,0}(\mathbb{Q})_{\mathrm{tors}} = \{(0 : 0 : 1), \mathcal{O}\}.$$

http://dx.doi.org/10.22108/IJGT.2022.131984.1769

We also know that these are all the rational points of $E_{7,0}(\mathbb{Q})$*, as this example is a special case of* [62, Proposition X.6.2]*: given an odd prime* $p \in \mathbb{Z}$ *such that* $p \equiv 7, 11 \bmod 16$*, we always have*

$$E_{p,0}(\mathbb{Q}) \simeq \mathrm{C}_2.$$

5.2. **Higher-degree number fields.** Even less is known when the underlying field is a number field F of degree greater than 1. In its generalization of Mordell's theorem, Weil proved that the group of points is still finitely generated [71], i.e.

$$E(F) \simeq E(F)_{\mathrm{tors}} \times \mathbb{Z}^r.$$

In the quadratic case, there are only 26 possible different torsion groups [26, 24], namely

$$E(\mathbb{Q}(\sqrt{D}))_{\mathrm{tors}} \simeq \begin{cases} \mathrm{C}_n & 1 \leq n \leq 16, \text{ or } n = 18, \\ \mathrm{C}_2 \times \mathrm{C}_{2n} & 1 \leq n \leq 6, \\ \mathrm{C}_3 \times \mathrm{C}_{3n} & 1 \leq n \leq 2, \\ \mathrm{C}_4 \times \mathrm{C}_4. \end{cases}$$

For a general number field K of degree d, a complete classification is still an open problem, but much is known when d is small [64]. Among others, we recall for $d = 3$ the classification of torsion subgroups arising from elliptic curves over cyclic cubic fields [12] or from rational curves that have been base extended to cubic fields [53]. For higher degree extensions, we know the possible torsion orders for $4 \leq d \leq 7$ [11]. Moreover, the groups occurring infinitely often are known for $d \leq 6$ [33, 34, 13].

In the general case, the size of these groups may be bounded by the Merel's positive solution to the torsion conjecture for elliptic curves [50], which shows that for every number field K of degree d there exists a constant $B(d) \in \mathbb{Z}$ such that

$$|E(K)_{\mathrm{tors}}| \leq B(d).$$

A generalization of the theorem of Nagell-Lutz may be applied to detect certain torsion points [62, Therem VIII.7.1].

6. Elliptic curves over $\mathbb{F}_q$

Let $q = p^e \in \mathbb{Z}$ be a prime power. It is well-known [69, Theorem 4.1 and Corollary 3.11] that the group of points of an elliptic curve over such field may have rank at most 2, as there are positive integers $n, k \in \mathbb{Z}_{\geq 1}$ such that $n|(q-1)$ and

$$E(\mathbb{F}_q) \simeq \mathrm{C}_n \times \mathrm{C}_{nk}.$$

The groups arising this way depend on the trace of the considered curve, namely the trace of the Frobenius endomorphism of E, which is

$$t = q + 1 - |E_{A,B}(\mathbb{F}_q)|.$$

An elliptic curve of trace 1 is called *anomalous*, since it is isomorphic to its base field.

http://dx.doi.org/10.22108/IJGT.2022.131984.1769

The possible values of t are known to be constrained by the Hasse bound [62, Theorem V.1.1]:

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

Not every integer t in the above interval occurs as the trace of an elliptic curve over $\mathbb{F}_q$. In fact, Waterhouse proved [70, Theorem 4.1] that t is the trace of such a curve if and only if one of the following conditions holds:

(1) $(t,p)=1$,
(2) $t=\pm 2\sqrt{q}$ and e is even,
(3) $t=\pm\sqrt{q}$, $p\neq 1 \bmod 3$ and e is even,
(4) $t=\pm\sqrt{pq}$, $p\in\{2,3\}$ and e is odd,
(5) $t=0$ and either e is odd or $p\not\equiv 1 \bmod 4$.

In particular, this implies that the Hasse interval over prime fields is full. From the above result, a complete characterization of the possible groups of points for elliptic curves over finite fields has seen the light, independently discovered by Ruck [57] and Voloch [68]. They proved that the following is a complete list of the group structures of the elliptic curves of trace t defined over $\mathbb{F}_q$, where the enumeration corresponds to the above cases.

(1) Let $\prod_l l^{e_l}$ 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 its group of points is isomorphic to
$$\mathrm{C}_{p^{e_p}}\times\prod_{l\neq p}\left(\mathrm{C}_{l^{a_l}}\times\mathrm{C}_{l^{e_l-a_l}}\right).$$
(2) $\mathrm{C}_{\sqrt{q}\pm 1}\times\mathrm{C}_{\sqrt{q}\pm 1}$.
(3) Cyclic.
(4) Cyclic.
(5) The group is
$$\begin{cases}\mathrm{C}_2\times\mathrm{C}_{\frac{q+1}{2}}\text{ or cyclic} & \text{if } q\equiv 3 \bmod 4,\\ \text{cyclic} & \text{if } q\not\equiv 3 \bmod 4.\end{cases}$$

Although the groups arising from curves over finite fields have been completely classified, the frequency with which they occur is still a field of open research [16].

Example 6.1. *Let us consider* $\mathbb{F}_{25}=\mathbb{F}_5[x]/(x^2+4x+2)=\mathbb{F}_5(\alpha)$, *over which an elliptic curve* $E_{A,B}(\mathbb{F}_{25})$ *of size* 20 *(equiv. of trace* $t=6$*) is defined. Since* $\gcd(t,p)=1$ *we are in case (i) of the above result: from* $20=2^2 5$ *we get* $e_2=2, e_5=1$, *hence* $0\leq a_2\leq 1$, *i.e. the possible groups arising from curves of trace* t *over* $\mathbb{F}_{25}$ *are precisely*

$$E_{A,B}(\mathbb{F}_{25})\simeq\begin{cases}\mathrm{C}_{20} & \text{for } a_2=0,\\ \mathrm{C}_2\times\mathrm{C}_{10} & \text{for } a_2=1.\end{cases}$$

One can verify that the first case is achieved for

$$E_{3,\alpha}(\mathbb{F}_{25})=\langle(\alpha:\alpha^8:1)\rangle\simeq\mathrm{C}_{20},$$

http://dx.doi.org/10.22108/IJGT.2022.131984.1769

while the second case holds for

$$E_{2,0}(\mathbb{F}_{25}) = \langle (0:0:1) \rangle \oplus \langle (\alpha:\alpha:1) \rangle \simeq \mathrm{C}_2 \times \mathrm{C}_{10}.$$

7. Elliptic curves over finite extensions of $\mathbb{Q}_p$

Let $R = \mathbb{Q}_p$ be the field of p-adic numbers and K be a finite extension of degree $d = [K : \mathbb{Q}_p]$. Let $\mathcal{O}_K$ be the local ring of integers of K, whose maximal ideal is $\mathfrak{m}$, and let $\kappa = \mathcal{O}_K/\mathfrak{m}$ be its residue field.

For every local field we classically define a reduction morphism $\sim : \mathcal{O}_K \to \kappa$ [62, Section VII.2], which may be extended to the curve map

$$\sim : E_{a_i}(K) \to E_{\tilde{a_i}}(\kappa), \quad (X:Y:Z) \mapsto (\tilde{X}:\tilde{Y}:\tilde{Z}).$$

The group structure of $E_{a_i}(K)$ depends on the landing curve $E_{\tilde{a_i}}(\kappa)$, which needs not to be elliptic:

- if $E_{\tilde{a_i}}(\kappa)$ is smooth, the reduction is called good (or stable),
- if $E_{\tilde{a_i}}(\kappa)$ has a node, the reduction is called multiplicative (or semistable),
- if $E_{\tilde{a_i}}(\kappa)$ has a cusp, the reduction is called additive (or unstable).

The case of multiplicative reduction is referred to as split reduction when the slope of the tangent lines at the node belongs to κ.

The set $E_{\mathrm{ns}} \subseteq E_{\tilde{a_i}}(\kappa)$ of nonsingular points of the reduced curve still forms a group [62, Proposition III.2.5]. Let $E_0(K) \subseteq E(K)$ be the set of points reducing to points in E_{ns}. The complete classification of special fibers of a Néron model [61, Section IV.8] shows that

$$E(K)/E_0(K) \simeq \begin{cases} \mathrm{C}_{\mathrm{v}_p(\Delta)} & \text{if } E \text{ has split multiplicative reduction,} \\ \mathrm{C}_n \text{ or } \mathrm{C}_2 \times \mathrm{C}_2 & 1 \leq n \leq 4, \text{ otherwise.} \end{cases}$$

Thus, the groups of points arising over K depend on those of $E_0(K)$.

The kernel $E_1(K) \subseteq E_0(K)$ of the reduction map is known to be isomorphic to the formal group associated to E [62, Proposition VII.2.2], and

$$0 \to E_1(K) \to E_0(K) \xrightarrow{\sim} E_{\mathrm{ns}} \to 0,$$

is a short exact sequence of groups [62, Proposition VII.2.1].

If the reduction is good, then we have $E(K) = E_0(K)$ and $E(\kappa) = E_{\mathrm{ns}}$, thus recovering the group structure of $E(K)$ amounts to investigating when the above sequence splits. In particular, for $K = \mathbb{Q}_p$ we have $E_1(\mathbb{Q}_p) \simeq \mathbb{Z}_p$, hence when the above sequence admits a section we get

$$E_{a_i}(\mathbb{Q}_p) \simeq \mathbb{Z}_p \times E_{\tilde{a_i}}(\mathbb{F}_p).$$

http://dx.doi.org/10.22108/IJGT.2022.131984.1769

The additive reductions have been studied in [32]: if $K/\mathbb{Q}_p$ is unramified, then we have the $\mathbb{Z}_p$-modules isomorphism

$$E_0(K) \simeq \begin{cases} (\mathbb{Z}_p)^d \times (\mathrm{C}_p)^b, & 0 \leq b \leq 2, \text{ if } p = 2, \\ (\mathbb{Z}_p)^d \times (\mathrm{C}_p)^b, & 0 \leq b \leq 1, \text{ if } p \in \{3, 5, 7\}, \\ (\mathbb{Z}_p)^d & \text{otherwise.} \end{cases}$$

while if the ramification index e is such that $1 < e < \frac{p-1}{6}$, then we have

$$E_0(K) \simeq (\mathbb{Z}_p)^d.$$

As a corollary, we obtain the structure of $E_0(\mathbb{Q}_p)$ with additive reduction in terms of its Weierstrass coefficients $a_1, \ldots, a_6$:

$$E_0(\mathbb{Q}_p) \simeq \mathbb{Z}_p \text{ or } \mathbb{Z}_p \times \mathrm{C}_p,$$

where the latter occurs precisely if one of the following conditions holds:

- $p = 2$, and $a_1 + a_3 \equiv 2 \bmod 4$,
- $p = 3$, and $a_2 \equiv 6 \bmod 9$,
- $p = 5$, and $a_4 \equiv 10 \bmod 25$,
- $p = 7$, and $a_6 \equiv 14 \bmod 49$.

Example 7.1. *Let $E = E_{-2,0}(\mathbb{Q}_3)$. Since this curve has good reduction then*

$$0 \to \mathbb{Z}_3 \to E \xrightarrow{\sim} E_{-2,0}(\mathbb{F}_3) \to 0,$$

is a short exact sequence of groups. It is easy to verify that

$$E_{-2,0}(\mathbb{F}_3) = \langle (1:2:1) \rangle \simeq \mathrm{C}_4,$$

and this point may be lifted to a point of E which has still order 4, since 1 is a root of the 4-division polynomial ψ_4 [62, Exercise 3.7], namely the polynomial whose roots are the abscissas of the 4-torsion points of the curve, but 1 is not a root of its derivative ψ_4'. Thus, we conclude that $E \simeq \mathbb{Z}_3 \times \mathrm{C}_4$.

8. Elliptic curves over other fields

Elliptic curves defined over other base fields F have been investigated by several authors, who usually aim at detecting the possible structures arising from their torsion subgroups.

Instances of finitely generated groups of points arise when $F = \mathbb{F}_q(T)$ is the function field of a finite field [36]. In such cases, the torsion groups that can appear, and appear infinitely often, have been characterized [46].

On the other side, let $F = \mathbb{Q}(d^\infty)$ be the compositum of all the number fields of degree d. Although we know that over such a field elliptic curves are not finitely generated, the torsion subgroups are finite and completely classified in cases $d = 2$ [18, 19, 39] and $d = 3$ [10], as follows.

http://dx.doi.org/10.22108/IJGT.2022.131984.1769

$$E\big(\mathbb{Q}(2^\infty)\big)_{\text{tors}} \simeq \begin{cases} \mathrm{C}_n & n \in \{1,3,5,7,9,15\}, \\ \mathrm{C}_2 \times \mathrm{C}_{2n} & n \in \{1,2,3,4,5,6,8\}, \\ \mathrm{C}_4 \times \mathrm{C}_{4n} & n \in \{1,2,3,4\}, \\ \mathrm{C}_n \times \mathrm{C}_n & n \in \{3,6,8\}. \end{cases}$$

$$E\big(\mathbb{Q}(3^\infty)\big)_{\text{tors}} \simeq \begin{cases} \mathrm{C}_2 \times \mathrm{C}_{2n} & n \in \{1,2,4,5,7,8,13\}, \\ \mathrm{C}_4 \times \mathrm{C}_{4n} & n \in \{1,2,4,7\}, \\ \mathrm{C}_6 \times \mathrm{C}_{6n} & n \in \{1,2,3,5,7\}, \\ \mathrm{C}_n \times \mathrm{C}_n & n \in \{8,12,14,18\}. \end{cases}$$

Another relevant instance of infinite algebraic extension of the rationals is its maximal abelian extension $F = \mathbb{Q}^{ab} = \mathbb{Q}(\{\zeta_n\}_{n\in\mathbb{Z}_{>0}})$, where ζ_n denotes a primitive n-th root of unity. We know that elliptic curves defined over *large* fields of zero-characteristic have an infinite rank, and this was proved true for $\mathbb{Q}^{ab}$ under certain hypotheses [30]. However, abelian varieties over $\mathbb{Q}^{ab}$ have been proved to always have finite torsion subgroups [56]. In fact, for elliptic curves we have a complete classification of such groups [6], as follows.

$$E\big(\mathbb{Q}^{ab}\big)_{\text{tors}} \simeq \begin{cases} \mathrm{C}_n & n \in \{1,3,5,7,9,11,13,15,17,19,21,25,27,37,43,67,163\}, \\ \mathrm{C}_2 \times \mathrm{C}_{2n} & 1 \leq n \leq 9, \\ \mathrm{C}_3 \times \mathrm{C}_{3n} & n \in \{1,3\}, \\ \mathrm{C}_4 \times \mathrm{C}_{4n} & n \in \{1,2,3,4\}, \\ \mathrm{C}_n \times \mathrm{C}_n & n \in \{5,6,8\}. \end{cases}$$

9. **Elliptic curves over rings of integers**

In this section we consider the rings of integer R of number fields F with trivial class groups, as those are the only rings of integers satisfying Condition 2.2 [40, Section 3].

As already discussed in Example 2.8, such curves may be smooth only if there are elliptic curves over F with everywhere good reduction, whose detection is a problem that has attracted considerable attention and that carries its own interest [7]. In the same example, we recalled that this may never occur for $F = \mathbb{Q}$, thus we will consider number fields of degree at least 2.

It is crucial to observe that no elliptic curves with short Weierstrass form may have everywhere good reduction, since $2|\Delta_{A,B}$ for every choice of $A, B \in F$. Thus, general addition laws [3] need to be used.

9.1. **Quadratic fields.** Let us here assume that $F = \mathbb{Q}(\sqrt{d})$. It is known that there are only 9 imaginary quadratic fields with trivial class group [54, Section I.6]. In all such cases, we know that

http://dx.doi.org/10.22108/IJGT.2022.131984.1769

there are no elliptic curves with everywhere good reduction [63], thus there are no elliptic curves as of Definition 2.7 over their rings of integers.

The case of real quadratic fields is more varied. There are many (conjectured: infinitely many [54, Section I.6]) such fields for positive values of d, such as $2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, \ldots$ (see OEIS: A003172). Over such fields, many of them (e.g. $d \in \{2, 3, 5, 11, 13, 17, 19, 21, 23, \ldots\}$) do not admit elliptic curves with everywhere good reduction [60, Theorem 4]. In the remaining cases, there are instances where the existence of such curves is still open (e.g. $d \in \{51, 62, 67, \ldots\}$), while there are cases where we know that such curves exist, namely $d \in \{6, 7, 14, 22, 29, \ldots\}$. Several authors have investigated algorithmic ways of producing such curves [9, 27]. For certain small values of d, elliptic curves with everywhere good reduction are completely determined and their structures have been classified [20, 21, 22, 23, 28]. Nevertheless, we do not have a complete characterization of the possible curves with everywhere good reduction arising from the remaining cases yet.

Moreover, no dedicated investigation had been conducted on the group structures of elliptic curves over the ring of integers of such admissible number fields. In fact, given number field F with ring of integers R, and an elliptic curve $E_{a_1,\ldots,a_6}(F)$ with everywhere good reduction, we know that $E_{a_1,\ldots,a_6}(R)$ is a subgroup of $E_{a_1,\ldots,a_6}(F)$, but it might be proper, as in the following example.

Example 9.1. *Let $F = \mathbb{Q}(\sqrt{22})$ and let R be its ring of integers, namely $R = \mathbb{Z}[\sqrt{22}]$. Over this field, there are (up to isomorphism) two elliptic curves with everywhere good reduction [curves `2.2.88.1-1.1-a1` and `2.2.88.1-1.1-a2` of LMFDB database], and their groups of points are both isomorphic to C_2. Let us consider the first one, the curve E defined by the equation*

$$Y^2Z + \sqrt{22}XYZ + (\sqrt{22}+1)YZ^2 = X^3 + X^2Z + (-18\sqrt{22}-79)XZ^2 + (38\sqrt{22}+185)Z^3,$$

whose group is cyclic, as

$$E(F) = \langle (4\sqrt{22}+10 : -7\sqrt{22}-46 : 4) \rangle \simeq \mathrm{C}_2.$$

We computationally verify that this curve has indeed everywhere good reduction, since its discriminant $\Delta_E = 6519870\sqrt{22} + 30580901$ satisfies

$$(30580901 - 6519870\sqrt{22})\Delta_E = 30580901^2 - 22 \cdot 6519870^2 = 1.$$

Thus, the same Weierstrass coefficients define an elliptic curve over the ring of integers $R = \mathbb{Z}[\sqrt{22}]$ of F. However, it is easy to see that

$$\langle 4\sqrt{22}+10, -7\sqrt{22}-46, 4 \rangle_R = \langle 2, \sqrt{22} \rangle \subsetneq R.$$

Thus, the torsion generator over F is not a point inside $\mathbb{P}^2(R)$, so we conclude

$$E_{\sqrt{22},1,\sqrt{22}+1,-18\sqrt{22}-79,38\sqrt{22}+185}(R) = \langle \mathcal{O} \rangle \simeq \mathrm{C}_1.$$

http://dx.doi.org/10.22108/IJGT.2022.131984.1769

9.2. **Higher degree number fields.** If the quadratic case still presents several challenges to be tackled, even less is known for higher degree number fields. Among them, many have class number one, but curves with everywhere good reduction over them are far from being understood.

In [65] special families of cubic number fields admitting elliptic curves with everywhere good reduction have been characterized, while the same problem over number fields of a given degree has been considered in [66].

The case of cyclotomic fields has also been investigated [59], but we miss complete classification results over such fields as well.

Given that, not much is known in general on the groups arising from these rings, and their classification remains an open and intriguing problem.

10. **Elliptic curves over** $\mathbb{Z}/N\mathbb{Z}$

Given a positive integer $N \in \mathbb{Z}_{>0}$, the groups arising from elliptic curved defined over $\mathbb{Z}/N\mathbb{Z}$ have been investigated in [40]. In particular, when $N = p^e$ is a power of a prime the group order is $p^{e-1}|E_{A,B}(\mathbb{F}_p)|$, while composite N's may be addressed via the Chinese Reminder Theorem.

In the unpublished paper [58] the exact determination of the group structure is exhibited. To be more precise, the group of points of an elliptic curve $E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ depends on whether the projected curve over $\mathbb{F}_p$ is anomalous, namely

$$E_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) \simeq \begin{cases} E_{A,B}(\mathbb{F}_p) \times \mathrm{C}_{p^{e-1}} & \text{if } |E_{A,B}(\mathbb{F}_p)| \neq p, \\ \mathrm{C}_{p^e} \text{ or } \mathrm{C}_p \times \mathrm{C}_{p^{e-1}} & \text{if } |E_{A,B}(\mathbb{F}_p)| = p. \end{cases}$$

By applying the Chinese Reminder Theorem to the curves defined over coprime components of N, we obtain every possible group arising from elliptic curves over $\mathbb{Z}/N\mathbb{Z}$ [58, Theorem 20]:

$$E_{A,B}(\mathbb{Z}/N\mathbb{Z}) \simeq \prod_{\substack{p|N \\ |E_{A,B}(\mathbb{F}_p)|\neq p}} \left(E_{A,B}(\mathbb{F}_p) \times \mathrm{C}_{p^{\mathrm{v}_p(N)-1}}\right) \times \prod_{\substack{p|N \\ |E(\mathbb{F}_p)|=p}} G_p,$$

where every G_p may be either $\mathrm{C}_{p^{\mathrm{v}_p(N)}}$ or $\mathrm{C}_p \times \mathrm{C}_{p^{\mathrm{v}_p(N)-1}}$.

The rank of elliptic curves over such rings may be arbitrarily high, but it has been sharply bounded in terms of the considered N [58, Proposition 23].

Example 10.1. *We consider the curve* $E = E_{63707931,239467091}(\mathbb{Z}/659902243\mathbb{Z})$. *One may straightforwardly check that every point of* E *has order* 13, *since we have*

$$E \simeq (\mathrm{C}_{13})^8.$$

In fact, this group has the largest rank among those of the above type [58, Example 25], *since every* 13*-group arising from an elliptic curve over* $\mathbb{Z}/N\mathbb{Z}$ *has rank not greater than* 8.

http://dx.doi.org/10.22108/IJGT.2022.131984.1769

11. Other rings

Other finite rings have been considered for constructing elliptic curves. Given a prime power $q = p^e \in \mathbb{Z}$ and an elliptic curve E over $R_k = \mathbb{F}_q[x]/(x^k) \simeq \mathbb{F}_q(\epsilon)$, we know that the infinity part of $E(R)$ is a p-group [40, Section 4]. There have been some attempts to classify the group of such curves: in [5] it is claimed that elliptic curves with a short Weierstrass model with a non-anomalous projection may be decomposed as

$$E_{A_0+A_1\epsilon,B_0+B_1\epsilon}(R_n) \simeq E_{A_0,B_0}(\mathbb{F}_q) \times \mathbb{F}_q^{k-1}.$$

However, this result appears to hold only for certain rings R_n. In fact, in general there may be points at infinity of order strictly greater than p, as portrayed by the following example.

Example 11.1. *Let $R = \mathbb{F}_7[x]/(x^8) \simeq \mathbb{F}_7(\epsilon)$, and let us consider the elliptic curve $E = E_{6,2}(R)$. We also consider its point at infinity*

$$P = (\epsilon : 1 : \epsilon^3 + 6\epsilon^7).$$

One can verify that

$$7P = (6\epsilon^7 : 1 : 0), \quad 49P = \mathcal{O},$$

thus P is a point of E of order 49, showing that the characteristic of a ring needs not to be the order of the infinity part of an elliptic curve constructed over that ring.

Finally, we point out that given a finite set of elliptic curves $\{E_{a_i^{(j)}}(R_j)\}_{1\le j\le n}$, we can construct an elliptic curve over the ring $\prod_{j=1}^n R_j$ with componentwise operation, whose group of points is simply

$$E_{A_1,\dots,A_6}\left(\prod_{j=1}^n R_j\right) \simeq \prod_{j=1}^n E_{a_1^{(j)},\dots,a_6^{(j)}}(R_j),$$

where $A_i = \left(a_i^{(1)}, a_i^{(2)}, \dots, a_i^{(n)}\right)$ for $i \in \{1,2,3,4,6\}$.

This way, a large assortment of groups may be achieved, by simply combining those discussed in the present work.

12. Final comments and open problems

We have surveyed the group structure arising from elliptic curves defined by a Weierstrass equation over rings satisfying Condition 2.2. Although for such abelian varieties a group law may be explicitly defined in terms of the coordinates of their projective points, the determination of their group structure is often challenging and still presents many unknown facets. The following is a summary of the main rings considered in this work, with the corresponding groups classification.

http://dx.doi.org/10.22108/IJGT.2022.131984.1769

Base ring	Paper section	Group structure
$\mathbb{C}$	3	$\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$
$\mathbb{R}$	4	$\mathbb{R}/\mathbb{Z}$ or $\mathbb{R}/\mathbb{Z} \times \mathrm{C}_2$
$\mathbb{Q}$, $\mathbb{Q}(\sqrt{D})$	5	torsion classified, rank open
Number fields of degree > 2	5	open
$\mathbb{F}_q$	6	all classified: cyclic or rank 2
$\mathbb{Q}_q$	7	open, depending on the reduction
$\mathbb{F}_q(T)$	8	torsion classified, rank open
$\mathbb{Q}(d^\infty)$	8	torsion classified for $d \in \{2, 3\}$, rank ∞
$\mathbb{Q}^{ab}$	8	torsion classified, rank open
Rings of integer of number fields	9	open
$\mathbb{Z}/N\mathbb{Z}$	10	all classified
$\mathbb{F}_q[x]/(x^k)$	11	open for large values of k

FIGURE 1. Group structures of elliptic curves defined over the given ring.

From the present work it is evident that much more research has been conducted for curves defined over fields, as they are the structures over which their group law has first been discovered. However, many more rings might be considered to perform similar constructions, and their groups of points may conceivably constitute a fertile field of both abstract objects and tools for concrete applications. As an instance, cryptographic protocols may be designed and proved secure over elliptic curves, when relations inside their groups of points cannot be explicitly reduced to efficient finite arithmetic. The construction of such curves is often linked to other thought-provoking problems, as is the case for the classification of curves with everywhere good reduction in order to define elliptic curves over rings of integers.

Acknowledgments

This article has been supported in part by the European Union's H2020 Programme under grant agreement number ERC-669891. The authors want to thank the anonymous reviewer for the detailed comments and many useful suggestions.

References

[1] V. A. Abrashkin, Galois modules of group schemes of period p over the ring of Witt vectors, *Izv. Akad. Nauk SSSR Ser. Mat.*, **51** (1987) 691–736.

[2] D. J. Bernstein and T. Lange, A complete set of addition laws for incomplete Edwards curves, *J. Number Theory*, **131** (2011) 858–872.

http://dx.doi.org/10.22108/IJGT.2022.131984.1769

[3] W. Bosma and H. W. Lenstra, Complete systems of two addition laws for elliptic curves, *J. Number Theory*, **53** (1995) 229–240.

[4] C. Breuil, B. Conrad, F. Diamond and R. Taylor, On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises, *J. Amer. Math. Soc.*, **14** (2001) 843–939.

[5] A. Chillali and L. El Fadil, *Elliptic Curve over a Local Finite Ring Rn*, in Number Theory and Its Applications, IntechOpen (2020).

[6] M. Chou, Torsion of rational elliptic curves over the maximal abelian extension of $\mathbb{Q}$, *Pacific J. Math.*, **302** (2019) 481–509.

[7] A. Clemm and S. Trebat-Leder, Elliptic curves with everywhere good reduction, *J. Number Theory*, **161** (2016) 135–145.

[8] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, **138**, Springer-Verlag, Berlin, 1993.

[9] J. E. Cremona and M. P. Lingham, Finding all elliptic curves with good reduction outside a given set of primes, *Experiment. Math.*, **16** (2007) 303–312.

[10] H. B. Daniels, A. Lozano-Robledo, F. Najman and A. V. Sutherland, Torsion subgroups of rational elliptic curves over the compositum of all cubic fields, *Math. Comp.*, **87** (2018) 425–458.

[11] M. Derickx, S. Kamienny, W. Stein and M. Stoll, Torsion points on elliptic curves over number fields of small degree, arXiv:1707.00364, (2021).

[12] M. Derickx and F. Najman, Torsion of elliptic curves over cyclic cubic fields, *Math. Comp.*, **88** (2019) 2443–2459.

[13] M. Derickx and A. V. Sutherland, Torsion subgroups of elliptic curves over quintic and sextic number fields, *Proc. Amer. Math. Soc.*, **145** (2017) 4233–4245.

[14] N. D. Elkies, $\mathbb{Z}^{28}$ in $E(\mathbb{Q})$, etc., *Number Theory Listserver*, 2006.

[15] N. D. Elkies and Z. Klagsbrun, New rank records for elliptic curves having rational torsion, arXiv:2003.00077 (2020).

[16] R. R. Farashahi and I. E. Shparlinski, On group structures realized by elliptic curves over a fixed finite field, *Exp. Math.*, **21** (2012) 1–10.

[17] J. M. Fontaine, Il n'y a pas de variété abélienne sur $\mathbb{Z}$, *Invent. Math.*, **81** (1985) 515–538.

[18] Y. Fujita, Torsion subgroups of elliptic curves with non-cyclic torsion over $\mathbb{Q}$ in elementary abelian 2-extensions of $\mathbb{Q}$, *Acta Arith.*, **115** (2004) 29–45.

[19] Y. Fujita, Torsion subgroups of elliptic curves in elementary abelian 2-extensions of $\mathbb{Q}$, *J. Number Theory*, **114** (2005) 124–134.

[20] T. Kagawa, Determination of elliptic curves with everywhere good reduction over $\mathbf{Q}(\sqrt{37})$, *Acta Arith.*, **83** (1998) 253–269.

[21] T. Kagawa, Determination of elliptic curves with everywhere good reduction over real quadratic fields, *Arch. Math. (Basel)*, **73** (1999) 25–32.

[22] T. Kagawa, Determination of elliptic curves with everywhere good reduction over real quadratic fields $\mathbb{Q}(\sqrt{3p})$, *Acta. Arith.*, **96** (2001) 231–245.

[23] T. Kagawa, Torsion Groups of Elliptic Curves with Everywhere Good Reduction over Quadratic Fields, *Int. J. Algebra*, **10** (2016) 461–467.

[24] S. Kamienny, Torsion points on elliptic curves and q-coefficients of modular forms, *Invent. Math.*, **109** (1992) 221–229.

[25] N. M. Katz and B. Mazur, *Arithmetic Moduli of Elliptic Curves*, Annals of Mathematics Studies, **108**, Princeton University Press, Princeton, NJ, 1985.

[26] M. A. Kenku and F. Momose, Torsion points on elliptic curves defined over quadratic fields, *Nagoya Math. J.*, **109** (1988) 125–149.

http://dx.doi.org/10.22108/IJGT.2022.131984.1769

[27] M. Kida, Computing elliptic curves having good reduction everywhere over quadratic fields, *Tokyo J. Math.*, **24** (2001) 545–558.

[28] M. Kida, Reduction of elliptic curves over certain real quadratic number fields, *Math. Comp.*, **68** (1999) 1679–1685.

[29] Z. Klagsbrun, T. Sherman and J. Weigandt, The Elkies curve has rank 28 subject only to GRH, *Math. Comp.*, **88** (2019) 837–846.

[30] E. Kobayashi, A remark on the Mordell-Weil rank of elliptic curves over the maximal abelian extension of the rational number field, *Tokyo J. Math.*, **29** (2006) 295–300.

[31] N. Koblitz, Elliptic curve cryptosystems, *Math. Comp.*, **48** (1987) 203–209.

[32] M. Kosters and R. Pannekoek, On the structure of elliptic curves over finite extensions of $\mathbb{Q}_p$ with additive reduction, (2017), arXiv:1703.07888.

[33] D. Jeon, C. H. Kim and A. Schweizer, On the torsion of elliptic curves over cubic number fields, *Acta Arith.*, **113** (2004) 291–301.

[34] D. Jeon, C. H. Kim and E. Park, On the torsion of elliptic curves over quartic number fields, *J. London Math. Soc. (2)*, **74** (2006), pp. 1–12.

[35] D. Johnson, A. Menezes and S. Vanstone, The Elliptic Curve Digital Signature Algorithm (ECDSA), *Int. J. Inf. Secur.*, (2001) 36–63.

[36] S. Lang and A. Néron, Rational points of abelian varieties over function fields, *Amer. J. Math.*, **81** (1959) 95–118.

[37] H. Lange and W. Ruppert, Complete systems of addition laws on abelian varieties, *Invent. Math.*, **79** (1985) 603–610.

[38] H. Lange and W. Ruppert, Addition laws on elliptic curves in arbitrary characteristics, *J. Algebra*, **107** (1987) 106–116.

[39] M. Laska and M. Lorenz, Rational points on elliptic curves over $\mathbf{Q}$ in elementary abelian 2-extensions of $\mathbf{Q}$, *J. Reine Angew. Math.*, **355** (1985) 163–172.

[40] H. W. Lenstra, Elliptic curves and number-theoretic algorithms, *Proceedings of the International Congress of Mathematicians*, **1, 2** (1986) 99–120.

[41] H. W. Lenstra, Factoring integers with elliptic curves, *Ann. of Math. (2)*, **126** (1987) 649–673.

[42] H. W. Lenstra and J. Pila, *Does the set of points of an elliptic curve determine the group?*, Computational algebra and number theory (Sydney, 1992), Math. Appl., **325**, Kluwer Acad. Publ., Dordrecht, 1995 111–118.

[43] E. Lutz, Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps p-adiques, *J. Reine Angew. Math.*, **177** (1937) 237–247.

[44] B. Mazur, Modular curves and the Eisenstein ideal, *Inst. Hautes Études Sci. Publ. Math.*, no. 47 (1977) 33–186.

[45] B. Mazur, Rational isogenies of prime degree, *Invent. Math.*, **44** (1978) 129–162.

[46] R. J. S. McDonald, Torsion subgroups of elliptic curves over function fields of genus 0, *J. Number Theory*, **193** (2018) 395–423.

[47] A. Meneghetti, M. Sala and D. Taufer, A survey on PoW-based consensus, *AETiC*, **4** (2020) 8–18.

[48] A. Meneghetti, M. Sala and D. Taufer, A New ECDLP-Based PoW Model, *Mathematicsl*, **8** (2020) pp. 11.

[49] B. Meyer and V. Müller, *A public key cryptosystem based on elliptic curves over* $\mathbf{Z}/n\mathbf{Z}$ *equivalent to factoring.*, Advances in cryptology—EUROCRYPT '96, Lecture Notes in Comput. Sci., **1070**, Springer, Berlin, 1996 49–59.

[50] L. Merel, Bornes pour la torsion des courbes elliptiques sur les corps de nombres, *Invent. Math.*, **124** (1996) 437–449.

[51] V. S. Miller, *Use of elliptic curves in cryptography*, Advances in cryptology—CRYPTO '85 (Santa Barbara, Calif., 1985), Lecture Notes in Comput. Sci., **218**, Springer, Berlin, 1986 417–426.

[52] L. J. Mordell, On the rational solutions of the indeterminate equations of the third and fourth degrees, *Proc. Camb. Phil. Soc.*, **21** (1922) 179–192.

[53] F. Najman, Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$, *Math. Res. Lett.*, **23** (2016) 245–272.

[54] J. Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag (1999).

[55] A. Ogg, Abelian curves of 2-power conductor, *Proc. Cambridge Philos. Soc.*, **62** (1966) 143–148.

http://dx.doi.org/10.22108/IJGT.2022.131984.1769

[56] K. Ribet, Torsion points of abelian varieties in cyclotomic extensions, *Enseign. Math.*, **27** (1981) 315–319.

[57] H. G. Rück, A Note on Elliptic Curves Over Finite Fields, *Math. Comp.*, **49** (1987) 301–304.

[58] M. Sala and D. Taufer, The group structure of elliptic curves over $\mathbb{Z}/N\mathbb{Z}$, (2020), arXiv:2010.15543.

[59] R. Schoof, Abelian varieties over cyclotomic fields with good reduction everywhere, *Math. Ann.*, **325** (2003) 413–448.

[60] B. Setzer, Elliptic curves over complex quadratic fields, *Pacific J. Math.*, **74** (1978) 235–250.

[61] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, **151**, Springer-Verlag, New York, 1994.

[62] J. H. Silverman, *The arithmetic of elliptic curves* Second edition, Graduate Texts in Mathematics, **106**, Springer, Dordrecht, 2009.

[63] R. J. Stroeker,Reduction of elliptic curves over imaginary quadratic number fields, *Pacific J. Math.*, **108** (1983) 451–463.

[64] A. V. Sutherland, Torsion subgroups of elliptic curves over number fields, Preprint (2012). Available at https://math.mit.edu/~drew/MazursTheoremSubsequentResults.pdf.

[65] N. Takeshi, Elliptic curves with good reduction everywhere over cubic fields, *Int. J. Number Theory*, **11** (2015) 1149–1164.

[66] N. Takeshi, Family of elliptic curves with good reduction everywhere over number fields of given degree, *Funct. Approx. Comment. Math.*, **56** (2017) 61–65.

[67] J. T. Tate, The arithmetic of elliptic curves, *Invent. Math.*, **23** (1974) 179–206.

[68] J. F. Voloch, A note on elliptic curves over finite fields, *Bull. Soc. Math. France*, **116** (1988) 455–458.

[69] L. C. Washington, *Elliptic curves, number theory and cryptography*, Chapman & Hall / CRC, 2008.

[70] W. C. Waterhouse, Abelian varieties over finite fields, *Ann. Sci. École Norm. Sup. (4)*, **2** (1969) 521–560.

[71] A. Weil, L'arithmétique sur les courbes algébriques, *Acta Arith.*, **52** (1929) 281–315.

[72] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, *Ann. Math.*, **142** (1995) 443–551.

Massimiliano Sala

Department of Mathematics, University of Trento, Trento, Italy

Email: maxsalacodesgmail.com

Daniele Taufer

CISPA, Helmholtz Center for Information Security, Saarbrücken, Germany

Email: daniele.taufer@cispa.de

http://dx.doi.org/10.22108/IJGT.2022.131984.1769