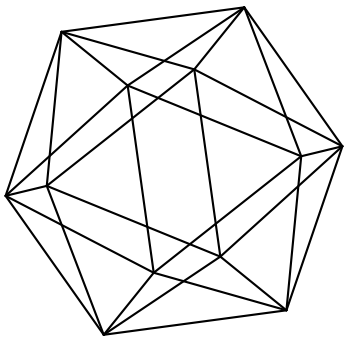
Max-Planck-Institut für Mathematik
Bonn

The divisibility by 2 of rational points on elliptic curves

by

Boris M. Bekker
Yuri G. Zarhin



Max-Planck-Institut für Mathematik
Preprint Series 2016 (32)

The divisibility by 2 of rational points on elliptic curves

Boris M. Bekker
Yuri G. Zarhin

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

St. Petersburg State University
Department of Mathematics and Mechanics
Universitetsky prospekt 28
Peterhof
St. Petersburg 198504
Russia

Pennsylvania State University
Department of Mathematics
University Park, PA 16802
USA

MPIM 16-32

THE DIVISIBILITY BY 2 OF RATIONAL POINTS ON ELLIPTIC CURVES

BORIS M. BEKKER AND YURI G. ZARHIN

Abstract. We give a simple proof of the well-known divisibility by 2 condition for rational points on elliptic curves with rational 2-torsion. As an application of the explicit division by 2^n formulas obtained in Sec.2, we construct versal families of elliptic curves containing points of orders 4, 5, 6, and 8 from which we obtain an explicit description of elliptic curves over certain finite fields $\mathbb{F}_q$ with a prescribed (small) group $E(\mathbb{F}_q)$. In the last two sections we study 3- and 5-torsion.

1. Division by 2

Let K be a field of characteristic different from 2. Let

$$E : y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3) \tag{1}$$

be an elliptic curve over K, where $\alpha_1, \alpha_2, \alpha_3$ are distinct elements of K. This means that $E(K)$ contains all three points of order 2, namely, the points

$$W_1 = (\alpha_1, 0), W_2 = (\alpha_2, 0), W_3 = (\alpha_3, 0). \tag{2}$$

The following statement is pretty well known ([3, pp. 269–270], [7, Ch. 5, pp. 102–104], [4], [5, Th. 4.2 on pp. 85-87], [2, Lemma 7.6 on p. 67] [1, pp. 331–332], [14, pp. 212–214]; see also [15]).

Theorem 1.1. *Let $P = (x_0, y_0)$ be a K-point on E. Then P is divisible by 2 in $E(K)$ if and only if all three elements $x_0 - \alpha_i$ are squares in K.*

This assertion is traditionally used in the course of a proof of the Weak Mordell-Weil Theorem for elliptic curves. While the proof of the claim that the divisibility implies the squareness is straightforward, it seems that the known elementary proofs of the converse statement are more involved/computational. (Notice that there is another approach, which is based on Galois cohomology [10, Sect. X.1, pp. 313–315].)

We start with an elementary proof of the divisibility that seems to be less computational. (In additional, it will give us immediately explicit formulas for the coordinates of all four $\frac{1}{2}P$.)

Proof. So, let us assume that all three elements $x_0 - \alpha_i$ are squares in K, and let $Q = (x_1, y_1)$ be a point on E with $2Q = P$. Since $P \neq \infty$, we have $y_1 \neq 0$, and

The first named author (B.B.) is partially supported by RFFI grant N 14-01-00393.

The second named author (Y.Z.) is partially supported by a grant from the Simons Foundation (#246625 to Yuri Zarkhin). Part of this work was done in May-June 2016 when he was a visitor at the Max-Planck-Institut für Mathematik (Bonn, Germany), whose hospitality and support are gratefully acknowledged.

therefore the equation of the *tangent line* L to E at Q may be written in the form

$$L : y = lx + m.$$

(Here x_1, y_1, l, m are elements of an overfield of K.) In particular, $y_1 = lx_1 + m$. By the definition of Q and L, the point $-P = (x_0, -y_0)$ is the "third" common point of L and E; in particular, $-y_0 = lx_0 + m$, i.e., $y_0 = -(lx_0 + m)$. Standard arguments (the restriction of the equation for E to L, see [11, pp. 25–27], [14, pp. 12–14], [1, p. 331]) tell us that the monic cubic polynomial

$$(x - \alpha_1)(x - \alpha_2)(x - \alpha_3) - (lx + m)^2$$

coincides with $(x - x_1)^2(x - x_0)$. This implies that

$$-(l\alpha_i + m)^2 = (\alpha_i - x_1)^2(\alpha_i - x_0) \text{ for all } i = 1, 2, 3.$$

Since $2Q = P \neq \infty$, none of $x_1 - \alpha_i$ vanishes. Recall that all $x_0 - \alpha_i$ are squares in K and they are obviously distinct. Consequently, the corresponding square roots [1, p. 331]

$$r_i := \frac{l\alpha_i + m}{x_1 - \alpha_i} = \sqrt{x_0 - \alpha_i}$$

are *distinct* elements of K. In other words, the transformation

$$z \mapsto \frac{lz + m}{-z + x_1}$$

of the projective line sends the three distinct K-points $\alpha_1, \alpha_2, \alpha_3$ to the three distinct K-points r_1, r_2, r_3, respectively. This implies that our transformation is *not* constant, i.e., is an honest linear fractional transformation [1] and is defined over K. Since one of the "matrix entries", -1, is already a nonzero element of K, all other matrix entries l, m, x_1 also lie in K. Since $y_1 = lx_1 + m$, it also lies in K. So, $Q = (x_1, y_1)$ is a K-point of E. □

Let us get explicit formulas for x_1, y_1, l, m in terms of r_1, r_2, r_3. We have

$$\alpha_i = x_0 - r_i^2,\ l\alpha_i + m = r_i(x_1 - \alpha_i),$$

and therefore

$$l(x_0 - r_i^2) + m = r_i[x_1 - (x_2 - r_i^2)] = r_i^3 + (x_1 - x_2)r_i,$$

which is equivalent to $r_i^3 + lr_i^2 + (x_1 - x_0)r_i - (lx_0 + m) = 0$, and this equality holds for all $i = 1, 2, 3$. This means that the monic cubic polynomial

$$h(t) = t^3 + lt^2 + (x_1 - x_0)t - (lx_0 + m)$$

coincides with $(t - r_1)(t - r_2)(t - r_3)$. Recall that $-(lx_0 + m) = y_0$ and get

$$r_1 r_2 r_3 = -y_0. \tag{3}$$

We also get

$$l = -(r_1 + r_2 + r_3),\ x_1 - x_0 = r_1 r_2 + r_2 r_3 + r_3 r_1.$$

This implies that

$$x_1 = x_0 + (r_1 r_2 + r_2 r_3 + r_3 r_1). \tag{4}$$

Since $y_1 = lx_1 + m$ and $-y_0 = lx_0 + m$, we obtain that

$$m = -y_0 - lx_0 = -y_0 + (r_1 + r_2 + r_3)x_0,$$

[1] Another way to see this is to assume the contrary. Then the *determinant* $lx_1 + m = 0$, i.e., $y_0 = 0$, and therefore $P = 2Q$ is the infinite point, which is not true.

and therefore

$$y_1 = -(r_1+r_2+r_3)[x_0+(r_1r_2+r_2r_3+r_3r_1)]+[-y_0+(r_1+r_2+r_3)x_0],$$

i.e.,

$$y_1 = -y_0-(r_1+r_2+r_3)(r_1r_2+r_2r_3+r_3r_1). \tag{5}$$

Notice that there are precisely four points $Q \in E(K)$ with $2Q = P$,

$$Q = (x_0+(r_1r_2+r_2r_3+r_3r_1), -y_0-(r_1+r_2+r_3)(r_1r_2+r_2r_3+r_3r_1)), \tag{6}$$

each of which corresponds to one of the *four* choices of the three square roots $r_i = \sqrt{x_0-\alpha_i} \in K$ $(i = 1, 2, 3)$ with $r_1r_2r_3 = -y_0$. Using the latter equality, we may rewrite (5) as [2]

$$y_1 = -(r_1+r_2)(r_2+r_3)(r_3+r_1). \tag{7}$$

In addition,

$$x_1 = \alpha_i+(r_i+r_j)(r_i+r_k), \tag{8}$$

where i, j, k is any permutation of $1, 2, 3$. Indeed,

$$x_1-\alpha_i = (x_0-\alpha_i)+r_1r_2+r_2r_3+r_3r_1 =$$
$$r_i^2+r_1r_2+r_2r_3+r_3r_1 = (r_i+r_j)(r_i+r_k).$$

The remaining four choices of the "signs" of r_1, r_2, r_3 bring us to the same values of abscissas and the opposite values of ordinates and give the results of division by 2 of the point $-P$.

Conversely, if we know $Q = (x_1, y_1)$, then we may recover the corresponding (r_1, r_2, r_3). Namely, the equalities (8) and (7) imply that

$$r_j+r_k = -\frac{y_1}{x_1-\alpha_i},$$
$$r_i = \frac{-(r_j+r_k)+(r_i+r_j)+(r_i+r_k)}{2}$$
$$= -\frac{y_1}{2}\cdot\left(-\frac{1}{x_1-\alpha_i}+\frac{1}{x_1-\alpha_j}+\frac{1}{x_1-\alpha_k}\right)$$

for any permutation i, j, k of $1, 2, 3$.

Example 1.2. Let us choose as $P = (x_0, y_0)$ the point $W_3 = (\alpha_3, 0)$ of order 2 on E. Then $r_3 = 0$, and we have two arbitrary independent choices of (nonzero) $r_1 = \sqrt{\alpha_3-\alpha_1}$ and $r_2 = \sqrt{\alpha_3-\alpha_2}$. Thus

$$Q = (\alpha_3+r_1r_2, -(r_1+r_2)r_1r_2) = (\alpha_3+r_1r_2, -r_1(\alpha_3-\alpha_2)-r_2(\alpha_3-\alpha_1))$$

is a point on E with $2Q = P$; in particular, Q is a point of order 4. The same is true for the (three remaining) points $-Q = (\alpha_3+r_1r_2, r_1(\alpha_3-\alpha_2)+r_2(\alpha_3-\alpha_1))$, $(\alpha_3-r_1r_2, -r_1(\alpha_3-\alpha_2)+r_2(\alpha_3-\alpha_1))$, and $(\alpha_3-r_1r_2, r_1(\alpha_3-\alpha_2)-r_2(\alpha_3-\alpha_1))$.

Recall that, in formula (6) for the coordinates of the points $\frac{1}{2}P$, one may arbitrarily choose the signs of r_1, r_2, r_3 under condition (3). Let Q be one of $\frac{1}{2}P$'s that corresponds to a certain choice of r_1, r_2, r_3. The remaining three *halves* of P correspond to $(r_1, -r_2, -r_3)$, $(-r_1, r_2, -r_3)$, $(-r_1, -r_2, r_3)$. Let us denote these halves by $\mathcal{Q}_1, \mathcal{Q}_2, \mathcal{Q}_3$, respectively. For each $i = 1, 2, 3$, the difference $\mathcal{Q}_i - Q$ is a point of order 2 on E. Which one? The following assertion answers this question.

[2]This was brought to our attention by Robin Chapman.

Theorem 1.3. *Let i, j, k be a permutation of $1, 2, 3$. Then*

(i) *If $P = W_i$, then $\mathcal{Q}_i = -Q$.*
(ii) *If $P \neq W_i$, then all three points $\mathcal{Q}_i, -Q, W_i$ are distinct.*
(iii) *The points $\mathcal{Q}_i, -Q, W_i$ lie on the line*

$$y = (r_j + r_k)(x - \alpha_i).$$

(iv) $\mathcal{Q}_i - Q = W_i$.

Proof. First, assume that $P = W_i$. In this case, formulas (4) and (5) tell us that

$$Q = (\alpha_i + r_j r_k, -r_j r_k (r_j + r_k)),$$

which implies that

$$\mathcal{Q}_i = (\alpha_i + r_j r_k, r_j r_k (r_j + r_k)) = -Q$$

and

$$\mathcal{Q}_i - Q = -2Q = -P = P = W_i.$$

This proves (i) and a special case of (iv) when $P = W_i$. Now assume that $P \neq W_i$ and prove that the three points $\mathcal{Q}_i, -Q, W_i$ are *distinct*. Since none of Q_i and $-Q$ is of order 2, none of them is W_i. On the other hand, if $\mathcal{Q}_i = -Q$, then

$$2Q = P = 2\mathcal{Q}_i = -2Q = -P,$$

and so P has order 2, say $P = W_j$. Applying (a) to j instead of i, we get $\mathcal{Q}_j = -Q$; but $\mathcal{Q}_i \neq \mathcal{Q}_j$ since $i \neq j$. Therefore $\mathcal{Q}_i, -Q, W_i$ are three *distinct* points. This proves (ii).

Let us prove (iii). Since

$$x_1 - \alpha_i = (r_i + r_j)(r_i + r_k),\ y_1 = -(r_1 + r_2)(r_2 + r_3)(r_3 + r_1),$$

we have $y_1 = (r_j + r_k)(x_1 - \alpha_i)$. Further

$$x(-\mathcal{Q}_i) - \alpha_i = (r_i - r_j)(r_i - r_k),$$

$$y(-\mathcal{Q}_i) = (r_i - r_j)(-r_j - r_k)(-r_k + r_i) = (r_j + r_k)\left(x(-\mathcal{Q}_i) - \alpha_i\right).$$

Therefore $\mathcal{Q}_i, -Q, W_i$ lie on the line

$$y = (r_k + r_l)(x - \alpha_i).$$

We have already proven (iv) when $P = W_i$. So, let us assume that $P \neq W_i$. Now (iv) follows from (iii) combined with (i). □

In what follows we discuss a criterion of divisibility by any power of 2 in $E(K)$ (Section 2). In Sections 3,4,5 we will use explicit formulas of Section 1 in order to construct *versal* families of elliptic curves E such that $E(K)$ contains a subgroup isomorphic to $\mathbb{Z}/2m\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ with $m = 2, 4, 3$ respectively. (In addition, in Section 3 we construct a *versal* family of elliptic curves E such that $E(K)$ contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.) Such families are parameterized by K-points of rational curves that are closely related to certain modular curves of genus zero (see [6, 9]); however, our approach remains quite elementary. In addition, in Sections 4 and 6 we construct *versal* families of elliptic curves E such that $E(K)$ contains a subgroup isomorphic to $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ respectively. These two families are parameterized by K-points of curves that are closely related to certain modular curves of genus 1.

As an unexpected application, we describe explicitly (and without computations) elliptic curves E over small finite fields $\mathbb{F}_q$ such that $E(\mathbb{F}_q)$ is isomorphic to a certain finite group (of small order).

Acknowledgements. We are grateful to Robin Chapman for helpful comments.

2. Division by 2^n

Using the formulas above that describe the division by 2 on E, one may easily deduce the following necessary and sufficient condition of divisibility by any power of 2. For an overfield L of K, we consider a sequence of points Q_μ in $E(L)$ such that $Q_0 = P$ and $2Q_{\mu+1} = Q_\mu$ for all $\mu = 0, 1, 2, \dots$. Let $r_1^{(\mu)}, r_2^{(\mu)}, r_3^{(\mu)}$ $(\mu = 0, 1, 2, \dots)$ be arbitrary sequences of elements of L that satisfy the relations

$$(r_i^{(\mu)})^2 = x(Q_\mu) - \alpha_i.$$

Then for each permutation i, j, k of $1, 2, 3$ we obtain, in light of the formula (8),

$$x(Q_{\mu+1}) - \alpha_i = \big(r_i^{(\mu)} + r_j^{(\mu)}\big)\big(r_i^{(\mu)} + r_k^{(\mu)}\big),$$

which implies that

$$(r_i^{(\mu+1)})^2 = (r_i^{(\mu)} + r_j^{(\mu)})(r_i^{(\mu)} + r_k^{(\mu)}).$$

By changing the signs of $r_i^{(\mu)}, r_j^{(\mu)}, r_k^{(\mu)}$ in the product $(r_i^{(\mu)} + r_j^{(\mu)})(r_i^{(\mu)} + r_k^{(\mu)})$, we obtain all possible values of the abscissas of $Q_{(\mu+1)}$ with $2Q_{\mu+1} = Q_\mu$.

Suppose that $Q_\mu \in E(K)$. Then Q_μ is divisible by 2 in $E(K)$ if and only if one may choose $r_i^{(\mu)}, r_j^{(\mu)}, r_k^{(\mu)}$ in such a way that $(r_i^{(\mu)} + r_j^{(\mu)})(r_i^{(\mu)} + r_k^{(\mu)})$ are squares in K for all $i = 1, 2, 3$. We proved the following statement.

Theorem 2.1. *Let $P = (x_0, y_0) \in E(K)$. Let $r_1^{(\mu)}, r_2^{(\mu)}, r_3^{(\mu)}$ $(\mu = 0, 1, 2, \dots)$ be sequences of elements of L that satisfy the relations*

$$(r_i^0)^2 = r_i^2 = x_0 - \alpha_i,\ (r_i^{(\mu+1)})^2 = (r_i^{(\mu)} + r_j^{(\mu)})(r_i^{(\mu)} + r_k^{(\mu)})$$

for all permutations i, j, k of $1, 2, 3$. Then P is divisible by 2^n in $E(K)$ if and only if all $x_0 - \alpha_i$ are squares in K, and for each $\mu = 0, 1, \dots n-1$ one may choose square roots $r_1^{(\mu)}, r_2^{(\mu)}, r_3^{(\mu)}$ in such a way that the products $(r_i^{(\mu)} + r_j^{(\mu)})(r_i^{(\mu)} + r_k^{(\mu)})$ are squares in K (and therefore for all $\mu = 0, 1, \dots n-1$ all $r_i^{(\mu)}$ lie in K).

The knowledge of sequences $r_1^{(\mu)}, r_2^{(\mu)}, r_3^{(\mu)}$ allows us step by step to find the points $\frac{1}{2}P, \frac{1}{4}P, \frac{1}{8}P$ etc.

Example 2.2. Let $P = (x_0, y_0)$, let R be a point of E such that $4R = P$, and let $Q = 2R = (x_1, y_1)$. By formulas (4) and (7),

$$x_1 = x_0 + (r_1r_2 + r_2r_3 + r_3r_1),\ y_1 = -(r_1 + r_2)(r_2 + r_3)(r_3 + r_1),$$

where the square roots

$$r_i = \sqrt{x_0 - \alpha_i},\ i = 1, 2, 3,$$

are chosen in such a way that $r_1r_2r_3 = -y_0$. Further, let

$$r_i^{(1)} = \sqrt{(r_i + r_j)(r_i + r_k)}$$

be square roots that are chosen in such a way that

$$r_1^{(1)}r_2^{(1)}r_3^{(1)} = -y_1 = (r_1 + r_2)(r_2 + r_3)(r_3 + r_1).$$

In light of (4) and (7),

$$x(R) = x_1 + r_1^{(1)} r_2^{(1)} + r_2^{(1)} r_3^{(1)} + r_3^{(1)} r_1^{(1)},$$
$$y(R) = -(r_1^{(1)} + r_2^{(1)})(r_2^{(1)} + r_3^{(1)})(r_3^{(1)} + r_1^{(1)}),$$

which implies that

$$\begin{aligned} x(R) &= x_0 + (r_1 r_2 + r_2 r_3 + r_3 r_1) + (r_1^{(1)} r_2^{(1)} + r_2^{(1)} r_3^{(1)} + r_3^{(1)} r_1^{(1)}), \\ y(R) &= -(r_1^{(1)} + r_2^{(1)})(r_2^{(1)} + r_3^{(1)})(r_3^{(1)} + r_1^{(1)}). \end{aligned} \tag{9}$$

3. Rational points of order 4

In the sequel, we will freely use the following well-known elementary observation.

Let κ be a nonzero element of K. Then there is a canonical isomorphism of the elliptic curves

$$E : y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

and

$$E(\kappa) : y'^2 = \left(x' - \frac{\alpha_1}{\kappa^2}\right)\left(x' - \frac{\alpha_2}{\kappa^2}\right)\left(x' - \frac{\alpha_3}{\kappa^2}\right)$$

that is given by the change of variables

$$x' = \frac{x}{\kappa^2},\ y' = \frac{y}{\kappa^3}$$

and respect the group structure. Under this isomorphism the point $(\alpha_i, 0) \in E(K)$ goes to $(\alpha_i/\kappa^2, 0) \in E(\kappa)(K)$ for all $i = 1, 2, 3$. In addition, if $P = (0, y(P))$ lies in $E(K)$, then it goes (under this isomorphism) to $(0, y(P)/\kappa^3) \in E(\kappa)(K)$.

We will also use the following classical result of Hasse (Hasse bound) [14, Th. 4.2 on p. 97]. *If q is a prime power, $\mathbb{F}_q$ a q-element finite field and E is an elliptic curve over $\mathbb{F}_q$, then $E(\mathbb{F}_q)$ is a finite abelian group, whose cardinality $|E(\mathbb{F}_q)|$ satisfies the inequalities*

$$q - 2\sqrt{q} + 1 \le |E(\mathbb{F}_q)| \le q + 2\sqrt{q} + 1. \tag{10}$$

We are going to describe explicitly elliptic curves (1) that contain a K-point of order 4. In order to do that, we consider the elliptic curve

$$\mathcal{E}_{1,\lambda} : y^2 = (x + \lambda^2)(x + 1)x$$

over K. Here λ is an element of $K \setminus \{0, \pm 1\}$. In this case, we have

$$\alpha_1 = -\lambda^2,\ \alpha_2 = -1,\ \alpha_3 = 0.$$

Notice that

$$\mathcal{E}_{1,\lambda} = \mathcal{E}_{1,-\lambda}.$$

All three differences

$$\alpha_3 - \alpha_1 = \lambda^2,\ \alpha_3 - \alpha_2 = 1^2,\ \alpha_3 - \alpha_3 = 0^2$$

are squares in K. Dividing the order 2 point $W_3 = (0, 0) \in \mathcal{E}_{1,\lambda}(K)$ by 2, we get $r_3 = 0$ and the four choices

$$r_1 = \pm\lambda,\ r_2 = \pm 1.$$

Now Example 1.2 gives us four points Q with $2Q = W_3$, namely,

$$(\lambda, \mp(\lambda + 1)\lambda),\ (-\lambda, \pm(\lambda - 1)\lambda).$$

This implies that the group $\mathcal{E}_{1,\lambda}(K)$ contains the subgroup generated by any Q and W_1, which is $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Remark 3.1. Our computations show that if Q is a K-point on $E_{1,\lambda}$, then

$$2Q = W_3 \text{ if and only if } x(Q) = \pm\lambda.$$

Both cases (signs) do occur.

Remark 3.2. There is another family of elliptic curves ([6, Table 3 on p. 217] (see also [9, Part 2], [8, Appendix E]))

$$y^2 + xy - \left(t^2 - \frac{1}{16}\right) y = x^3 - \left(t^2 - \frac{1}{16}\right) x^2,$$

whose group of rational points contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Theorem 3.3. *Let E be an elliptic curve over K. Then $E(K)$ contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ if and only if there exists $\lambda \in K \setminus \{0, \pm 1\}$ such that E is isomorphic to $\mathcal{E}_{1,\lambda}$.*

Proof. We already know that $\mathcal{E}_{1,\lambda}(K)$ contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Conversely, suppose that E is an elliptic curve over K such that $E(K)$ contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Then $E(K)$ contains all three points of order 2, and therefore E can be represented in the form (1). It is also clear that at least one of the points (2) is divisible by 2 in $E(K)$. Suppose that W_3 is divisible by 2. We may assume that $\alpha_3 = 0$. By Theorem 1.1, both nonzero differences

$$-\alpha_1 = \alpha_3 - \alpha_1, \ -\alpha_2 = \alpha_3 - \alpha_2$$

are squares in K; in addition, they are *distinct* elements of K. Thus there are nonzero $a, b \in K$ such that $a \neq \pm b$ and $-\alpha_1 = a^2, \ -\alpha_2 = b^2$. Since $\alpha_3 = 0$, the equation for E is

$$E : y^2 = (x + a^2)(x + b^2)x.$$

If we put $\kappa = b$, then we obtain that E is isomorphic to

$$E(\kappa) : y'^2 = \left(x' + \frac{a^2}{b^2}\right)(x' + 1)x',$$

which is nothing else but $\mathcal{E}_{1,\lambda}$ with $\lambda = a/b$. □

Corollary 3.4. *Let E be an elliptic curve over $\mathbb{F}_5$. The group $E(\mathbb{F}_5)$ is isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ if and only if E is isomorphic to the elliptic curve $y^2 = x^3 - x$.*

Proof. Suppose that $E(\mathbb{F}_5)$ is isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. By Theorem 3.3, E is isomorphic to

$$y^2 = (x + \lambda^2)(x + 1)x \ \text{ with } \lambda \in \mathbb{F}_5 \setminus \{0, 1, -1\}.$$

This implies that $\lambda = \pm 2, \lambda^2 = -1$, and so E is isomorphic to

$$\mathcal{E}_{1,2} : y^2 = (x - 1)(x + 1) = x^3 - x.$$

Now we need to check that $\mathcal{E}_{1,2}(\mathbb{F}_5) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. By Theorem 3.3, $E(\mathbb{F}_5)$ contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$; in particular, 8 divides $|E(\mathbb{F}_5)|$. In order to finish the proof, it suffices to check that $|E(\mathbb{F}_5)| < 16$, but this inequality follows from the Hasse bound (10)

$$|E(\mathbb{F}_5)| \leq 5 + 2\sqrt{5} + 1 < 11.$$

□

Corollary 3.5. *Let E be an elliptic curve over $\mathbb{F}_7$. The group $E(\mathbb{F}_7)$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ if and only if E is isomorphic to the elliptic curve $y^2 = (x+2)(x+1)x$.*

Proof. Suppose that $E(\mathbb{F}_7)$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$. It follows from Theorem 3.3 that E is isomorphic to $y^2 = (x+\lambda^2)(x+1)x$ with $\lambda \in \mathbb{F}_7 \setminus \{0, 1, -1\}$. This implies that $\lambda = \pm 2$ or ± 3, and therefore $\lambda^2 = 4$ or 2, i.e., E is isomorphic to one of the two elliptic curves

$$\mathcal{E}_{1,3} : y^2 = (x+2)(x+1)x,\ \mathcal{E}_{1,2} : y^2 = (x+4)(x+1)x.$$

Since $1/4 = 2$ in $\mathbb{F}_7$, the elliptic curve $\mathcal{E}_{1,3}$ coincides with $\mathcal{E}_{1,2}(2)$; in particular, $\mathcal{E}_{1,2}$ and $\mathcal{E}_{1,3}$ are isomorphic.

Now suppose that $E = \mathcal{E}_{1,2}$. We need to prove that $E(\mathbb{F}_7)$ is isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. By Theorem 3.3, $E(\mathbb{F}_7)$ contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$; in particular, 8 divides $|E(\mathbb{F}_7)|$. In order to finish the proof, it suffices to check that $|E(\mathbb{F}_7)| < 16$, but this inequality follows from the Hasse bound (10)

$$|E(\mathbb{F}_7)| \le 7 + 2\sqrt{7} + 1 < 14.$$

□

Theorem 3.6. *Suppose that K contains $\mathbf{i} = \sqrt{-1}$. Let a, b be nonzero elements of K such that $a \ne \pm b,\ a \ne \pm\mathbf{i}b$. Let us consider the elliptic curve*

$$E_{a,b} : y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$$

over K with $\alpha_1 = (a^2-b^2)^2,\ \alpha_2 = (a^2+b^2)^2,\ \alpha_3 = 0$. Then all points of order 2 on E are divisible by 2 in $E(K)$, i.e., $E(K)$ contains all twelve points of order 4. In particular, $E_{a,b}(K)$ contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

Proof. Clearly, all α_i and $-\alpha_j$ are squares in K. In addition,

$$\alpha_2 - \alpha_1 = (a^2+b^2)^2 - (a^2-b^2)^2 = (2ab)^2,\ \alpha_1 - \alpha_2 = (2\mathbf{i}ab)^2.$$

This implies that all $\alpha_i - \alpha_j$ are squares in K. It follows from Theorem 1.1 that all points $W_i = (\alpha_i, 0)$ of order 2 are divisible by 2 in $E(K)$, and therefore $E(K)$ contains all twelve (3×4) points of order 4. □

Keeping the notation and assumptions of Theorem 3.6, we describe explicitly all twelve points of order 4, using formula (6).

(1) Dividing the point $W_2 = (\alpha_2, 0) = \big((a^2+b^2)^2, 0\big)$ by 2, we have $r_2 = 0$ and get four choices $r_1 = \pm 2ab,\ r_3 = \pm(a^2+b^2)$. This gives us four points Q with $2Q = W_2$, namely, two points

$$\big((a^2+b^2)^2 + 2ab(a^2+b^2),\ \pm(a^2+b^2+2ab)2ab(a^2+b^2)\big)$$
$$= \big((a^2+b^2)(a+b)^2,\ \pm 2ab(a^2+b^2)(a+b)^2\big)$$

and two points $\big((a^2+b^2)(a-b)^2,\ \pm 2ab(a^2+b^2)(a-b)^2\big)$.

(2) Dividing the point $W_3 = (\alpha_3, 0) = (0, 0)$ by 2, we have $r_3 = 0$ and get four choices $r_1 = \pm\mathbf{i}(a^2-b^2),\ r_2 = \pm\mathbf{i}(a^2+b^2)$. This gives us four points Q with $2Q = W_3$, namely, two points

$$\big((a^2-b^2)(a^2+b^2),\ \pm(\mathbf{i}((a^2-b^2)+\mathbf{i}(a^2+b^2))(a^2-b^2)(a^2+b^2)\big)$$
$$= \big(a^4-b^4,\ \pm 2\mathbf{i}a^2(a^4-b^4)\big)$$

and two points $\big(b^4-a^4,\ \pm 2\mathbf{i}b^2(b^4-a^4)\big)$.

(3) Dividing the point $W_1 = (\alpha_1, 0) = \big((a^2 - b^2)^2, 0\big)$ by 2, we have $r_1 = 0$ and get four choices $r_2 = \pm 2\mathbf{i}ab,\ r_3 = \pm(a^2 - b^2)$. This gives us four points Q with $2Q = W_3$, namely, two points

$$\big((a^2 - b^2)^2 + 2\mathbf{i}ac(a^2 - b^2),\ \pm(2\mathbf{i}ab + (a^2 - b^2))2\mathbf{i}ab(a^2 - b^2)\big)$$

$$= \big((a^2 - b^2)(a + \mathbf{i}b)^2,\ \pm 2\mathbf{i}ab(a^2 - b^2)(a + \mathbf{i}b)^2\big)$$

and two points $\big((a^2 - b^2)(a - \mathbf{i}b)^2,\ \pm 2\mathbf{i}ab(a^2 - b^2)(a - \mathbf{i}b)^2\big)$.

Remark 3.7. Let λ be an element of $K \setminus \{0, \pm 1, \pm\sqrt{-1}\}$. We write $\mathcal{E}_{2,\lambda}$ for the elliptic curve

$$\mathcal{E}_{2,\lambda} : y^2 = \left(x + \frac{(\lambda^2 - 1)^2}{(\lambda^2 + 1)^2}\right)(x + 1)x$$

over K. The elliptic curves $\mathcal{E}_{2,\lambda}$ and $E_{a,b}$ are isomorphic if $a = \lambda b$. Indeed, one has only to put $\kappa = a^2 + b^2$ and notice that $E_{a,b}(\kappa) = \mathcal{E}_{2,\lambda}$. It follows from Theorem 3.6 that $\mathcal{E}_{2,\lambda}(K)$ contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

There is another family of elliptic curves with this property, namely,

$$y^2 = x(x - 1)\left(x - \frac{(u + u^{-1})^2}{4}\right)$$

([12], [9, pp. 451–453]; see also Remark 3.9).

Theorem 3.8. *Let E be an elliptic curve over K. Then $E(K)$ contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ if and only if K contains $\sqrt{-1}$ and there exists $\lambda \in K \setminus \{0, \pm 1, \pm\sqrt{-1}\}$ such that E is isomorphic to $\mathcal{E}_{2,\lambda}$.*

Proof. Recall (Remark 3.7) that $\mathcal{E}_{2,\lambda}(K)$ contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

Conversely, suppose that E is an elliptic curve over K and $E(K)$ contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. By Theorem 3.3, there is $\delta \in K \setminus \{0, \pm 1\}$ such that E is isomorphic to

$$\mathcal{E}_{1,\delta} : y^2 = (x + \delta^2)(x + 1)x.$$

Hence we may assume that $\alpha_1 = -\delta^2, \alpha_2 = -1, \alpha_3 = 0$. It follows from Theorem 1.1 that all $\pm 1, \pm(\delta^2 - 1)$ are squares in K. (In particular, $\mathbf{i} = \sqrt{-1}$ lies in K.) So, there is $\gamma \in K$ with $\gamma^2 = 1 - \delta^2$. Clearly, $\gamma \neq 0, \pm 1$. We have

$$\delta^2 + \gamma^2 = 1.$$

The well-known parametrization of the "unit circle" (that goes back to Euler) tells us that there exists $\lambda \in K$ such that $\lambda^2 + 1 \neq 0$ and

$$\delta = \frac{\lambda^2 - 1}{\lambda^2 + 1},\ \gamma = \frac{2\lambda}{\lambda^2 + 1}.$$

Now one has only to plug in the formula for δ into the equation of $\mathcal{E}_{1,\delta}$ and get $\mathcal{E}_{2,\lambda}$. □

Remark 3.9. Using a different parametrization of the unit circle in the proof of Theorem 3.8, we obtain the family of elliptic curves

$$E : y^2 = \left(x + \frac{(2\lambda)^2}{(\lambda^2 + 1)^2}\right)(x + 1)x$$

with the same property as family $\mathcal{E}_{2,\lambda}$. Notice that, for each $\lambda \in K \setminus \{0, \pm 1\}$, the elliptic curve E is isomorphic to the elliptic curve

$$y^2 = x(x-1)\left(x - (u+u^{-1})^2/4\right)$$

mentioned in Remark 3.7. Indeed, the latter differs from $E(\kappa)$, where $\kappa = 2\lambda\sqrt{-1}/(\lambda^2+1)$, only in the change of the parameter λ by u.

Corollary 3.10. *Let E be an elliptic curve over $\mathbb{F}_q$, where $q = 9, 13, 17$. The group $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$ if and only if E is isomorphic to one of elliptic curves $\mathcal{E}_{2,\lambda}$. If $q = 9$, then $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ if and only if E is isomorphic to $y^2 = x^3 - x$.*

Proof. First, $\mathbb{F}_q$ contains $\sqrt{-1}$. Suppose that $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$. It follows from Theorem 3.8 that E is isomorphic to $\mathcal{E}_{2,\lambda}$.

Conversely, suppose that E is isomorphic to one of these curves. We need to prove that $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. By Theorem 3.8, $E(\mathbb{F}_q)$ contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$; in particular, 16 divides $|E(\mathbb{F}_q)|$. In order to finish the proof, it suffices to check that $|E(\mathbb{F}_q)| < 32$, but this inequality follows from the Hasse bound (10)

$$|E(\mathbb{F}_q)| \le q + 2\sqrt{q} + 1 \le 17 + 2\sqrt{17} + 1 < 27.$$

Now assume that $q = 9$. Then $\lambda \in \{\pm(1 \pm \mathbf{i}\}$. For all such λ

$$\lambda^2 = \pm 2\mathbf{i} = \mp\mathbf{i}, \ \frac{(\lambda^2-1)^2}{(\lambda^2+1)^2} = \frac{(1\mp\mathbf{i})^2}{(-1\mp\mathbf{i})^2} = \frac{\mp 2\mathbf{i}}{\pm 2\mathbf{i}} = -1.$$

Therefore the equation for $\mathcal{E}_{2,\lambda}$ is

$$y^2 = (x-1)(x+1)x = x^3 - x.$$

□

Corollary 3.11. *Let E be an elliptic curve over $\mathbb{F}_{29}$. The group $E(\mathbb{F}_{29})$ is isomorphic to $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ if and only if E is isomorphic to one of elliptic curves $\mathcal{E}_{2,\lambda}$.*

Proof. First, $\mathbb{F}_{29}$ contains $\sqrt{-1}$. Suppose that $E(\mathbb{F}_{29})$ is isomorphic to $\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$. Then $E(\mathbb{F}_{29})$ contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. It follows from Theorem 3.8 that E is isomorphic to $\mathcal{E}_{2,\lambda}$.

Conversely, suppose that E is isomorphic to one of these curves. We need to prove that $E(\mathbb{F}_{29})$ is isomorphic to $\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$. By Theorem 3.8, $E(\mathbb{F}_{29})$ contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$; in particular, 16 divides $|E(\mathbb{F}_{29})|$. The Hasse bound (10) tells us that

$$29 + 1 - 2\sqrt{29} \le |E(\mathbb{F}_q)| \le 29 + 1 + 2\sqrt{29}$$

and therefore

$$11 < |E(\mathbb{F}_{29})| < 41.$$

It follows that $|E(\mathbb{F}_{29})| = 32$; in particular, $E(\mathbb{F}_{29})$ is a finite 2-group. Clearly, $E(\mathbb{F}_{29})$ is isomorphic to a product of two cyclic 2-groups, each of which has order divisible by 4. It follows that $E(\mathbb{F}_{29})$ is isomorphic to $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. □

4. Points of order 8

Let us return to the curve $\mathcal{E}_{1,\lambda}$ and consider $Q \in \mathcal{E}_{1,\lambda}(K)$ with $2Q = W_3$. Let us try to divide Q by 2 in $E(K)$. By Remark 3.1, $x(Q) = \pm\lambda$. First, we assume that $x(Q) = \lambda$ (such a Q does exist).

Lemma 4.1. *Let Q be a point of $\mathcal{E}_{1,\lambda}(K)$ with $x(Q) = \lambda$. Then Q is divisible by 2 in $\mathcal{E}_{1,\lambda}(K)$ if and only if there exists $c \in K \setminus \{0, \pm 1, \pm 1 \pm \sqrt{2}, \pm\sqrt{-1}\}$ such that*

$$\lambda = \left[\frac{c - \frac{1}{c}}{2}\right]^2.$$

Proof. We have

$$\lambda - \alpha_1 = \lambda - (-\lambda^2) = \lambda + \lambda^2,\ \lambda - \alpha_2 = \lambda - (-1) = \lambda + 1,\ \lambda - \alpha_3 = \lambda - 0 = \lambda.$$

By Theorem 1.1, $Q \in 2\mathcal{E}_{1,\lambda}(K)$ if and only if all three $\lambda + \lambda^2, \lambda + 1, \lambda$ are squares in K. The latter means that both λ and $\lambda + 1$ are squares in K, i.e., there exist $a, b \in K$ such that $a^2 = \lambda + 1, \lambda = b^2$. This implies that the pair (a, b) is a K-point on the hyperbola

$$u^2 - v^2 = 1.$$

Recall that $\lambda \neq 0, \pm 1$. Using the well-known parametrization

$$u = \frac{t + \frac{1}{t}}{2}, v = \frac{t - \frac{1}{t}}{2}$$

of the hyperbola, we obtain that both λ and $\lambda + 1$ are squares in K if and only if there exists a *nonzero* $c \in K$ such that

$$\lambda = \left[\frac{c - \frac{1}{c}}{2}\right]^2.$$

If this is the case, then

$$a = \pm\frac{c + \frac{1}{c}}{2},\ b = \pm\frac{c - \frac{1}{c}}{2}$$

and

$$\lambda + 1 = \left[\frac{c + \frac{1}{c}}{2}\right]^2.$$

Recall that $\lambda \neq 0, \pm 1$. This means that

$$\frac{c - \frac{1}{c}}{2} \neq 0, \pm 1, \pm\sqrt{-1}, \quad \text{i.e.,}$$

$$c \neq 0, \pm 1, \pm 1 \pm \sqrt{2}, \pm\sqrt{-1}.$$

□

Now let us assume that $x(Q) = -\lambda$ (such a Q does exist).

Lemma 4.2. *Let Q be a point of $\mathcal{E}_{1,\lambda}(K)$ with $x(Q) = -\lambda$. Then Q is divisible by 2 in $\mathcal{E}_{1,\lambda}(K)$ if and only if there exists $c \in K \setminus \{0, \pm 1, \pm 1 \pm \sqrt{2}, \pm\sqrt{-1}\}$ such that*

$$\lambda = -\left[\frac{c - \frac{1}{c}}{2}\right]^2.$$

Proof. Applying Lemma 4.1 to $-\lambda$ (instead of λ) and the curve $\mathcal{E}_{1,-\lambda} = \mathcal{E}_{1,\lambda}$, we obtain that $Q \in 2\mathcal{E}_{1,-\lambda}(K) = 2\mathcal{E}_{1,\lambda}(K)$ if and only if there exists

$$c \in K \setminus \{0, \pm 1, \pm 1 \pm \sqrt{2}, \pm\sqrt{-1}\}$$

such that

$$-\lambda = \left[\frac{c - \frac{1}{c}}{2}\right]^2.$$

□

Lemmas 4.1 and 4.2 give us the following statement.

Proposition 4.3. *The point $W_3 = (0,0)$ is divisible by 4 in $\mathcal{E}_{1,\lambda}(K)$ if and only if there exists $c \in K$ such that $c \ne 0, \pm, \pm 1 \pm \sqrt{2}, \pm\sqrt{-1}$ and*

$$\lambda = \pm \left[\frac{c - \frac{1}{c}}{2}\right]^2, \quad \textit{i.e.,} \quad \lambda^2 = \left[\frac{c - \frac{1}{c}}{2}\right]^4.$$

Proposition 4.4. *The following conditions are equivalent.*

(i) *If $Q \in \mathcal{E}_{1,\lambda}(K)$ is any point with $2Q = W_3$, then it lies in $2\mathcal{E}_{1,\lambda}(K)$.*
(ii) *If R is any point of $\mathcal{E}_{1,\lambda}$ with $4R = W_3$, then R lies in $\mathcal{E}_{1,\lambda}(K)$.*
(iii) *There exist $c, d \in K \setminus \{0, \pm 1, \pm 1 \pm \sqrt{2}, \pm\sqrt{-1}\}$ such that*

$$\lambda = \left[\frac{c - \frac{1}{c}}{2}\right]^2, \ -\lambda = \left[\frac{d - \frac{1}{d}}{2}\right]^2.$$

If these equivalent conditions hold, then K contains $\sqrt{-1}$ and $\mathcal{E}_{1,\lambda}(K)$ contains all (twelve) points of order 4.

Proof. The equivalence of (i) and (ii) is obvious. It is also clear that (ii) implies that all points of order (dividing) 4 lie in $\mathcal{E}_{1,\lambda}(K)$.

Recall (Remark 3.1) that Q with $2Q = W_3$ are exactly the points of $\mathcal{E}_{1,\lambda}$ with $x(Q) = \pm\lambda$. Now the equivalence of (ii) and (iii) follows from Lemmas 4.1 and 4.2.

In order to finish the proof, notice that $\lambda \ne 0$ and

$$-1 = \frac{-\lambda}{\lambda} = \left[\frac{\left[\frac{d - \frac{1}{d}}{2}\right]}{\left[\frac{c - \frac{1}{c}}{2}\right]}\right]^2.$$

□

Suppose that

$$\lambda = \left[\frac{c - \frac{1}{c}}{2}\right]^2 \quad \text{with } c \in K \setminus \{0, \pm 1, \pm 1 \pm \sqrt{2}, \pm\sqrt{-1}\}$$

and consider $Q = (\lambda, (\lambda+1)\lambda) \in \mathcal{E}_{1,\lambda}(K)$ of order 4 with $2Q = W_3$. Let us find a point $R \in \mathcal{E}_{1,\lambda}(K)$ of order 8 with $2R = Q$. First, notice that

$$Q = (\lambda, (\lambda+1)\lambda) = \left(\left[\frac{c - \frac{1}{c}}{2}\right]^2, \left[\frac{c + \frac{1}{c}}{2}\right]^2 \cdot \left[\frac{c - \frac{1}{c}}{2}\right]^2\right)$$

$$= \left(\frac{(c^2-1)^2}{4c^2}, \frac{(c^4-1)^2}{4c^4}\right).$$

We have

$$r_1 = \sqrt{\lambda + \lambda^2} = \sqrt{(\lambda+1)\lambda},\ r_2 = \sqrt{\lambda+1},\ r_3 = \sqrt{\lambda};\ r_1 r_2 r_3 = -(\lambda+1)\lambda.$$

This means that

$$r_1 = \pm\frac{c-\frac{1}{c}}{2}\cdot\frac{c+\frac{1}{c}}{2},\ r_2 = \pm\frac{c+\frac{1}{c}}{2},\ r_3 = \pm\frac{c-\frac{1}{c}}{2},$$

and the signs should be chosen in such a way that the product $r_1 r_2 r_3$ coincides with

$$-\left[\frac{c-\frac{1}{c}}{2}\right]^2\cdot\left[\frac{c+\frac{1}{c}}{2}\right]^2.$$

For example, we may take

$$r_1 = -\frac{c-\frac{1}{c}}{2}\cdot\frac{c+\frac{1}{c}}{2} = -\frac{c^2-\frac{1}{c^2}}{4} = -\frac{c^4-1}{4c^2},\ r_2 = \frac{c+\frac{1}{c}}{2},\ r_3 = \frac{c-\frac{1}{c}}{2}$$

and get (since $r_2 + r_3 = c$ and $r_2 r_3 = (c^4-1)/4c^2$))

$$r_1 + r_2 + r_3 = -\frac{c^4-1}{4c^2} + c = \frac{-c^4+4c^3+1}{4c^2},$$

$$r_1 r_2 + r_2 r_3 + r_3 r_1 = c r_1 + r_2 r_3 = -\frac{c(c^4-1)}{4c^2} + \frac{c^4-1}{4c^2} = \frac{(1-c)(c^4-1)}{4c^2}.$$

Now (4) and (7) tell us that the coordinates of the corresponding R with $2R = Q$ are as follows:

$$x(R) = x(Q) + r_1 r_2 + r_2 r_3 + r_3 r_1 = \frac{(c^2-1)^2}{4c^2} + \frac{(1-c)(c^4-1)}{4c^2} = \frac{(1-c)^3(c+1)}{4c},$$

$$y(R) = -(r_1+r_2)(r_2+r_3)(r_1+r_3) =$$

$$-\left(-\frac{c-\frac{1}{c}}{2}\cdot\frac{c+\frac{1}{c}}{2} + \frac{c+\frac{1}{c}}{2}\right)c\left(-\frac{c-\frac{1}{c}}{2}\cdot\frac{c+\frac{1}{c}}{2} + \frac{c-\frac{1}{c}}{2}\right) =$$

$$-\left(1 - \frac{c-\frac{1}{c}}{2}\right)\cdot\frac{c+\frac{1}{c}}{2}\cdot c\cdot\left(1-\frac{c+\frac{1}{c}}{2}\right)\frac{c-\frac{1}{c}}{2} =$$

$$-\frac{c^2-\frac{1}{c^2}}{16}\cdot\left(c-2-\frac{1}{c}\right)\left(c-2+\frac{1}{c}\right)c = -\frac{\left(c^2-\frac{1}{c^2}\right)\left((c-2)^2-\frac{1}{c^2}\right)c}{16}.$$

So, we get the K-point of order 8

$$R = \left(\frac{(1-c)^3(c+1)}{4c}, -\frac{\left(c^2-\frac{1}{c^2}\right)\left((c-2)^2-\frac{1}{c^2}\right)c}{16}\right)$$

on the elliptic curve

$$\mathcal{E}_{4,c} := \mathcal{E}_{1,\left(\pm\frac{c-\frac{1}{c}}{2}\right)^2} : y^2 = \left[x + \left(\frac{c-\frac{1}{c}}{2}\right)^4\right](x+1)x$$

for any $c \in K \setminus \{0, \pm 1, \pm 1 \pm \sqrt{2}, \pm\sqrt{-1}\}$. The group $\mathcal{E}_{4,c}(K)$ contains the subgroup generated by R and W_1, which is isomorphic to $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Remark 4.5. See ([6, Table 3 on p. 217], [8, Appendix E])) for another family of elliptic curves,

$$y^2 + (1 - a(t))xy - b(t)y = x^3 - b(t)x^2$$

with

$$a(t) = \frac{(2t+1)(8t^2+4t+1)}{2(4t+1)(8t^2-1)t},\ b(t) = \frac{(2t+1)(8t^2+4t+1)}{(8t^2-1)^2},$$

whose group of rational points contains a subgroup isomorphic to $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Theorem 4.6. *Let E be an elliptic curve over K. Then $E(K)$ contains a subgroup isomorphic to $\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ if and only if there exists $c \in K\setminus\{0, \pm 1, \pm 1 \pm \sqrt{2}, \pm\sqrt{-1}\}$ such that E is isomorphic to $\mathcal{E}_{4,c}$.*

Proof. We know that $\mathcal{E}_{4,c}(K)$ contains a subgroup isomorphic to $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Conversely, suppose that $E(K)$ contains a subgroup isomorphic to $\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$. This implies that $E(K)$ contains all three points of order 2, i.e., E may be represented in the form (1). Clearly, one of the points (2) is divisible by 4 in $E(K)$. We may assume that W_3 is divisible by 4. We may also assume that $\alpha_3 = 0$, i.e., $W_3 = (0, 0)$. Then we know that there exist distinct nonzero $a, b \in K$ such that $\alpha_1 = -a^2, \alpha_2 = -b^2$, i.e., the equation of E is

$$y^2 = (x + a^2)(x + b^2)x$$

Replacing E by $E(b)$ and putting $\lambda = a/b$, we may assume that

$$E = \mathcal{E}_{1,\lambda} : y^2 = (x + \lambda^2)(x + 1)x.$$

Since W_3 is divisible by 4 in $\mathcal{E}_{1,\lambda}(K)$, the desired result follows from Proposition 4.3. □

Remark 4.7. Suppose that $K = \mathbb{F}_q$ with $q = 3, 5, 7$ or 9. Then

$$\mathbb{F}_q \setminus \{0, 1, -1, \pm 1 \pm \sqrt{2}, \pm\sqrt{-1}\} = \emptyset.$$

Corollary 4.8. *Let E be an elliptic curve over $\mathbb{F}_q$, where $q = 11, 13, 17, 19$. The group $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ if and only if E is isomorphic to one of elliptic curves $\mathcal{E}_{4,c}$.*

Proof. Suppose that $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$. It follows from Theorem 4.6 that E is isomorphic to one of elliptic curves

$$\mathcal{E}_{4,c} : y^2 = \left[x + \left(\frac{c - \frac{1}{c}}{2}\right)^4\right](x + 1)x$$

with $c \in K \setminus \{0, \pm 1, \pm\sqrt{-1}, \pm\sqrt{-1}\}$. Conversely, suppose that E is isomorphic to of these curves. We need to prove that $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. By Theorem 4.6, $E(\mathbb{F}_q)$ contains a subgroup isomorphic to $\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$; in particular, 16 divides $|E(\mathbb{F}_q)|$. In order to finish the proof, it suffices to check that $|E(\mathbb{F}_q)| < 32$, but this inequality follows from the Hasse bound (10)

$$|E(\mathbb{F}_q)| \le q + 2\sqrt{q} + 1 \le 19 + 2\sqrt{19} + 1 < 29.$$

□

Corollary 4.9. *Let E be an elliptic curve over $\mathbb{F}_{47}$. The group $E(\mathbb{F}_{47})$ is isomorphic to $\mathbb{Z}/24\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ if and only if E is isomorphic to one of elliptic curves $\mathcal{E}_{4,c}$.*

Proof. Suppose that $E(\mathbb{F}_{47})$ is isomorphic to $\mathbb{Z}/24\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Then it contains a subgroup isomorphic to $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. It follows from Theorem 4.6 that E is isomorphic to one of elliptic curves

$$\mathcal{E}_{4,c} : y^2 = \left[x + \left(\frac{c - \frac{1}{c}}{2}\right)^4\right](x+1)x$$

with $c \in K \setminus \{0, \pm 1, \pm 1 \pm \sqrt{2}, \pm\sqrt{-1}\}$.

Conversely, suppose that E is isomorphic to one of these curves. We need to prove that $E(\mathbb{F}_{47})$ is isomorphic to $\mathbb{Z}/24\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. By Theorem 4.6, $E(\mathbb{F}_{47})$ contains a subgroup isomorphic to $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$; in particular, 16 divides $|E(\mathbb{F}_{47})|$. The Hasse bound tells us that

$$47 + 1 - 2\sqrt{47} \le |E(\mathbb{F}_{47})| \le 47 + 1 + 2\sqrt{47}$$

and therefore $34 < |E(\mathbb{F}_{47})| < 62$. This implies that $|E(\mathbb{F}_{47})| = 48$; in particular, $E(\mathbb{F}_{47})$ contains a point of order 3. This implies that $E(\mathbb{F}_{47})$ contains a subgroup isomorphic to

$$(\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/24\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Since this subgroup has the same order 48 as the whole group $E(\mathbb{F}_{47})$, we get the desired result. □

Theorem 4.10. *Let E be an elliptic curve over K. Then $E(K)$ contains a subgroup isomorphic to $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ if and only if K contains $\mathbf{i} = \sqrt{-1}$ and there exist*

$$c, d \in K \setminus \{0, \pm 1, \pm 1 \pm \sqrt{2}, \pm\sqrt{-1}\} \quad \text{such that} \quad c - \frac{1}{c} = \mathbf{i}\left(d - \frac{1}{d}\right)$$

and E is isomorphic to $\mathcal{E}_{4,c}$.

Remark 4.11. The above equation defines an open dense set in the plane affine curve

$$\mathcal{M}_{8,4} : (c^2 - 1)d = \mathbf{i}(d^2 - 1)c. \tag{11}$$

It is immediate that the corresponding projective closure is a nonsingular cubic $\bar{\mathcal{M}}_{8,4}$ with a K-point, i.e., an elliptic curve. To obtain a Weierstrass normal form of $\bar{\mathcal{M}}_{8,4}$, we first slightly simplify equation(11) by the change of variables $d = s, \mathbf{i}c = t$ and get $s^2t + ts^2 + s - t = 0$. Then, using the birational transformation

$$s = \frac{\eta}{\xi + \xi^2}, \ t = \frac{\eta}{1 + \xi},$$

we obtain $\eta^2 = \xi^3 - \xi$.

Proof of Theorem 4.10. We have already seen that $\mathcal{E}_{4,c}(K)$ contains an order 8 point R with $4R = W_3$. It follows from Proposition 4.4 that $\mathcal{E}_{4,c}(K)$ contains all points of order 4. In particular, it contains an order 4 point $\mathcal{Q}$ with $2\mathcal{Q} = W_1$. Clearly, R and $\mathcal{Q}$ generate a subgroup isomorphic to $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

Conversely, suppose that $E(K)$ contains a subgroup isomorphic to $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. This implies that $E(K)$ contains all twelve points of order 4. In particular, E may be represented in the form (1). Clearly, one of the points of order 2 is divisible by 4 in $E(K)$. We may assume that W_3 is divisible by 4. The same arguments as in the proof of Theorem 4.6 allow us to assume that

$$E = \mathcal{E}_{1,\lambda} : y^2 = (x + \lambda^2)(x+1)x.$$

Since W_3 is divisible by 4 in $\mathcal{E}_{1,\lambda}(K)$ and all points of order dividing 4 lie in $\mathcal{E}_{1,\lambda}(K)$, every point R of $\mathcal{E}_{1,\lambda}$ with $4R = W_3$ also lies in $\mathcal{E}_{1,\lambda}(K)$. It follows from Proposition 4.3 that K contains $\mathbf{i} = \sqrt{-1}$ and there exist

$$c, d \in K \setminus \{0, 1, -1, \pm 1 \pm \sqrt{2}, \pm\sqrt{-1}\}$$

such that

$$\lambda = \left[\frac{c - \frac{1}{c}}{2}\right]^2, \ -\lambda = \left[\frac{d - \frac{1}{d}}{2}\right]^2.$$

This implies that

$$c - \frac{1}{c} = \pm\mathbf{i}\left(d - \frac{1}{d}\right).$$

Replacing if necessary d by $-d$, we obtain the desired

$$c - \frac{1}{c} = \mathbf{i}\left(d - \frac{1}{d}\right).$$

□

5. Points of order 3

The following assertion gives a simple description of points of order 3 on elliptic curves.

Proposition 5.1. *A point $P = (x_0, y_0) \in E(K)$ has order 3 if and only if one can choose three square roots $r_i = \sqrt{x_0 - \alpha_i}$ in such a way that*

$$r_1 r_2 + r_2 r_3 + r_3 r_1 = 0.$$

Proof. Indeed, let P be a point of order 3. Then $2(-P) = P$. Hence, all $x_0 - \alpha_i$ are squares in K. By (4),

$$x(-P) = x_0 + (r_1 r_2 + r_2 r_3 + r_3 r_1)$$

for a suitable choice of r_1, r_2, r_3. Since $x(-P) = x(P) = x_0$, we get $r_1 r_2 + r_2 r_3 + r_3 r_1 = 0$.

Conversely, suppose that there exists a triple of square roots $r_i = \sqrt{x_0 - \alpha_i}$ such that $r_1 r_2 + r_2 r_3 + r_3 r_1 = 0$. Since $P \in E(K)$,

$$(r_1 r_2 r_3)^2 = (x_0 - \alpha_1)(x_0 - \alpha_2)(x_0 - \alpha_3) = y_0^2,$$

i.e., $r_1 r_2 r_3 = \pm y_0$. Replacing r_1, r_2, r_3 by $-r_1, -r_2, -r_3$ if necessary, we may assume that $r_1 r_2 r_3 = -y_0$. Then there exists a point $Q = (x(Q), y(Q)) \in E(K)$ such that $2Q = P$, and $x_1 = x(Q), y_1 = y(Q)$ are expressed in terms of r_1, r_2, r_3 as in (6). Therefore

$$x(Q) = x_0 + (r_1 r_2 + r_2 r_3 + r_3 r_1) = x_0,$$

$$y(Q) = -y_0 - (r_1 + r_2 + r_3)(r_1 r_2 + r_2 r_3 + r_3 r_1) = -y_0,$$

i.e., $Q = -P, 2(-P) = P$, and so P has order 3. □

Theorem 5.2. *Let a_1, a_2, a_3 be elements of K such that all a_1^2, a_2^2, a_3^2 are distinct. Let us consider the elliptic curve*

$$E = E_{a_1,a_2,a_3} : y^2 = (x + a_1^2)(x + a_2^2)(x + a_3^2)$$

over K. Let $P = (0, a_1 a_2 a_3)$. Then P enjoys the following properties.

(i) *P is divisible by 2 in $E(K)$. More precisely, there are four points $Q \in E(K)$ with $2Q = P$, namely,*

$$(a_2a_3 - a_1a_2 - a_3a_1, (a_1 - a_2)(a_2 + a_3)(a_3 - a_1)),$$
$$(a_3a_1 - a_1a_2 - a_2a_3, (a_1 - a_2)(a_2 - a_3)(a_3 + a_1)),$$
$$(a_1a_2 - a_2a_3 - a_3a_1, (a_1 + a_2)(a_2 - a_3)(a_3 - a_1),$$
$$(a_1a_2 + a_2a_3 + a_3a_1, (a_1 + a_2)(a_2 + a_3)(a_3 + a_1)).$$

(ii) *The following conditions are equivalent.*
   (1) *P has order 3.*
   (2) *None of a_i vanishes, i.e., $\pm a_1, \pm a_2, \pm a_3$ are six distinct elements of K, and one of the following four equalities holds:*

$$a_2a_3 = a_1a_2 + a_3a_1,\ a_3a_1 = a_1a_2 + a_2a_3,$$
$$a_1a_2 = a_2a_3 + a_3a_1,\ a_1a_2 + a_2a_3 + a_3a_1 = 0.$$

(iii) *Suppose that equivalent conditions $(i)-(ii)$ hold. Then one of four points Q coincides with $-Q$ and has order 3, while the three other points are of order 6. In addition, $E(K)$ contains a subgroup isomorphic to $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.*

Remark 5.3. Clearly, $E_{a_1,a_2,a_3} = E_{\pm a_1,\pm a_2,\pm a_3}$.

Proof of Theorem 5.2. We have

$$\alpha_1 = -a_1^2,\ \alpha_2 = -a_2^2,\ \alpha_3 = -a_3^2.$$

Let us try to divide P by 2 in $E(K)$. We have

$$r_1 = \pm a_1,\ r_2 = \pm a_2,\ r_3 = \pm a_3.$$

Since all r_i lie in K, the point $P = (0, a_1a_2a_3)$ is divisible by 2 in $E(K)$. Let Q be a point on E with $2Q = P$. By (4) and (7),

$$x(Q) = r_1r_2 + r_2r_3 + r_3r_1,\ y(Q) = -(r_1 + r_2)(r_2 + r_3)(r_3 + r_1)$$

with $r_1r_2r_3 = -a_1a_2a_3$. Plugging in $r_i = \pm a_i$ into the formulas for $x(Q)$ and $y(Q)$, we get explicit formulas for points Q as in the statement of the theorem. This proves (i).

Let us prove (ii). Suppose that P has order 3. Since P is not of order 2, we have $0 = x(P) \neq \alpha_i$ for all $i = 1, 2, 3$. Since

$$\{\alpha_1, \alpha_2, \alpha_3\} = \{-a_1^2, -a_2^2, -a_3^2\},$$

none of a_i vanishes. It follows from Proposition 5.1 that one may choose the signs for r_i in such a way that $r_1r_2 + r_2r_3 + r_3r_1 = 0$. Plugging in $r_i = \pm a_i$ into this formula, we get four relations between a_1, a_2, a_3 as in (ii)(2).

Now suppose that one of the relations as in (ii)(2) holds. This means that one may choose the signs of $r_i = \pm a_i$ in such a way that $r_1r_2 + r_2r_3 + r_3r_1 = 0$. It follows from Proposition 5.1 that P has order 3. This proves (ii).

Let us prove (iii). Since P has order 3, $2(-P) = P$, i.e., $-P$ is one of the four Q's. Suppose that Q is a point of E with $2Q = P,\ Q \neq -P$. Clearly, the order of Q is either 3 or 6. Assume that Q has order 3. Then $P = 2Q = -Q$ and therefore $Q = -P$, which is not the case. Hence Q has order 6. Then $3Q$ has order 2, i.e., coincides with $W_i = (-a_i^2, 0)$ for some $i \in \{1, 2, 3\}$. Pick $j \in \{1, 2, 3\} \setminus \{i\}$ and consider the point $W_j = (-a_j^2, 0) \neq W_i$. Then the subgroup of $E(K)$ generated by Q and W_j is isomorphic to $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. This proves (iii). □

Remark 5.4. In Theorem 5.2 we do *not* assume that $\mathrm{char}(K) \neq 3$!

Corollary 5.5. *Let a_1, a_2, a_3 be elements of K such that a_1^2, a_2^2, a_3^2 are distinct. Then the following conditions are equivalent.*

(i) *The point $P = (0, a_1a_2a_3) \in E_{a_1,a_2,a_3}(K)$ has order 3.*

(ii) *None of a_i vanishes, and one may choose signs for*

$$a = \pm a_1,\ b = \pm a_2,\ c = \pm a_3$$

in such a way that $c = ab/(a+b)$.

If these conditions hold, then

$$E_{a_1,a_2,a_3} = E_{\lambda,b} : y^2 = \left(x^2 + (\lambda b)^2\right)\left(x + b^2\right)\left(x + \left[\frac{\lambda}{\lambda+1}b\right]^2\right),$$

where $\lambda = a/b \in K \setminus \{0, \pm 1, -2, -\frac{1}{2}\}$.

Proof. Suppose that none of a_i vanishes and we may choose

$$a = \pm a_1, b = \pm a_2, c = \pm a_3$$

in such a way that $c = ab/(a+b)$. Then none of a, b, c vanishes and $ab = ac + bc$. By Theorem 5.2(ii), $\mathcal{P} = (0, abc)$ is a point of order 3 on the elliptic curve

$$E_{\lambda,b} = E_{a_1,a_2,a_3}.$$

Since $abc = \pm a_1a_2a_3$, either $\mathcal{P} = P$ or $\mathcal{P} = -P$. In both cases P has order 3.

Notice that $\pm a_1, \pm a_2, \pm a_3$ are six distinct elements of K. This means that $\pm a, \pm b, \pm c$ are also six distinct elements of K. If we put $\lambda = a/b$, then

$$\pm\lambda b,\ \pm b,\ \pm\frac{\lambda+1}{\lambda}b$$

are six distinct elements of K. This means (in light of the inequalities $a \neq 0, b \neq 0$) that

$$\lambda \neq 0, \pm 1, -2, -\frac{1}{2}.$$

Suppose P has order 3. By Theorem 5.2(ii), none of a_i vanishes and one of the following four equalities holds:

$$a_2a_3 = a_1a_2 + a_3a_1,\ a_3a_1 = a_1a_2 + a_2a_3,$$
$$a_1a_2 = a_2a_3 + a_3a_1,\ a_1a_2 + a_2a_3 + a_3a_1 = 0.$$

Here are the corresponding choices of a, b, c with $c = ab/(a+b)$:

$$a = a_1, b = -a_2, c = a_3;\ a = a_1, b = -a_2, c = a_3;$$
$$a = a_1, b = a_2, c = a_3;\ a = a_1, b = a_2, c = -a_3.$$

In order to finish the proof, we just need to notice that $a = \lambda b$ and

$$c = \frac{ab}{a+b} = \frac{\lambda b \cdot b}{\lambda b + b} = \frac{\lambda}{\lambda+1}b.$$

□

Theorem 5.6. *Let E be an elliptic curve over K. Then $E(K)$ contains a subgroup isomorphic to $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ if and only if there exists $\lambda \in K \setminus \{0, \pm 1, -2, -\frac{1}{2}\}$ such that E is isomorphic to*

$$\mathcal{E}_{3,\lambda} : y^2 = \left(x^2 + \lambda^2\right)(x+1)\left(x + \left[\frac{\lambda}{\lambda+1}\right]^2\right).$$

Remark 5.7. There is another family of elliptic curves in characteristic $\neq 3$ [6, Table 3 on p. 217] (see also [8, Appendix E]),

$$y^2 + (1 - a(t))xy - b(t)y = x^3 - b(t)x^2,$$

with

$$a(t) = \frac{10 - 2t}{t^2 - 9}, b(t) = \frac{-2(t-1)^2(t-5)}{(t^2-9)^2},$$

whose group of rational points contains a subgroup isomorphic to $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Proof of Theorem 5.6. Let $\lambda \in K \setminus \{0, \pm 1, -2, -1/2\}$ and put $a_1 = \lambda, a_2 = 1, a_3 = \lambda/(\lambda+1)$. Then all a_i do not vanish, a_1^2, a_2^2, a_3^2 are three distinct elements of K, $a_1a_2 = a_2a_3 + a_3a_1$, and $\mathcal{E}_{3,\lambda} = E_{a_1,a_2,a_3}$. It follows from Theorem 5.2 that $\mathcal{E}_{3,\lambda}$ contains a subgroup isomorphic to $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Conversely, suppose that E is an elliptic curve over K such that $E(K)$ contains a subgroup isomorphic to $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. It follows that all three points of order 2 lie in $E(K)$, and therefore E can be represented in the form (1). It is also clear that $E(K)$ contains a point of order 3. Let us choose a point $P = (x(P), y(P)) \in E(K)$ of order 3. We may assume that $x(P) = 0$. We have $P = 2(-P)$, and therefore P is divisible by 2 in $E(K)$. By Theorem 1.1, all $x(P) - \alpha_i = -\alpha_i$ are squares in K. This implies that there exist elements $a_1, a_2, a_3 \in K$ such that $\alpha_i = -a_i^2$. Clearly, all three a_1^2, a_2^2, a_3^2 are distinct. Since P lies on E,

$$y(P)^2 = (x(P) + a_1^2)(x(P) + a_2^2)(x(P) + a_3^2) = a_1^2a_2^2a_3^2 = (a_1a_2a_3)^2,$$

and therefore $y(P) = \pm a_1a_2a_3$. Replacing P by $-P$ if necessary, we may assume that $y(P) = a_1a_2a_3$, i.e., $P = (0, a_1a_2a_3)$ is a K-point of order 3 on

$$E = E_{a_1,a_2,a_3} : y^2 = (x + a_1)^2(x + a_2^2)(x + a_3)^2.$$

It follows from Corollary 5.5 that there exist *nonzero* $b \in K$ and $\lambda \in K \setminus \{0, \pm 1, -2, -1/2\}$ such that

$$E = E_{a_1,a_2,a_3} = E_{\lambda,b} : y^2 = \left(x + (\lambda b)^2\right)\left(x + b^2\right)\left(x + \left[\frac{\lambda}{\lambda+1}b\right]^2\right).$$

But $E_{\lambda,b}$ is isomorphic to

$$E_{\lambda,b}(b) : y'^2 = (x' + \lambda^2)(x' + 1)\left(x' + \left[\frac{\lambda}{\lambda+1}\right]^2\right)$$

while the latter coincides with $\mathcal{E}_{3,\lambda}$. □

Corollary 5.8. *Let E be an elliptic curve over $\mathbb{F}_q$, where $q = 7, 9, 11, 13$. The group $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ if and only if E is isomorphic to one of elliptic curves $\mathcal{E}_{3,\lambda}$.*

Proof. Suppose that $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. By Theorem 5.6, E is isomorphic to one of elliptic curves $\mathcal{E}_{3,\lambda}$.

Conversely, suppose that E is isomorphic to one of these curves. We need to prove that $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. By Theorem 5.6, $E(\mathbb{F}_q)$ contains a subgroup isomorphic to $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$; in particular, 12 divides $|E(\mathbb{F}_q)|$. In order to finish the proof, it suffices to check that $|E(\mathbb{F}_q)| < 24$, but this inequality follows from the Hasse bound (10)

$$|E(\mathbb{F}_q)| \leq q + 2\sqrt{q} + 1 \leq 13 + 2\sqrt{13} + 1 < 22.$$

□

Corollary 5.9. *Let E be an elliptic curve over $\mathbb{F}_{23}$. The group $E(\mathbb{F}_{23})$ is isomorphic to $\mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ if and only if E is isomorphic to one of elliptic curves $\mathcal{E}_{3,\lambda}$.*

Proof. Suppose that $E(\mathbb{F}_{23})$ is isomorphic to $\mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Then it contains a subgroup isomorphic to $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. It follows from Theorem 5.6 that E is isomorphic to one of elliptic curves $\mathcal{E}_{3,\lambda}$.

Conversely, suppose that E is isomorphic to one of these curves. We need to prove that $E(\mathbb{F}_{23})$ is isomorphic to $\mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. By Theorem 5.6, $E(\mathbb{F}_{23})$ contains a subgroup isomorphic to $\mathbb{Z}/6\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$; in particular, 12 divides $|E(\mathbb{F}_{23})|$. The Hasse bound (10) tells us that

$$23 + 1 - 2\sqrt{23} \le |E(\mathbb{F}_{23})| \le 23 + 1 + 2\sqrt{23}$$

and therefore $14 < |E(\mathbb{F}_{23})| < 34$. It follows that $|E(\mathbb{F}_{23})| = 24$; in particular the 2-primary component $E(\mathbb{F}_{23})(2)$ of $E(\mathbb{F}_{23})$ has order 8. On the other hand, $E(\mathbb{F}_{23})(2)$ is isomorphic to a product of two cyclic groups, each of which has even order. This implies that $E(\mathbb{F}_{23})(2)$ is isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Taking into account that $E(\mathbb{F}_{23})$ contains a point of order 3, we conclude that it contains a subgroup isomorphic to

$$(\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

This subgroup has the same order 24 as the whole group $E(\mathbb{F}_{23})$, which ends the proof. □

6. Points of order 5

The following assertion gives a description of points of order 5 on elliptic curves.

Proposition 6.1. *Let $P = (x_0, y_0) \in E(K)$. The point P has order 5 if and only if, for any permutation i, j, k of $1, 2, 3$, one can choose square roots $r_i = \sqrt{x_0 - \alpha_i}$ and $r_i^{(1)} = \sqrt{(r_i + r_j)(r_i + r_k)}$ in such a way that*

$$\begin{aligned} (r_1r_2 + r_2r_3 + r_3r_1) + (r_1^{(1)}r_2^{(1)} + r_2^{(1)}r_3^{(1)} + r_3^{(1)}r_1^{(1)}) = 0,\\ r_1r_2 + r_2r_3 + r_3r_1 \ne 0. \end{aligned} \tag{12}$$

Remark 6.2. Notice that if we drop the condition $r_1r_2r_3 = -y_0$ in formulas (4) and (7), then we get 8 points Q such that $2Q = \pm P$. Similarly, if we drop the conditions $r_1r_2r_3 = -y_0$, $r_1^{(1)}r_2^{(1)}r_3^{(1)} = (r_1 + r_2)(r_2 + r_3)(r_3 + r_1)$ in the formulas (9), then we obtain all points R for which $4R = \pm P$.

Proof. Suppose that P has order 5. Then $-P$ is a 1/4th of P. Therefore there exist r_i and $r_j^{(1)}$ such that

$$x(-P) = x(P) + (r_1r_2 + r_2r_3 + r_3r_1) + (r_1^{(1)}r_2^{(1)} + r_2^{(1)}r_3^{(1)} + r_3^{(1)}r_1^{(1)}).$$

Since $x(P) = x(-P)$, we have

$$(r_1r_2 + r_2r_3 + r_3r_1) + (r_1^{(1)}r_2^{(1)} + r_2^{(1)}r_3^{(1)} + r_3^{(1)}r_1^{(1)}) = 0.$$

On the other hand, if $r_1r_2 + r_2r_3 + r_3r_1$, then the corresponding Q (with $2Q = P$) satisfies

$$x(Q) = x(P) + (r_1r_2 + r_2r_3 + r_3r_1) = x(P)$$

and therefore $Q = P$ or $-P$. Since $2Q = P$, either $P = 2P$ or $Q = -P = -2Q$ has order 5. Clearly, $P \neq 2P$. If $Q = -2Q$ then Q has order dividing 3, which is not true, because its order is 5. The obtained contadiction proves that $r_1r_2 + r_2r_3 + r_3r_1 \neq 0$.

Conversely, suppose there exist square roots

$$r_i = \sqrt{x_0 - \alpha_i} \text{ and } r_i^{(1)} = \sqrt{(r_i + r_j)(r_i + r_k)}$$

that satisfy (12). Replacing if necessary all r_i by $-r_i$, we may and will assume that $r_1r_2r_3 = -y(P)$. Let $Q = (x(Q), y(Q))$ be the corresponding half of P with $x(Q) = x(P) + (r_1r_2 + r_2r_3 + r_3r_1)$. Since $r_1r_2 + r_2r_3 + r_3r_1 \neq 0$, we have $x(Q) \neq x(P)$; in particular, $Q \neq -P$. Replacing if necessary all $r_i^{(1)}$ by $r_i^{(1)}$, we may and will assume that

$$r_1^{(1)}r_2^{(1)}r_3^{(1)} = (r_1 + r_2)(r_2 + r_3)(r_3 + r_1) = -y(Q).$$

Let $R = (x(R), y(R))$ be the corresponding half of Q. Then $4R = 2(2R) = 2Q = P$ and

$$x(R) = x(P) + (r_1r_2 + r_2r_3 + r_3r_1) + (r_1^{(1)}r_2^{(1)} + r_2^{(1)}r_3^{(1)} + r_3^{(1)}r_1^{(1)}) = x(P).$$

This means that either $R = P$ or $R = -P$. If $R = P$, then $R = 4R$ and R has order 3. This implies that both $Q = 2R$ and $P = 4R$ also have order 3. It follows that $P = 2Q = -Q$ and therefore $P = -Q$, which is not the case. Therefore $R = -P$. This means that $R = -4R$, i.e., R has order 5 and therefore $P = -R$ also has order 5. □

In what follows we will use the following identities in the polynomial ring $\mathbb{Z}[t_1, t_2, t_3]$ that could be checked either directly or by using **magma**.

$$\begin{aligned}(-t_1^2 + t_2^2 + t_3^2)(t_1^2 - t_2^2 + t_3^2) + (t_1^2 - t_2^2 + t_3^2)(t_1^2 + t_2^2 - t_3^2)\\ +(t_1^2 + t_2^2 - t_3^2)(-t_1^2 + t_2^2 + t_3^2) =\\ -(t_1 + t_2 + t_3)(-t_1 + t_2 + t_3)(t_1 - t_2 + t_3)(t_1 + t_2 - t_3),\end{aligned} \tag{13}$$

$$\begin{aligned}(-t_1^2 + t_2^2 + t_3^2)(t_1^2 - t_2^2 + t_3^2) + (t_1^2 - t_2^2 + t_3^2)(t_1^2 + t_2^2 - t_3^2)\\ +(t_1^2 + t_2^2 - t_3^2)(-t_1^2 + t_2^2 + t_3^2) + 4t_1^2t_2t_3 + 4t_1t_2^2t_3 + 4t_1t_2t_3^2\\ = t_1^4 + t_2^4 + t_3^4 - 2t_1^2t_2^2 - 2t_2^2t_3^2 - 2t_1^2t_3^2 - 4t_1^2t_2t_3 - 4t_1t_2^2t_3 - 4t_1t_2t_3^2\\ = (t_1 + t_2 + t_3)\left(t_1^3 + t_2^3 + t_3^3 - t_1^2t_2 - t_1t_2^2 - t_2^2t_3 - t_2t_3^2 - t_1^2t_3 - t_1t_3^2 - 2t_1t_2t_3\right).\end{aligned} \tag{14}$$

Theorem 6.3. *Let a_1, a_2, a_3 be elements of K such that $\pm a_1, \pm a_2, \pm a_3$ are six distinct elements of K and none of three elements*

$$\beta_1 = -a_1^2 + a_2^2 + a_3^2, \beta_2 = a_1^2 - a_2^2 + a_3^2, \beta_3 = a_1^2 + a_2^2 - a_3^2$$

vanishes. Then the following conditions hold.

(i) *None of a_i vanishes and $\beta_1^2, \beta_2^2, \beta_3^2$ are three distinct elements of K.*

(ii) *Let us consider an elliptic curve*

$$E_{5;a_1,a_2,a_3} : y^2 = \left(x + \frac{\beta_1^2}{4}\right)\left(x + \frac{\beta_2^2}{4}\right)\left(x + \frac{\beta_3^2}{4}\right)$$

with $P = (0, -\beta_1\beta_2\beta_3/8) \in E_{5;a_1,a_2,a_3}(K)$.

Then P enjoys the following properties.

(1) $P \in 2E_{5;a_1,a_2,a_3}(K)$.
(2) *Assume that*

$$a_1^3+a_2^3+a_3^3-a_1^2a_2-a_1a_2^2-a_2^2a_3-a_2a_3^2-a_1^2a_3-a_1a_3^2-2a_1a_2a_3=0, \quad (a_1+a_2+a_3)(a_1-a_2-a_3)(a_1+a_2-a_3)(a_1-a_2+a_3)\neq 0. \tag{15}$$

Then P has order 5. In addition, $E_{5;a_1,a_2,a_3}(K)$ contains a subgroup isomorphic to $\mathbb{Z}/10\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$.

Proof. (i) Since $a_i \neq -a_i$, none of a_i vanishes. Let $i,j \in \{1,2,3\}$ be two distinct indices and $k \in \{1,2,3\}$ is the third one. Then

$$\beta_i-\beta_j=a_j^2-a_i^2\neq 0,\ \beta_i+\beta_j=2a_k^2\neq 0.$$

This implies that $\beta_i^2 \neq \beta_j^2$.

(ii) Keeping our notation, we obtain that

$$r_1=\pm\frac{\beta_1}{2}=\pm\frac{-a_1^2+a_2^2+a_3^2}{2}, r_2=\pm\frac{\beta_2}{2}=\frac{a_1^2-a_2^2+a_3^2}{2}, r_3=\pm\frac{\beta_3}{2}=\pm\frac{a_1^2+a_2^2-a_3^2}{2},$$

$$r_i^{(1)}=\pm\sqrt{(r_i+r_j)(r_i+r_k)}$$

where i,j,k is any permutation of $1,2,3$. Thanks to Proposition 6.1, it suffices to check that one may choose the square roots r_i and $r_i^{(1)}$ in such a way that $r_1r_2+r_2r_3+r_3r_1\neq 0$ and

$$(r_1r_2+r_2r_3+r_3r_1)+(r_1^{(1)}r_2^{(1)}+r_2^{(1)}r_3^{(1)}+r_3^{(1)}r_1^{(1)})=0. \tag{16}$$

Let us put

$$r_i=\frac{\beta_i}{2}=\frac{-a_i^2+a_j^2+a_k^2}{2}.$$

We have

$$r_1+r_2=a_3^2, \quad r_1+r_3=a_2^2, \quad r_2+r_3=a_1^2.$$

It follows that

$$(r_1^{(1)})^2=a_2^2a_3^2, \quad (r_2^{(1)})^2=a_1^2a_3^2, \quad (r_3^{(1)})^2=a_1^2a_1^2.$$

Let us put

$$r_1^{(1)}=a_2a_3, \quad r_2^{(1)}=a_1a_3, \quad r_3^{(1)}=a_1a_2.$$

Then the condition (16) may be rewritten as follows.

$$(-a_1^2+a_2^2+a_3^2)(a_1^2-a_2^2+a_3^2)+(a_1^2-a_2^2+a_3^2)(a_1^2+a_2^2-a_3^2)$$
$$+(a_1^2+a_2^2-a_3^2)(-a_1^2+a_2^2+a_3^2)+4a_1^2a_2a_3+4a_1a_2^2a_3+4a_1a_2a_3^2=0.$$

In light of (14), the condition (16) may be rewritten as

$$(a_1+a_2+a_3)(a_1^3+a_2^3+a_3^3-a_1^2a_2-a_1a_2^2-a_2^2a_3-a_2a_3^2-a_1^2a_3-a_1a_3^2-2a_1a_2a_3)=0.$$

The latter equality follows readily from the assumption (15) of Theorem. By Proposition 6.1, it suffices to check that $r_1r_2+r_2r_3+r_3r_1\neq 0$. In other words, we need to prove that

$$(-a_1^2+a_2^2+a_3^2)(a_1^2-a_2^2+a_3^2)+(a_1^2-a_2^2+a_3^2)(a_1^2+a_2^2-a_3^2)$$
$$+(a_1^2+a_2^2-a_3^2)(-a_1^2+a_2^2+a_3^2)\neq 0. \tag{17}$$

In light of (13), this inequalty is equivalent to

$$(a_1+a_2+a_3)(a_1-a_2-a_3)(a_1+a_2-a_3)(a_1-a_2+a_3)\neq 0.$$

But the latter inequality holds, by the assumption (15) of Theorem. Hence, P has order 5. Clearly, P and all points of order 2 generate a subgroup that is isomorphic to $\mathbb{Z}/10\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$. □

Theorem 6.4. *Let E be an elliptic curve over K. Then the following conditions are equivalent.*

(i) *$E(K)$ contains a subgroup isomorphic to $\mathbb{Z}/10\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$.*
(ii) *There exists a triple $\{a_1,a_2,a_3\}\subset K$ that satisfies all the conditions of Theorem 6.3, including (15) and such that E is isomorphic to $E_{5;a_1,a_2,a_3}$.*

Proof. (i) follows from (ii), thanks to Theorem 6.3.

Suppose (i) holds. In order to prove (ii) it suffices to check that E is isomorphic to a certain $E_{5;a_1,a_2,a_3}$ over K. We may assume that E is defined by an equation of the form (1). Suppose that $P=(0,y(P))\in E(K)$ has order 5. Then $P=4(-P)$ is divisible by 4 in $E(K)$. This implies the existence of square roots $r_i=\sqrt{-\alpha_i}\in K$ and $r_i^{(1)}=\sqrt{(r_i+r_j)(r_i+r_k)}\in K$ in such a way that

$$x(-P)=x(P)+(r_1r_2+r_2r_3+r_3r_1)+(r_1^{(1)}r_2^{(1)}+r_2^{(1)}r_3^{(1)}+r_3^{(1)}r_1^{(1)}),$$

$$r_1^{(1)}r_2^{(1)}r_3^{(1)}=(r_1+r_2)(r_2+r_3)(r_3+r_1).$$

Since $x(-P)=x(P)=0$,

$$(r_1r_2+r_2r_3+r_3r_1)+(r_1^{(1)}r_2^{(1)}+r_2^{(1)}r_3^{(1)}+r_3^{(1)}r_1^{(1)})=0. \tag{18}$$

Since the order of P is *not* 3,

$$r_1r_2+r_2r_3+r_3r_1\neq 0. \tag{19}$$

Recall that none of r_i+r_j vanishes. Let us choose square roots

$$b_1=\sqrt{r_2+r_3}, b_2=\sqrt{r_1+r_3}, b_3=\sqrt{r_1+r_2}$$

in such a way that $r_1^{(1)}=b_2b_3, r_2^{(1)}=b_3b_1$. Since

$$r_1^{(1)}r_2^{(1)}r_3^{(1)}=b_1^2b_2^2b_3^2=(b_1b_2b_3)^2,$$

we conclude that

$$r_3^{(1)}=\frac{r_1^{(1)}r_2^{(1)}r_3^{(1)}}{r_2^{(1)}r_3^{(1)}}=\frac{(b_1b_2b_3)^2}{(b_2b_3)(b_3b_1)}=b_1b_2.$$

We obtain that

$$r_1^{(1)}=b_2b_3, r_2^{(1)}=b_3b_1, r_3^{(1)}=b_1b_2. \tag{20}$$

Unfortunately, b_i do not have to lie in K. However, all the ratios b_i/b_j lie in K^*. We have

$$r_2+r_3=b_1^2, r_1+r_3=b_2^2, r_1+r_2=b_3^2$$

and therefore

$$
\begin{aligned}
&r_1 = \frac{-b_1^2+b_2^2+b_3^2}{2},\ r_2 = \frac{b_1^2-b_2^2+b_3^2}{2},\ r_3 = \frac{b_1^2+b_2^2-b_3^2}{2},\\
&\alpha_1 = -r_1^2 = \frac{(-b_1^2+b_2^2+b_3^2)^2}{4},\ \alpha_2 = -r_2^2 = -\frac{(b_1^2-b_2^2+b_3^2)^2}{4},\\
&\alpha_3 = -r_3^2 = -\frac{(b_1^2+b_2^2-b_3^2)^2}{4},\\
&P = (0, -(r_1+r_2)(r_2+r_3)(r_3+r_1)) = (0, -b_1^2b_2^2b_3^2) \in E(K).
\end{aligned} \tag{21}
$$

Since none of r_i vanishes, we get

$$-b_1^2+b_2^2+b_3^2 \neq 0,\ b_1^2-b_2^2+b_3^2 \neq 0,\ b_1^2+b_2^2-b_3^2 \neq 0.$$

Let us put

$$\gamma_1 = -b_1^2+b_2^2+b_3^2, \gamma_2 = b_1^2-b_2^2+b_3^2, \gamma_3 = b_1^2+b_2^2-b_3^2.$$

It follows from Theorem 6.3(i) that all β_i are *distinct* nonzero elements of K. The inequality (19) combined with first formula of (21) gives us

$$
\begin{aligned}
(-b_1^2+b_2^2+b_3^2)(b_1^2-b_2^2+b_3^2) + (b_1^2-b_2^2+b_3^2)(b_1^2+b_2^2-b_3^2)\\
+(b_1^2+b_2^2-b_3^2)(-b_1^2+b_2^2+b_3^2) \neq 0,
\end{aligned}
$$

which is equivalent (thanks to (13)) to

$$(b_1+b_2+b_3)(b_1-b_2-b_3)(b_1+b_2-b_3)(b_1-b_2+b_3) \neq 0.$$

In particular,

$$b_1+b_2+b_3 \neq 0.$$

The equality (18) gives us (thanks to (14))

$$(b_1+b_2+b_3)(b_1^3+b_2^3+b_3^3-b_1^2b_2-b_1b_2^2-a_2^2b_3-b_2b_3^2-b_1^2b_3-b_1b_3^2-2b_1b_2b_3) = 0,$$

i.e.,

$$(b_1^3+b_2^3+b_3^3-b_1^2b_2-b_1b_2^2-a_2^2b_3-b_2b_3^2-b_1^2b_3-b_1b_3^2-2b_1b_2b_3) = 0.$$

Let us put

$$a_1 = \frac{b_1}{b_3},\ a_2 = \frac{b_2}{b_3},\ a_3 = \frac{b_3}{b_3} = 1.$$

All a_i lie in K. Clearly, the triple $\{a_1, a_2, a_3\}$ satisfies all the conditions of Theorem 6.3 including (15). Let us put

$$
\begin{aligned}
\beta_1 = -a_1^2+a_2^2+a_3^2 = \frac{\gamma_1}{b_3^2} = \frac{\gamma_1}{r_1+r_2},\\
\beta_2 = a_1^2-a_2^2+a_3^2 = \frac{\gamma_2}{b_3^2} = \frac{\gamma_2}{r_1+r_2},\\
\beta_3 = a_1^2+a_2^2-a_3^2 = \frac{\gamma_3}{b_3^2} = \frac{\gamma_3}{r_1+r_2}.
\end{aligned}
$$

The equation of E is

$$y^2 = \left(x+\frac{\gamma_1^2}{4}\right)\left(x+\frac{\gamma_2^2}{4}\right)\left(x+\frac{\gamma_3^2}{4}\right).$$

Then E is isomorphic to

$$E(r_1+r_2): y'^2 = \left(x' + \frac{\gamma_1^2}{4(r_1+r_2)^2}\right)\left(x' + \frac{\gamma_2^2}{4(r_1+r_2)^2}\right)\left(x' + \frac{\gamma_3^2}{4(r_1+r_2)^2}\right) = \left(x' + \frac{\beta_1^2}{4}\right)\left(x' + \frac{\gamma_2^2}{4}\right)\left(x' + \frac{\gamma_3^2}{4}\right).$$

Clearly, $E(r_1+r_2)$ coincides with $E_{5;a_1,a_2,a_3}$. □

Remark 6.5. Let $E_{5;a_1,a_2,a_3}$ be as in Theorem 6.3. Clearly, $E_{5;a_1,a_2,a_3}(a_3) = E_{5;a_1/a_3,a_2/a_3,1}$. Let us put $\lambda = a_1/a_3, \mu = a_2/a_3$. Then

(22)
$$E_{5;a_1/a_3,a_2/a_3,1} = E_{5;\lambda,\mu,1}:$$
$$y^2 = \left[x + \left(\frac{-\lambda^2+\mu^2+1}{2}\right)^2\right]\left[x + \left(\frac{\lambda^2-\mu^2+1}{2}\right)^2\right]\left[x + \left(\frac{\lambda^2+\mu^2-1}{2}\right)^2\right].$$

The equation of (isomorphic) $E_{5;\lambda,\mu,1}\left(\frac{\lambda^2+\mu^2-1}{2}\right)$ is as follows.

(23)
$$E_{5;\lambda,\mu,1}\left(\frac{\lambda^2+\mu^2-1}{2}\right): y^2 = \left[x + \left(\frac{1-\lambda^2+\mu^2}{\lambda^2+\mu^2-1}\right)^2\right]\left[x + \left(\frac{\lambda^2-\mu^2+1}{\lambda^2+\mu^2-1}\right)^2\right](x+1).$$

The conditions on a_1, a_2, a_3 may be rewritten in terms of λ, μ as follows.

$$\begin{gathered}\lambda^3+\mu^3-\lambda^2\mu-\lambda\mu^2-\lambda^2-2\lambda\mu-\mu^2-\lambda-\mu+1=0,\\ \lambda\pm\mu\neq\pm1,\ \lambda\neq0,\ \mu\neq0,\ \lambda\neq\pm\mu,\\ \lambda^2+\mu^2\neq1,\ \lambda^2-\mu^2\neq\pm1.\end{gathered} \tag{24}$$

The equality (24) is equivalent to

$$(\lambda+\mu)(\lambda-\mu)^2-(\lambda+\mu)^2-(\lambda+\mu)+1=0. \tag{25}$$

Multiplying (25) by (non-vanishing) $(\lambda+\mu)$, we get the equivalent equation

$$(\lambda^2-\mu^2)^2-(\lambda+\mu)^3-(\lambda+\mu)^2+(\lambda+\mu)=0. \tag{26}$$

Let us make the change of variables

$$\xi = \lambda+\mu, \eta = \lambda^2-\mu^2.$$

Then (26) may be rewritten as

$$\eta^2 = \xi(\xi^2+\xi-1), \tag{27}$$

which is an (affine model of an) elliptic curve if $\mathrm{char}(K)\neq5$ and a singular rational plane cubic (Cartesian leaf) if $\mathrm{char}(K)=5$. Since

$$\lambda^2+\mu^2 = \frac{(\lambda+\mu)^2+(\lambda-\mu)^2}{2} = \frac{\xi^2+\frac{\eta^2}{\xi^2}}{2} = \frac{\xi^2+\frac{\xi^2+\xi-1}{\xi}}{2} = \frac{\xi^3+\xi^2+\xi-1}{2\xi}, \tag{28}$$

the only restrictions on (ξ,η) besides the equality (27) are the inequalities

$$\xi(\xi^2+\xi-1)\neq0,\pm1;\ \xi^3+\xi^2+\xi-1\neq2\xi,\ \pm1\neq\frac{\eta}{\xi}=\sqrt{\frac{\xi(\xi^2+\xi-1)}{\xi^2}},$$

i.e.

$$\xi\neq0,\pm1,\frac{-1\pm\sqrt{5}}{2}. \tag{29}$$

This means that

$$(\xi,\eta) \notin \{(0,0), (\pm 1, \pm 1), (\frac{-1 \pm \sqrt{5}}{2}, 0)\}. \tag{30}$$

In light of (28), the equation (22) may be rewritten with coefficients being rational functions in ξ, η (rather than (λ, μ)) as follows.

$$\mathcal{E}_{5,\xi,\eta} : y^2 = y^2 = \left[x + \left(\frac{2(1-\eta)}{\xi^3+\xi^2+\xi-3}\right)^2\right]\left[x + \left(\frac{2(\eta+1)}{\xi^3+\xi^2+\xi-3}\right)^2\right](x+1).$$

Theorem 6.6. *Let E be an elliptic curve over K. Then the following conditions are equivalent.*

(i) *$E(K)$ contains a subgroup isomorphic to $\mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.*
(ii) *There exist $(\xi, \eta) \in K^2$ that satisfy the equation (27) and inequalities (30) and such that E is isomorphic to $\mathcal{E}_{5,\xi,\eta}$.*

Proof. The result follows from Theorem 6.4 combined with Remark 6.5. □

Remark 6.7. In Theorem 6.6 we do *not* assume that $\mathrm{char}(K) \neq 5$!

Corollary 6.8. *Let E be an elliptic curve over $\mathbb{F}_q$ with $q = 13, 17, 19, 23, 25, 27$. Then $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ if and only if E is isomorphic to one of $\mathcal{E}_{5,\xi,\eta}$.*

Proof. Suppose that $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. By Theorem 6.6, E is isomorphic to one of elliptic curves $\mathcal{E}_{5,\xi,\eta}$.

Conversely, suppose that E is isomorphic to one of these curves. We need to prove that $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. By Theorem 6.6, $E(\mathbb{F}_q)$ contains a subgroup isomorphic to $\mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$; in particular, 20 divides $|E(\mathbb{F}_q)|$. In order to finish the proof, it suffices to check that $|E(\mathbb{F}_q)| < 40$, but this inequality follows from the Hasse bound (10)

$$|E(\mathbb{F}_q)| \le q + 2\sqrt{q} + 1 \le 27 + 2\sqrt{27} + 1 < 40.$$

□

Corollary 6.9. *Let E be an elliptic curve over $\mathbb{F}_q$ with $q = 31, 37, 41, 43$. Then $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/20\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ if and only if E is isomorphic to one of $\mathcal{E}_{5,\xi,\eta}$.*

Proof. Suppose that $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/20\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$; the latter contains a subgroup isomorphic to $\mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. By Theorem 6.6, E is isomorphic to one of elliptic curves $\mathcal{E}_{5,\xi,\eta}$.

Conversely, suppose that E is isomorphic to one of these curves. We need to prove that $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/20\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. By Theorem 6.6, $E(\mathbb{F}_q)$ contains a subgroup isomorphic to $\mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$; in particular, 20 divides $|E(\mathbb{F}_q)|$. It follows from the Hasse bound (10) that

$$20 < 31 - 2\sqrt{31} + 1 \le |E(\mathbb{F}_q)| \le 43 + 2\sqrt{43} + 1 < 60.$$

This implies that $|E(\mathbb{F}_q)| = 40$, and therefore $E(\mathbb{F}_q)$ is isomorphic to a direct sum of $\mathbb{Z}/5\mathbb{Z}$ and an order 8 abelian group $E(\mathbb{F}_q)(2)$; in addition, the latter group is isomorphic to a direct sum of two cyclic groups of even order (because it contains

a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$). This implies that $E(\mathbb{F}_q)(2)$ is isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. It follows that $E(\mathbb{F}_q)$ is isomorphic to a direct sum

$$\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/20\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

□

Corollary 6.10. *Let E be an elliptic curve over $\mathbb{F}_q$ with $q = 59$ or 61. Then $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/30\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ if and only if E is isomorphic to one of $\mathcal{E}_{5,\xi,\eta}$.*

Proof. Suppose that $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/30\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$; the latter contains a subgroup isomorphic to $\mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. By Theorem 6.6, E is isomorphic to one of elliptic curves $\mathcal{E}_{5,\xi,\eta}$.

Conversely, suppose that E is isomorphic to one of these curves. We need to prove that $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/30\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. By Theorem 6.6, $E(\mathbb{F}_q)$ contains a subgroup isomorphic to $\mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$; in particular, 20 divides $|E(\mathbb{F}_q)|$. It follows from the Hasse bound (10) that

$$40 < 59 - 2\sqrt{59} + 1 \leq |E(\mathbb{F}_q)| < 61 + 2\sqrt{61} + 1 < 80.$$

This implies that $|E(\mathbb{F}_q)| = 60$; in particular, $E(\mathbb{F}_q)$ contains a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z}$. This implies that $E(\mathbb{F}_q)$ contains a subgroup isomorphic to

$$(\mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/30\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z};$$

the order of this subgroup is 60, i.e., it coincides with the order of the whole group $E(\mathbb{F}_q)$. □

References

[1] E. Bombieri, W. Gubler, Heights in Diophantine Geometry. New Mathematical Monographs, **4**. Cambridge University Press, Cambridge, 2006.

[2] J.P. Buhler, *Elliptic curves, modular forms and applications*, pp. 5–81. In: Arithmetic Algebraic Geometry (B. Conrad, K. Rubin, eds.) IAS/Park City Mathematics Series **9**, American Mathematical Society, Providence, RI, 2001.

[3] J.W.C. Cassels, Diophantine equations with special reference to elliptic curves. J. London Math. Soc. **41** (1966), 193–291.

[4] D. Hüsemoller, Elliptic Curves. Second edition. With appendices by O. Forster, R. Lawrence and S. Theisen. Graduate Texts in Mathematics **111** Springer-Verlag, New York, 2004.

[5] A. Knapp, Elliptic Curves. Mathematical Notes **40**, Princeton University Press, Princeton, NJ, 1992.

[6] D.S. Kubert, *Universal bounds on the torsion of elliptic curves*. Proc. London Math. Soc. (3) **33** (1976), 193–237.

[7] S. Lang, Elliptic Curves: Diophantine Analysis. Grundlehren der Mathematischen Wissenschaften **231**, Springer-Verlag, Berlin-New York, 1978.

[8] A. Lozano-Robledo, Elliptic Curves, Modular Forms and their L-functions. Student Mathematical Library **38**, American Mathematical Society, Providence, RI, 2011.

[9] A. Silverberg, *Explicit Families of Elliptic Curves with Prescribed Mod N representations*, pp. 447–461. In: Modular Forms and Fermat's Last Theorem (G. Cornell, J.H. Silverman, G. Stevens, eds.) Springer-Verlag New York Inc., 1997.

[10] J.S. Silverman, Arithmetic of Elliptic Curves. Second edition. Graduate Texts in Mathematics **106**, Springer, Dordrecht Heidelberg London New York, 2009.

[11] J.S. Silverman, J.T. Tate, Rational Points on Elliptic Curves. Second Edition. Springer Cham Heidelberg New York Dordrecht London, 2015.

[12] T. Shioda, *On rational points of the generic elliptic curve with level N structure over the field of modular functions of level N*. J. Math. Soc. Japan **25** (1973), 144-157.

[13] J. Tate, *Algebraic Formulas in Arbitrary Characteristic*. Appendix 1 to: S. Lang, Elliptic Functions, Second Edition. Springer-Verlag New York Inc., 1987.

[14] L.C. Washington, Elliptic Curves: Number Theory and Cryptography. Second edition. Chapman & Hall/CRC Press, Boca Raton London New York, 2008.
[15] J. Yelton, Dyadic torsion of elliptic curves. European J. Math. **1** (2015), no. 4, 704–716.

St. Petersburg State University, Department of Mathematics and Mechanics, Universitetsky prospekt, 28, Peterhof, St. Petersburg, 198504, Russia8
E-mail address: bekker.boris@gmail.com

Pennsylvania State University, Department of Mathematics, University Park, PA 16802, USA
E-mail address: zarhin@math.psu.edu