Алгебра и анализ
Том 29 (2017), № 4

St. Petersburg Math. J.
Vol. 29 (2018), No. 4, Pages 683–713
http://dx.doi.org/10.1090/spmj/1512
Article electronically published on June 1, 2018

DIVISION BY 2 OF RATIONAL POINTS ON ELLIPTIC CURVES

B. M. BEKKER AND YU. G. ZARHIN

Easy reading for professionals

Abstract. The well-known divisibility by 2 condition for rational points on elliptic curves with rational 2-torsion is reproved in a simple way. Next, the explicit formulas for division by 2^n obtained in §2 are used to construct versal families of elliptic curves that contain points of orders 4, 5, 6, and 8. These families are further employed to describe explicitly elliptic curves over certain finite fields $\mathbb{F}_q$ with a prescribed (small) group $E(\mathbb{F}_q)$. The last two sections are devoted to the cases of 3- and 5-torsion.

§1. Introduction

Let E be an elliptic curve over a number field K. The famous Mordell–Weil theorem asserts that the (Abelian) group $E(K)$ of K-points on E is finitely generated [3, 18, 21]. The first step in its proof (and actual finding a finite set that generates $E(K)$) is the weak Mordell–Weil theorem that asserts that the quotient $E(K)/2E(K)$ is a finite (Abelian) group. This step is called 2-descent and its basic ingredient is a criterion for a K-point on E to be twice another K-point (under an additional assumption that all points of order 2 on E are defined over K). In this paper we give a new treatment of this criterion, which seems to be less computational than the previous ones (see [10, Chapter 5, pp. 102–104], [4], [8, Theorem 4.2 on pp. 85–87], [2, Lemma 7.6 on p. 67], [1, pp. 331–332]). Our approach allows us to describe explicitly 2-power torsion on elliptic curves. Also, we obtain explicit description of families of elliptic curves with various torsion subgroups over arbitrary fields of characteristic different from 2 (the problem of constructing elliptic curves with given torsion goes back to B. Levi [14]).

The paper is organized as follows. We work with elliptic curves E over an arbitrary field K with $\mathrm{char}(K) \neq 2$. In §2 we discuss the criterion of divisibility by 2 and explicit formulas for the “half-points” in $E(K)$. Next we discuss a criterion of divisibility by any power of 2 in $E(K)$ (§3). In §4 we collect useful results about elliptic curves and their torsion. In §§5, 6, and 7 we use the explicit formulas of §2 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. (Moreover, in §5 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 parametrized by K-points of rational curves that are closely related to certain modular curves of genus zero (see [9, 14–16]); however, our approach remains quite elementary. Also, in §§6 and 8 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 $\mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$,

2010 *Mathematics Subject Classification.* Primary 14H52.

Key words and phrases. Torsion subgroup, 2-descent, Mordell–Weil theorem.

The first author was partially supported by RFBR (grant no. 14-01-00393).

The second author was partially supported by a grant from the Simons Foundation (#246625 to Yuri Zarkhin). This work was started 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.

respectively. These two families are parametrized 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). Using deep and highly nontrivial results of Mazur [12], Kamienny [5], and Kenku–Momose [7], we describe explicitly the elliptic curves E over the field $\mathbb{Q}$ of rational numbers and over quadratic fields K such that the torsion subgroup $E(\mathbb{Q})_t$ of $E(\mathbb{Q})$ (respectively $E(K)_t$ of $E(K)$) is isomorphic to a certain finite group.

§2. 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

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

The following statement is pretty well known, see [3, pp. 269–270], [10, Chapter 5, pp. 102–104], [4], [8, Theorem 4.2 on pp. 85–87], [2, Lemma 7.6 on p. 67] [1, pp. 331–332], [21, pp. 212–214] and also [22].

Theorem 2.1. *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 statement is traditionally used in the proof of the weak Mordell–Weil theorem. While the proof of the claim that divisibility implies squareness is straightforward, it seems that the known elementary proofs of the converse statement are more involved/computational. (Note that there is another approach, based on Galois cohomology [17, X.1, pp. 313–315], which works for hyperelliptic Jacobians as well, see [13].)

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

Proof. So, 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 $y_1\neq 0$, so that 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 [18, pp. 25–27], [21, 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, obviously, they are distinct. Consequently, the corresponding square roots (see [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, which proves the required statement. $\square$

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

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

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 identity holds true 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 $(t - r_1)(t - r_2)(t - r_3)$. Recalling that $-(lx_0 + m) = y_0$, we get

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

Also,

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

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

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

whence

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

i.e.,

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

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

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

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 $r_1 r_2 r_3 = -y_0$. Using the last relation, we may rewrite (5) as[2]

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

Moreover,

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

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

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

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

$$\begin{aligned} x_1 - \alpha_i &= (x_0 - \alpha_i) + r_1 r_2 + r_2 r_3 + r_3 r_1 \\ &= r_i^2 + r_1 r_2 + r_2 r_3 + r_3 r_1 = (r_i + r_j)(r_i + r_k). \end{aligned}$$

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 can recover the corresponding (r_1, r_2, r_3). Namely, formulas (8) and (7) imply that

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

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

Example 2.2. Let the role of $P = (x_0, y_0)$ be played by 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,

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

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

Recall that, in formula (6) for the coordinates of the points $\frac{1}{2}P$, we may choose the signs of r_1, r_2, r_3 arbitrarily 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 $(r_1, -r_2, -r_3)$, $(-r_1, r_2, -r_3)$, and $(-r_1, -r_2, r_3)$. Let these halves be denoted 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.

Theorem 2.3. *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

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

which implies

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

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 $\mathcal{Q}_i$ 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 in place of i, we get $\mathcal{Q}_j = -Q$; but $\mathcal{Q}_i \neq \mathcal{Q}_j$ because $i \neq j$. Therefore, $\mathcal{Q}_i, -Q, W_i$ are three distinct points. This proves (ii).

We prove (iii). Since

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

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

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

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

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

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

§3. Division by 2^n

Using the above formulas that describe division by 2 on E, we 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 $\mu = 0, 1, 2, \ldots$. Let $r_1^{(\mu)}, r_2^{(\mu)}, r_3^{(\mu)}$ $(\mu = 0, 1, 2, \ldots)$ be arbitrary sequences of elements of L that satisfy the relations

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

Then for each permutation i, j, k of $1, 2, 3$, using formula (8), we get

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

which implies that

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

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 the $(r_i^{(\mu)} + r_j^{(\mu)})(r_i^{(\mu)} + r_k^{(\mu)})$ are squares in K for all $i = 1, 2, 3$. We have proved the following statement.

Theorem 3.1. *Let $P = (x_0, y_0) \in E(K)$. Let $r_1^{(\mu)}, r_2^{(\mu)}, r_3^{(\mu)}$ $(\mu = 0, 1, 2, \ldots)$ be sequences of elements of L such that*

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

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 $\mu = 0, 1, \ldots n-1$, the square roots $r_1^{(\mu)}, r_2^{(\mu)}, r_3^{(\mu)}$ may be chosen 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, all $r_i^{(\mu)}$ lie in K for $\mu = 0, 1, \ldots n-1$).

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

Example 3.2. 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),

$$x_1 = x_0 + (r_1 r_2 + r_2 r_3 + r_3 r_1), \quad y_1 = -(r_1 + r_2)(r_2 + r_3)(r_3 + r_1),$$

where the square roots

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

are chosen in such a way that $r_1 r_2 r_3 = -y_0$. Next, let

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

be square roots chosen so that

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

By (4) and (7), we have

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

which implies that

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

§4. Torsion of elliptic curves

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

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

and respects 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 $i = 1, 2, 3$. Moreover, if $P = (0, y(P))$ lies in $E(K)$, then it goes (under the above isomorphism) to $(0, y(P)/\kappa^3) \in E(\kappa)(K)$.

We will also use the following classical result of Hasse (Hasse bound), see [21, Theorem 4.2 on p. 97].

Theorem 4.1. *If q is a prime power, $\mathbb{F}_q$ a q-element finite field and E 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*

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

Another result that we are going to use is the following immediate corollary to a celebrated theorem of Mazur (see [12] and [11, Theorem 2.5.2 on p. 187]).

Theorem 4.2. *If E is an elliptic curve over $\mathbb{Q}$ and the torsion subgroup $E(\mathbb{Q})_t$ of $E(\mathbb{Q})$ is not cyclic, then $E(\mathbb{Q})_t$ is isomorphic to $\mathbb{Z}/2m\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ with $m = 1, 2, 3$ or 4. In particular, if m equals 3 or 4 and $E(\mathbb{Q})$ contains a subgroup isomorphic to $\mathbb{Z}/2m\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, then $E(\mathbb{Q})_t$ is isomorphic to $\mathbb{Z}/2m\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.*

The next assertion follows readily from the list of possible torsion subgroups of elliptic curves over quadratic fields, as obtained by Kamienny in [5] and Kenku–Momose in [7] (see also [6, Theorem 1]).

Theorem 4.3. *Let E be an elliptic curve over a quadratic field K. Assume that all points of order 2 on E are defined over K. Let $E(K)_t$ be the torsion subgroup of $E(K)$. Then $E(K)_t$ is isomorphic either to $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$, or to $\mathbb{Z}/2m\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ with $1 \le m \le 6$.*

In particular, $E(K)_t$ enjoys the following properties.

1. *If $m = 5$ or 6 and $E(K)$ contains a subgroup isomorphic to $\mathbb{Z}/2m\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$, then $E(K)_t$ is isomorphic to $\mathbb{Z}/2m\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$.*
2. *If $E(K)$ contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$, then $E(K)_t$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$.*

§5. Rational points of order 4

We are going to describe explicitly the elliptic curves (1) that contain a K-point of order 4. For 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

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

Notice that

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

All three differences

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

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

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

Now Example 2.2 gives us four points Q with $2Q = W_3$, namely,

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

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 5.1. Our computations show that whenever Q is a K-point on $E_{1,\lambda}$, we have

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

Both cases (signs) do occur.

Remark 5.2. There is another family of elliptic curves (see [9, Table 3 on p. 217] and also [15, Part 2] and [11, Appendix E])

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

whose group of K-points contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$. If we put

$$y_1 := y + \frac{x - (t^2 - \frac{1}{16})}{2},$$

then the equation may be rewritten as

$$y_1^2 = x^3 - \left(t^2 - \frac{1}{16}\right) x^2 + \left[\frac{x - (t^2 - \frac{1}{16})}{2}\right]^2 = \left(x - t^2 + \frac{1}{16}\right)\left(x + \frac{t}{2} + \frac{1}{8}\right)\left(x - \frac{t}{2} + \frac{1}{8}\right).$$

If we put $x_1 := x - t^2 + 1/16$, then the equation becomes

$$y_1^2 = x_1\left(x_1 + \left(t + \frac{1}{4}\right)^2\right)\left(x_1 + \left(t - \frac{1}{4}\right)^2\right),$$

which determines the elliptic curve $\mathcal{E}_{1,\lambda}(1/\kappa)$ with

$$\lambda = \frac{t - \frac{1}{4}}{t + \frac{1}{4}}, \quad \kappa = t + \frac{1}{4}.$$

In particular, $\mathfrak{E}_{1,t}$ is isomorphic to $\mathcal{E}_{1,\lambda}$.

Theorem 5.3. *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 2.1, both nonzero differences

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

are squares in K; moreover, 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 see that E is isomorphic to

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

which is none other than $\mathcal{E}_{1,\lambda}$ with $\lambda = a/b$. ☐

Corollary 5.4. *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 5.3, E is isomorphic to

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

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

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

Conversely, let $E = \mathcal{E}_{1,2}$. 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 5.3, $E(\mathbb{F}_5)$ contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$; in particular, 8 divides $|E(\mathbb{F}_5)|$. To finish the proof, now it suffices to check that $|E(\mathbb{F}_5)| < 16$, but this follows from the Hasse bound (10)

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

Corollary 5.5. *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 $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. From Theorem 5.3 it follows 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 λ equals ± 2 or ± 3, and, therefore, λ^2 is 4 or 2, i.e., E is isomorphic to one of the two elliptic curves

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

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 5.3, $E(\mathbb{F}_7)$ 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 follows from the Hasse bound (10)

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

Theorem 5.6. *Suppose that K contains $\mathbf{i} = \sqrt{-1}$. Let a, b be nonzero elements of K such that $a \neq \pm b$, $a \neq \pm \mathbf{i}b$. 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. Moreover,

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

This implies that all $\alpha_i - \alpha_j$ are squares in K. From Theorem 2.1 it follows 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. $\square$

Keeping the notation and assumptions of Theorem 5.6, we use formula (6) to describe explicitly all twelve points of order 4.

(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

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

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 5.7. 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, it only suffices to put $\kappa = a^2 + b^2$ and observe that $E_{a,b}(\kappa) = \mathcal{E}_{2,\lambda}$. Theorem 5.6 shows 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,

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

(see [19] and [15, pp. 451–453]; see also Remark 5.9).

Theorem 5.8. *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 5.7) 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 5.3, 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 $\alpha_1 = -\delta^2, \alpha_2 = -1, \alpha_3 = 0$. From Theorem 2.1 it follows 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

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

Now it only suffices to plug the formula for δ in the equation of $\mathcal{E}_{1,\delta}$ and get $\mathcal{E}_{2,\lambda}$. $\square$

Remark 5.9. Using a different parametrization of the unit circle in the proof of Theorem 5.8, 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 the 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 5.7. Indeed, the latter differs from $E(\kappa)$ with $\kappa = 2\lambda\sqrt{-1}/(\lambda^2+1)$, only by the change of the parameter λ by u.

Corollary 5.10. *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 the elliptic curves $\mathcal{E}_{2,\lambda}$. Moreover, 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 $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Theorem 5.8 shows that E is isomorphic to $\mathcal{E}_{2,\lambda}$.

Conversely, suppose that E is isomorphic to one of those 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 5.8, $E(\mathbb{F}_q)$ contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$; in particular, 16 divides $|E(\mathbb{F}_q)|$. Now it suffices to check that $|E(\mathbb{F}_q)| < 32$, but this inequality follows from the Hasse bound (10)

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

Now we assume that $q = 9$. Then λ is one of four $\pm(1 \pm \mathbf{i})$. For all such λ we have

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

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

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

Corollary 5.11. *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 the 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 $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Theorem 5.8 shows that E is isomorphic to $\mathcal{E}_{2,\lambda}$.

Conversely, suppose that E is isomorphic to one of those 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 5.8, $E(\mathbb{F}_{29})$ 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) yields

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

whence

$$19 < |E(\mathbb{F}_{29})| < 41.$$

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 the product of two cyclic 2-groups, each of which has order divisible by 4. Consequently, $E(\mathbb{F}_{29})$ is isomorphic to $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. $\square$

Theorem 5.12. *Let $K = \mathbb{Q}(\sqrt{-1})$, and let E be an elliptic curve over $\mathbb{Q}(\sqrt{-1})$. Then the torsion subgroup $E(\mathbb{Q}(\sqrt{-1}))_t$ of $E(\mathbb{Q}(\sqrt{-1}))$ is isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ if and only if there exists $\lambda \in K \setminus \{0, \pm 1, \pm\sqrt{-1}\}$ such that E is isomorphic to $\mathcal{E}_{2,\lambda}$.*

Proof. By Theorem 4.3, if $E(\mathbb{Q}(\sqrt{-1}))$ contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, then $E(\mathbb{Q}(\sqrt{-1})_t$ is isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Now the desired result follows from Theorem 5.3. $\square$

§6. Points of order 8

We 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 5.1, $x(Q) = \pm\lambda$. First, we assume that $x(Q) = \lambda$ (such Q does exist).

Lemma 6.1. *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

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

By Theorem 2.1, $Q \in 2\mathcal{E}_{1,\lambda}(K)$ 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

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

of the hyperbola, we see 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

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

and

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

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

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

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

Lemma 6.2. *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 6.1 to $-\lambda$ (in place of λ) and the curve $\mathcal{E}_{1,-\lambda} = \mathcal{E}_{1,\lambda}$, we see 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

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

Lemmas 6.1 and 6.2 give us the following statement.

Proposition 6.3. *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 $c \neq 0, \pm 1, \pm 1 \pm \sqrt{2}, \pm\sqrt{-1}$ 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 6.4. *The following conditions are equivalent.*

(i) *If $Q \in \mathcal{E}_{1,\lambda}(K)$ is any point with $2Q = W_3$, then Q 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*

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

If these equivalent conditions are fulfilled, 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 5.1) that the 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 6.1 and 6.2.

To finish the proof, we note that $\lambda \neq 0$ and

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

Suppose that

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

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, observe 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

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

This means that

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

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

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

obtaining

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

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

(because $r_2 + r_3 = c$ and $r_2 r_3 = (c^4-1)/4c^2$)).

Now (4) and (7) show that the coordinates of the corresponding R with $2R = Q$ look like this:

$$\begin{aligned}
x(R) &= x(Q) + r_1r_2 + r_2r_3 + r_3r_1 = \frac{(c^2-1)^2}{4c^2} + \frac{(1-c)(c^4-1)}{4c^2} = \frac{(1-c)^3(c+1)}{4c},\\
y(R) &= -(r_1+r_2)(r_2+r_3)(r_1+r_3)\\
&= -\left(-\frac{c-\frac{1}{c}}{2}\cdot\frac{c+\frac{1}{c}}{2} + \frac{c+\frac{1}{c}}{2}\right)c\left(-\frac{c-\frac{1}{c}}{2}\cdot\frac{c+\frac{1}{c}}{2} + \frac{c-\frac{1}{c}}{2}\right)\\
&= -\left(1-\frac{c-\frac{1}{c}}{2}\right)\cdot\frac{c+\frac{1}{c}}{2}\cdot c\cdot\left(1-\frac{c+\frac{1}{c}}{2}\right)\frac{c-\frac{1}{c}}{2}\\
&= -\frac{c^2-\frac{1}{c^2}}{16}\cdot\left(c-2-\frac{1}{c}\right)\left(c-2+\frac{1}{c}\right)c = -\frac{\left(c^2-\frac{1}{c^2}\right)\left((c-2)^2-\frac{1}{c^2}\right)c}{16}.
\end{aligned}$$

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 $c \in K \setminus \{0, \pm1, \pm1 \pm \sqrt{2}, \pm\sqrt{-1}\}$. The group $\mathcal{E}_{4,c}(K)$ contains the subgroup generated by R and W_1, which is isomorphic to $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Theorem 6.5. *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 $c \in K \setminus \{0, \pm1, \pm1 \pm \sqrt{2}, \pm\sqrt{-1}\}$ 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 can 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 6.3. □

Remark 6.6. There is another family of elliptic curves (see [9, Table 3 on p. 217], [11, Appendix E]))

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

with

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

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

Assume that t is an element of an arbitrary field K (with $\mathrm{char}(K) \neq 2$) such that

$$t \neq 0, \quad 8t^2 - 1 \neq 0, \quad 4t + 1 \neq 0$$

and put

$$U(t) := (2t+1)(8t^2+4t+1), \quad A(t) = 2(4t+1)(8t^2-1)t \neq 0, \quad B(t) = (8t^2-1)^2 \neq 0,$$
$$a(t) = \frac{U(t)}{A(t)}, \quad b(t) = \frac{U(t)}{B(t)}.$$

Consider the cubic curve $\mathfrak{E}_{4,t}$ over K defined by the same equation

$$\mathfrak{E}_{4,t} \,:\, y^2 + (1-a(t))xy - b(t)y = x^3 - b(t)x^2$$

as above. By Theorem 6.5, if $\mathfrak{E}_{4,t}$ is an elliptic curve over K, then $\mathfrak{E}_{4,t}$ is isomorphic to $\mathcal{E}_{4,c}$ for some $c \in K$. Let us find the corresponding λ (as a rational function of t). First, we rewrite the equation for $\mathcal{E}_{4,t}$ as

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

i.e.,

$$\left(y + \frac{(1-a(t)x) - b(t)}{2}\right)^2 = x^3 - \frac{U(t)}{B(t)} \cdot x^2 + \left(\frac{\left(1 - \frac{U(t)}{A(t)}\right)x - \frac{U(t)}{B(t)}}{2}\right)^2.$$

Second, multiplying the last equation by $(A(t)B(t))^6$ and introducing the new variables

$$y_1 = (A(t)B(t))^3 \cdot \left(y + \frac{(1-a(t))x - b(t)}{2}\right), \quad x_1 = (A(t)B(t))^2 \cdot x,$$

we obtain (with the help of **magma**) the following equation for an isomorphic cubic curve $\widetilde{\mathfrak{E}}_{4,t}$:

$$\begin{aligned} y_1^2 = x_1^3 &+ \frac{-U(t)A(t)^2B(t) + ((U(t)-A(t))^2B(t)^2}{4}x_1^2 \\ &+ \frac{(U(t)-A(t))U(t)A(t)^3B(t)^3}{2}x_1 + \frac{A(t)^6B(t)^4U(t)^2}{4} \\ &= (x_1-\alpha_1)(x_1-\alpha_2)(x_1-\alpha_3), \end{aligned}$$

where

$$\begin{aligned} \alpha_1 = &-(-4194304t^{15} - 5242880t^{14} - 262144t^{13} + 2162688t^{12} + 753664t^{11} \\ &- 262144t^{10} - 172032t^9 - 2048t^8 + 14336t^7 + 2304t^6 - 320t^5 - 112t^4 - 8t^3), \\ \alpha_2 = &-(4194304t^{16} + 4194304t^{15} - 1048576t^{14} - 2359296t^{13} - 327680t^{12} \\ &+ 491520t^{11} + 163840t^{10} - 40960t^9 - 25600t^8 + 1792t^6 + 192t^5 - 48t^4 - 8t^3), \\ \alpha_3 = &-(-4194304t^{15} - 5242880t^{14} - 262144t^{13} + 2424832t^{12} + 1015808t^{11} \\ &- 294912t^{10} - 286720t^9 - 25600t^8 + 30720t^7 + 8960t^6 - 832t^5 \\ &- 720t^4 - 72t^3 + 16t^2 + 4t + 1/4). \end{aligned}$$

Using **magma**, we obtain

$$\alpha_2 - \alpha_1 = -2^{22}t^4(t+1/2)^4(t^2-1/8)^4, \quad \alpha_3 - \alpha_1 = -2^{18}(t+1/4)^4(t^2-1/8)^4.$$

This implies that $\widetilde{\mathfrak{E}}_{4,t}$ (and, therefore, $\mathfrak{E}_{4,t}$) is an elliptic curve over K (i.e., all three $\alpha_1, \alpha_2, \alpha_3$ are *distinct* elements of K) if and only if

$$t \neq 0, \, -\frac{1}{2}, \, -\frac{1}{4}, \, \pm\frac{1}{2\sqrt{2}}$$

and

$$\frac{\alpha_2-\alpha_1}{\alpha_3-\alpha_1} = \left(\frac{2t(t+1/2)}{t+1/4}\right)^4 \neq 1.$$

Assume that all these inequalities are satisfied. Then the change of variable $x_2 = x_1 + \alpha_1$ transforms $\widetilde{\mathfrak{E}}_{3,t}$ to the elliptic curve

$$\begin{aligned} E\,:\, y_1^2 &= x_2(x_2-(\alpha_2-\alpha_1))(x_2-(\alpha_3-\alpha_1)) \\ &= x_2\left(x_2+2^{22}t^4(t+1/2)^4(t^2-1/8)^4\right)\left(x_2+2^{18}(t+1/4)^4(t^2-1/8)^4\right). \end{aligned}$$

Putting $\kappa = 2^9(t+1/4)^2(t^2-1/8)^2$, we get

$$\kappa^2 = -(\alpha_3-\alpha_1)$$

and E is isomorphic to the elliptic curve

$$E(\kappa)\,:\, {y'}^2 = x'\left(x'+\frac{\alpha_2-\alpha_1}{\alpha_3-\alpha_1}\right)(x'+1) = x'\left(x'+\left(\frac{2t(t+1/2)}{t+1/4}\right)^4\right)(x'+1).$$

Notice that

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

whence $E(\kappa) = \mathcal{E}_{4,c}$ with $c = (4t+1)$. This implies that $\mathfrak{E}_{4,t}$ is isomorphic to $\mathcal{E}_{4,c}$ with $c = (4t+1)$.

Remark 6.7. Suppose that $K = \mathbb{F}_q$ with q equal to $3, 5, 7$, or 9. Then

$$\mathbb{F}_q \setminus \{0, 1, -1, \pm1\pm\sqrt{2}, \pm\sqrt{-1}\} = \varnothing.$$

Corollary 6.8. *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 the elliptic curves $\mathcal{E}_{4,c}$.*

Proof. Suppose that $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$. Theorem 6.5 shows that E is isomorphic to one of the elliptic curves

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

with $c \in K\setminus\{0,\pm1,\pm\sqrt{-1},\pm\sqrt{-1}\}$. Conversely, suppose that E is isomorphic to one of those 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 6.5, $E(\mathbb{F}_q)$ contains a subgroup isomorphic to $\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$; in particular, 16 divides $|E(\mathbb{F}_q)|$. Now, it suffices to check that $|E(\mathbb{F}_q)| < 32$, but this follows from the Hasse bound (10)

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

Corollary 6.9. *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 the 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 $\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$. From Theorem 6.5 it follows that E is isomorphic to one of the elliptic curves

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

with $c \in K\setminus\{0,\pm1,\pm1\pm\sqrt{2},\pm\sqrt{-1}\}$.

Conversely, suppose that E is isomorphic to one of those 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 6.5, $E(\mathbb{F}_{47})$ contains a subgroup isomorphic to $\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$; in particular, 16 divides $|E(\mathbb{F}_{47})|$. By the Hasse bound, we have

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

whence $34<|E(\mathbb{F}_{47})|<62$. 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 entire group $E(\mathbb{F}_{47})$, we get the desired result. □

Theorem 6.10. *Let $K=\mathbb{Q}$, and let E be an elliptic curve over $\mathbb{Q}$. Then the torsion subgroup $E(\mathbb{Q})_t$ of $E(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ if and only if there exists $c\in\mathbb{Q}\setminus\{0,\pm1\}$ such that E is isomorphic to $\mathcal{E}_{4,c}$.*

Proof. By Theorem 4.2 applied to $m=4$, if $E(\mathbb{Q})$ contains a subgroup isomorphic to $\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$, then $E(\mathbb{Q})_t$ is isomorphic to $\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$. Now the desired result follows from Theorem 6.5, because neither $\sqrt{2}$ nor $\sqrt{-1}$ lies in $\mathbb{Q}$. □

Theorem 6.11. *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*

$$c,d\in K\setminus\{0,\pm1,\pm1\pm\sqrt{2},\pm\sqrt{-1}\}\quad \textit{such that}\quad c-\frac{1}{c}=\mathbf{i}\left(d-\frac{1}{d}\right)$$

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

Remark 6.12. The above equation and inequalities determine a dense open 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 $\bar{\mathcal{M}}_{8,4}$, first we slightly simplify equation(11) by the change of variables $d=s,\mathbf{i}c=t$, getting $s^2t+ts^2+s-t=0$. Then, using the birational transformation

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

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

Proof of Theorem 6.11. We have already seen that $\mathcal{E}_{4,c}(K)$ contains an order 8 point R with $4R=W_3$. From Proposition 6.4 it follows 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 can 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 6.5 allow us to assume that

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

[3]See [16, Example 1.4.2 on p. 88] for an explicit description of the (finite) set of all $\mathbb{Q}(\mathbf{i})$-points on this elliptic curve; none of them corresponds to the (c,d) that satisfy the conditions of Theorem 6.11.

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 $\mathcal{E}_{1,\lambda}(K)$. Proposition 6.3 shows 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

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

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 relation

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

§7. Points of order 3

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

Proposition 7.1. *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 $P \in E(K)$, we have

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

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., $Q = -P, 2(-P) = P$, whence P has order 3. $\square$

Theorem 7.2. *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. 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 and its K-point $P = (0, a_1 a_2 a_3)$. 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,*

$$(a_2 a_3 - a_1 a_2 - a_3 a_1, (a_1 - a_2)(a_2 + a_3)(a_3 - a_1)),$$
$$(a_3 a_1 - a_1 a_2 - a_2 a_3, (a_1 - a_2)(a_2 - a_3)(a_3 + a_1)),$$
$$(a_1 a_2 - a_2 a_3 - a_3 a_1, (a_1 + a_2)(a_2 - a_3)(a_3 - a_1)),$$
$$(a_1 a_2 + a_2 a_3 + a_3 a_1, (a_1 + a_2)(a_2 + a_3)(a_3 + a_1)).$$

(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 relations is fulfilled*:

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

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

Remark 7.3. Clearly, $E_{a_1,a_2,a_3} = E_{\pm a_1,\pm a_2,\pm a_3}$.

Proof of Theorem 7.2. We have

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

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

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

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 $r_i = \pm a_i$ in 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).

We 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 the a_i vanishes. Proposition 7.1 allows us to choose the signs for r_i in such a way that $r_1r_2 + r_2r_3 + r_3r_1 = 0$. Plugging $r_i = \pm a_i$ in this formula, we get four relations between a_1, a_2, a_3 as in (ii), (2).

Now suppose that one of relations as in (ii), (2) is fulfilled. This means that the signs of $r_i = \pm a_i$ can be chosen in such a way that $r_1r_2 + r_2r_3 + r_3r_1 = 0$. From Proposition 7.1 it follows that P has order 3. This proves (ii).

Now we prove (iii). Since P has order 3, we have $2(-P) = P$, 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 $P = 2Q = -Q$, whence $Q = -P$, which is not the case. Hence, Q has order 6. Then $3Q$ has order 2, i.e., $3Q$ 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 7.4. In Theorem 7.2 we do *not* assume that $\mathrm{char}(K) \neq 3$!

Corollary 7.5. *Let a_1, a_2, a_3 be elements of K such that a_1^2, a_2^2, a_3^2 are distinct. 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 the a_i vanishes, and the signs for*

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

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

If these conditions are satisfied, 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 condition (ii) of the corollary is fulfilled, i.e., none of the a_i vanishes, and the signs for

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

can be chosen in such a way that $c = ab/(a+b)$. Then none of a, b, c vanishes and $ab = ac + bc$. By Theorem 7.2(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 $abc = \pm a_1 a_2 a_3$, either $\mathcal{P} = P$, or $\mathcal{P} = -P$. In both cases P has order 3.

Observe 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

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

are six distinct elements of K. This means (since $a \neq 0, b \neq 0$) that

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

Suppose P has order 3. By Theorem 7.2(ii), none of the a_i vanishes and one of the following four identities is true:

$$a_2 a_3 = a_1 a_2 + a_3 a_1, \quad a_3 a_1 = a_1 a_2 + a_2 a_3,$$
$$a_1 a_2 = a_2 a_3 + a_3 a_1, \quad a_1 a_2 + a_2 a_3 + a_3 a_1 = 0.$$

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

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

To finish the proof, now we only need to note that $a = \lambda b$ and

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

Theorem 7.6. *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*

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

Proof of Theorem 7.6. 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, $a_1 a_2 = a_2 a_3 + a_3 a_1$, and $\mathcal{E}_{3,\lambda} = E_{a_1,a_2,a_3}$. Referring to Theorem 7.2, we see 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 $E(K)$, so that 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 2.1, 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, we have

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

whence $y(P) = \pm a_1 a_2 a_3$. Replacing P by $-P$ if necessary, we may assume that $y(P) = a_1 a_2 a_3$, i.e., $P = (0, a_1 a_2 a_3)$ is a K-point of order 3 on

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

By Corollary 7.5, there exists *a nonzero element* $b \in K$ 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

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

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

Remark 7.7. There is a family of elliptic curves over $\mathbb{Q}$ (see [9, Table 3 on p. 217] and also [11, Appendix E]),

$$\mathfrak{E}_{3,t} \,:\, y^2 + (1 - a(t))xy - b(t)y = x^3 - b(t)x^2,$$

where

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

and $t \in \mathbb{Q} \setminus \{1, 5, \pm 3, 9\}$, whose group of rational points contains a subgroup isomorphic to $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. (The point $(0,0)$ of $\mathfrak{E}_{3,t}$ has order 6, *ibid.*) Assume that $t \neq \pm 3$ is an element of an arbitrary field K (with $\mathrm{char}(K) \neq 2$) and consider the cubic curve $\mathfrak{E}_{3,t}$ over K defined by the same equation as above.

By Theorem 7.6, if $\mathfrak{E}_{3,t}$ is an elliptic curve over K, then $\mathfrak{E}_{3,t}$ is isomorphic to $\mathcal{E}_{3,\lambda}$ for some $\lambda \in K$. Let us find the corresponding λ (as a rational function of t). First, rewrite the equation for $\mathcal{E}_{3,\lambda}$ as

$$\left(y + \frac{(1 - a(t)x) - b(t)}{2}\right)^2 = x^3 - b(t)x^2 + \left(\frac{(1 - a(t))x - b(t)}{2}\right)^2.$$

Second, multiplying the last equation by $(t^2 - 9)^6$ and introducing the new variables

$$y_1 = (t^2 - 9)^3 \cdot \left(y + \frac{(1 - a(t))x - b(t)}{2}\right), \quad x_1 = (t^2 - 9)^2 \cdot x,$$

we obtain (with the help of **magma**) an equation for an isomorphic cubic curve

$$\widetilde{\mathfrak{E}}_{3,t} \,:\, y_1^2 = (x_1 - \alpha_1)(x_1 - \alpha_2)(x_1 - \alpha_3),$$

where

$$\alpha_1 = -(2t^3 - 10t^2 - 18t + 90) = -2(t-5)(t-3)(t+3),$$
$$\alpha_2 = -(2t^3 - 10t^2 + 14t - 6) = -2(t-3)(t-1)^2,$$
$$\alpha_3 = -\left(\frac{1}{4}t^4 - t^3 - \frac{5}{2}t^2 + 7t - \frac{15}{4}\right) = -\frac{1}{4}(t-5)(t+3)(t-1)^2.$$

We have

$$\alpha_1 - \alpha_2 = -2^5(t-3), \quad \alpha_2 - \alpha_3 = \frac{1}{4} \cdot (t-1)^3(t-9), \quad \alpha_3 - \alpha_1 = -\frac{1}{4} \cdot (t-5)^3(t+3).$$

This implies that $\widetilde{\mathfrak{E}}_{3,t}$ (and, therefore, $\mathfrak{E}_{3,t}$) is an elliptic curve over K if and only if

$$t \in K \setminus \{1, \pm 3, 5, 9\}.$$

Next, assume that this condition is fulfilled, so that $\widetilde{\mathfrak{E}}_{3,t}$ and $\mathfrak{E}_{3,t}$ are elliptic curves over K. Clearly, all three points of order 2 on $\widetilde{\mathfrak{E}}_{3,t}$ are defined over K, and the K-point

$$Q = (x_1(Q), y_1(Q)) = (0, -(t-5)(t-3)(t+3)(t-1)^2)$$

lies on $\widetilde{\mathfrak{E}}_{3,t}$. We prove that Q has order 6. Consider the point $P = 2Q \in E(K)$ with coordinates $x_1(P), y_1(P) \in K$. (Since $y_1(P) \neq 0$, we have $P \neq \infty$.) In accordance with the formulas of §1, there exists a unique triple r_1, r_2, r_3 of distinct elements of K such that

$$(r_1 + r_2)(r_2 + r_3)(r_3 + r_1) = -y_1(Q) = (t-5)(t-3)(t+3)(t-1)^2$$

and, for all $i = 1, 2, 3$,

$$x_1(P) - \alpha_i = r_i^2,$$
$$0 \neq -\alpha_i = x_1(Q) - \alpha_i = (r_i + r_j)(r_i + r_k),$$

where (i, j, k) is a permutation of $(1, 2, 3)$. This implies that

$$\begin{aligned}
r_1 + r_2 &= \frac{(t-5)(t-3)(t+3)(t-1)^2}{-a_3} = \frac{(t-5)(t-3)(t+3)(t-1)^2}{\frac{1}{4}(t-5)(t+3)(t-1)^2} = 4(t-3),\\
r_2 + r_3 &= \frac{(t-5)(t-3)(t+3)(t-1)^2}{-a_1} = \frac{(t-5)(t-3)(t+3)(t-1)^2}{2(t-5)(t-3)(t+3)} = \frac{1}{2} \cdot (t-1)^2,\\
r_3 + r_1 &= \frac{(t-5)(t-3)(t+3)(t-1)^2}{-a_2} = \frac{(t-5)(t-3)(t+3)(t-1)^2}{2(t-3)(t-1)^2}\\
&= \frac{1}{2} \cdot (t-5)(t+3).
\end{aligned}$$

Consequently,

$$r_1 + r_2 = 4(t-3), \quad r_2 + r_3 = \frac{(t-1)^2}{2}, \quad r_3 + r_1 = \frac{(t+3)(t-5)}{2},$$

whence

$$r_1 + r_2 + r_3 = \frac{1}{2} \cdot ((r_1 + r_2) + (r_2 + r_3) + (r_3 + r_1)) = \frac{1}{2} \cdot (t^2 + 2t - 19),$$

which, in turn, implies that

$$r_1 = 2t - 10 = 2(t-5), \quad r_2 = 2t - 2 = 2(t-1), \quad r_3 = \frac{1}{2} \cdot (t-1)(t-5) = \frac{1}{8} r_1 r_2.$$

It is easy to check that

$$c(t) := -2t^3 + 14t^2 - 22t + 10 = r_i^2 + \alpha_i \quad \text{for all} \quad i = 1, 2, 3.$$

This implies that

$$x_1(P) = c(t), \quad c(t) - \alpha_i = r_i^2 \quad \text{for all} \quad i = 1, 2, 3,$$

and $\widetilde{\mathfrak{E}}_{3,t}$ is isomorphic to the elliptic curve

$$E_{r_1, r_2, r_3} : y_1^2 = (x_2 + r_1^2)(x_2 + r_2^2)(x_3 + r_3^2)$$

with $x_2 = x_1 - c(t)$. Moreover,

$$y_1(P) = -r_1 r_2 r_3 = -2(t-1)^2(t-5).$$

We have

$$r_1 r_2 = 8 r_3, \quad r_2 - r_1 = 8.$$

This implies $(r_2 - r_1)r_3 = r_1 r_2$, which means that

$$(-r_1)r_2 + r_2 r_3 + (-r_1)r_3 = 0.$$

Proposition 7.1 shows that P has order 3 in $\widetilde{\mathfrak{E}}_{3,t}(K)$. (In particular, all $r_i \neq 0$.) Since $2Q = P$, the order of Q in $\widetilde{\mathfrak{E}}_{3,t}$ is 6.

Observe that

$$-r_3 = \frac{(-r_1)r_2}{(-r_1) + r_2}$$

and

$$E_{r_1,r_2,r_3} = E_{-r_1,r_2,-r_3}.$$

From Corollary 7.5 and the end of the proof of Theorem 7.6 it follows that E_{r_1,r_2,r_3} is isomorphic to $\mathcal{E}_{3,\lambda}$ with

$$\lambda = \frac{-r_1}{r_2} = \frac{-(2t-10)}{2t-2} = -\frac{t-5}{t-1}.$$

This implies that $\mathfrak{E}_{3,t}$ is isomorphic to $\mathcal{E}_{3,\lambda}$ with $\lambda = -(t-5)/(t-1)$.

Corollary 7.8. *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 the 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 7.6, E is isomorphic to one of the elliptic curves $\mathcal{E}_{3,\lambda}$.

Conversely, suppose that E is isomorphic to one of those 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 7.6, $E(\mathbb{F}_q)$ contains a subgroup isomorphic to $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$; in particular, 12 divides $|E(\mathbb{F}_q)|$. Now, it suffices to check that $|E(\mathbb{F}_q)| < 24$, but this follows from the Hasse bound (10)

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

Corollary 7.9. *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 the 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 $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. By Theorem 7.6, E is isomorphic to one of the elliptic curves $\mathcal{E}_{3,\lambda}$.

Conversely, suppose that E is isomorphic to one of those 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 7.6, $E(\mathbb{F}_{23})$ 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) shows that

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

whence $14 < |E(\mathbb{F}_{23})| < 34$. 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 $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Since $E(\mathbb{F}_{23})$ 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 entire group $E(\mathbb{F}_{23})$, which finishes the proof. $\square$

Theorem 7.10. *Let $K = \mathbb{Q}$, and let E be an elliptic curve over $\mathbb{Q}$. Then the torsion subgroup $E(\mathbb{Q})_t$ of $E(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ if and only if there exists $\lambda \in \mathbb{Q} \setminus \{0, \pm 1, -2, -\frac{1}{2}\}$ such that E is isomorphic to $\mathcal{E}_{3,\lambda}$.*

Proof. By Theorem 4.2 applied to $m = 3$, if $E(\mathbb{Q})$ contains a subgroup isomorphic to $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, then $E(\mathbb{Q})_t$ is isomorphic to $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Now the desired result follows from Theorem 7.6. □

§8. Points of order 5

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

Proposition 8.1. *Let $P = (x_0, y_0) \in E(K)$. The point P has order 5 if and only if the square roots $r_i = \sqrt{x_0 - \alpha_i}$ and $r_i^{(1)} = \sqrt{(r_i + r_j)(r_i + r_k)}$, where i, j, k is a permutation of $1, 2, 3$, can be chosen in such a way that*

$$(r_1r_2 + r_2r_3 + r_3r_1) + \left(r_1^{(1)}r_2^{(1)} + r_2^{(1)}r_3^{(1)} + r_3^{(1)}r_1^{(1)}\right) = 0, \qquad r_1r_2 + r_2r_3 + r_3r_1 \neq 0. \tag{12}$$

Remark 8.2. Observe 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 formulas (9), then we obtain all points R for which $4R = \pm P$.

Proof of Proposition 8.1. Suppose that P has order 5. Then $-P$ is a 1/4th of P. Therefore, there exist r_i and $r_i^{(1)}$ such that

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

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

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

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

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

whence $Q = P$ 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 contradiction obtained proves that $r_1r_2 + r_2r_3 + r_3r_1 \neq 0$.

Conversely, suppose there exist square roots

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

that satisfy (12). Replacing if necessary all r_i by $-r_i$, we may and shall 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

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

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 $P = 2Q = -Q$, whence $P = -Q$, 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. □

Below, we use the following identities in the polynomial ring $\mathbb{Z}[t_1, t_2, t_3]$, which can be checked either directly, or by using **magma**:

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

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

Theorem 8.3. *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*

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

vanishes. Then the following conditions are satisfied.

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

(ii) *Consider the 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*

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

Then P has order 5. Moreover, $E_{5;a_1,a_2,a_3}(K)$ 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 the a_i vanishes. Let $i, j \in \{1, 2, 3\}$ be two distinct indices and $k \in \{1, 2, 3\}$ the third index. Then

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

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

(ii) Keeping our notation, we obtain

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

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

where i, j, k is any permutation of $1, 2, 3$. By Proposition 8.1, it suffices to check that the square roots r_i and $r_i^{(1)}$ can be chosen in such a way that $r_1r_2 + r_2r_3 + r_3r_1 \neq 0$ and

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

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
$$r_1^{(1)} = a_2a_3, \quad r_2^{(1)} = a_1a_3, \quad r_3^{(1)} = a_1a_2.$$
Then condition (16) can be rewritten as follows:
$$(-a_1^2+a_2^2+a_3^2)(a_1^2-a_2^2+a_3^2)+(a_1^2-a_2^2+a_3^2)(a_1^2+a_2^2-a_3^2) \\ +(a_1^2+a_2^2-a_3^2)(-a_1^2+a_2^2+a_3^2)+4a_1^2a_2a_3+4a_1a_2^2a_3+4a_1a_2a_3^2=0.$$
By (14), 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 last identity follows readily from the assumption (15) of Theorem. By Proposition 8.1, now it suffices to check that $r_1r_2+r_2r_3+r_3r_1 \neq 0$. In other words, we need to prove that
$$(-a_1^2+a_2^2+a_3^2)(a_1^2-a_2^2+a_3^2)+(a_1^2-a_2^2+a_3^2)(a_1^2+a_2^2-a_3^2) \\ +(a_1^2+a_2^2-a_3^2)(-a_1^2+a_2^2+a_3^2) \neq 0. \tag{17}$$
By (13), this inequality 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 last inequality holds true by the assumption (15) of the theorem. Hence, P has order 5. Clearly, P and all points of order 2 generate a subgroup isomorphic to $\mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. □

Theorem 8.4. *Let E be an elliptic curve over K. 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* 8.3, *including* (15), *and such that E is isomorphic to $E_{5;a_1,a_2,a_3}$.*

Proof. Statement (i) follows from (ii), thanks to Theorem 8.3.

Suppose (i) is true. 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 $r_i^{(1)} = \sqrt{(r_i + r_j)(r_i + r_k)} \in K$ such that
$$x(-P) = x(P) + (r_1r_2 + r_2r_3 + r_3r_1) + \big(r_1^{(1)}r_2^{(1)} + r_2^{(1)}r_3^{(1)} + r_3^{(1)}r_1^{(1)}\big),$$
$$r_1^{(1)}r_2^{(1)}r_3^{(1)} = (r_1+r_2)(r_2+r_3)(r_3+r_1).$$
Since $x(-P) = x(P) = 0$, we have
$$(r_1r_2 + r_2r_3 + r_3r_1) + \big(r_1^{(1)}r_2^{(1)} + r_2^{(1)}r_3^{(1)} + r_3^{(1)}r_1^{(1)}\big) = 0. \tag{18}$$
Since the order of P is *not* 3, it follows that
$$r_1r_2 + r_2r_3 + r_3r_1 \neq 0. \tag{19}$$
Recall that none of $r_i + r_j$ vanishes. Let the square roots
$$b_1 = \sqrt{r_2+r_3}, \quad b_2 = \sqrt{r_1+r_3}, \quad b_3 = \sqrt{r_1+r_2}$$
be chosen 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

$$r_3^{(1)} = \frac{r_1^{(1)} r_2^{(1)} r_3^{(1)}}{r_2^{(1)} r_3^{(1)}} = \frac{(b_1 b_2 b_3)^2}{(b_2 b_3)(b_3 b_1)} = b_1 b_2.$$

We obtain

$$r_1^{(1)} = b_2 b_3, \quad r_2^{(1)} = b_3 b_1, \quad r_3^{(1)} = b_1 b_2. \tag{20}$$

Unfortunately, b_i may fail to lie in K. However, all the ratios b_i/b_j lie in K^*. We have

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

whence

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

Since none of the r_i vanishes, we get

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

Put

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

Theorem 8.3(i) shows that all β_i are *distinct* nonzero elements of K. Inequality (19) combined with the first formula in (21) yields

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

which is equivalent (by (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,

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

Identity (18) (with the help of (14)) yields

$$(b_1 + b_2 + b_3)(b_1^3 + b_2^3 + b_3^3 - b_1^2 b_2 - b_1 b_2^2 - a_2^2 b_3 - b_2 b_3^2 - b_1^2 b_3 - b_1 b_3^2 - 2 b_1 b_2 b_3) = 0,$$

i.e.,

$$b_1^3 + b_2^3 + b_3^3 - b_1^2 b_2 - b_1 b_2^2 - a_2^2 b_3 - b_2 b_3^2 - b_1^2 b_3 - b_1 b_3^2 - 2 b_1 b_2 b_3 = 0.$$

Put

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

All a_i lie in K. Clearly, the triple $\{a_1, a_2, a_3\}$ satisfies all the conditions of Theorem 8.3, including (15). Let

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

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

$$\begin{aligned} E(r_1+r_2): {y'}^2 &= \left(x' + \frac{\gamma_1^2}{4(r_1+r_2)^2}\right)\left(x' + \frac{\gamma_2^2}{4(r_1+r_2)^2}\right)\left(x' + \frac{\gamma_3^2}{4(r_1+r_2)^2}\right) \\ &= \left(x' + \frac{\beta_1^2}{4}\right)\left(x' + \frac{\beta_2^2}{4}\right)\left(x' + \frac{\beta_3^2}{4}\right). \end{aligned}$$

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

Remark 8.5. Suppose that $E_{5;a_1,a_2,a_3}$ is as in Theorem 8.3. Clearly, $E_{5;a_1,a_2,a_3}(a_3) = E_{5;a_1/a_3,a_2/a_3,1}$. Putting $\lambda = a_1/a_3, \mu = a_2/a_3$, we have

$$E_{5;a_1/a_3,a_2/a_3,1} = E_{5;\lambda,\mu,1}:$$

$$y^2 = \left[x + \left(\frac{-\lambda^2+\mu^2+1}{2}\right)^2\right]\left[x + \left(\frac{\lambda^2-\mu^2+1}{2}\right)^2\right]\left[x + \left(\frac{\lambda^2+\mu^2-1}{2}\right)^2\right]. \tag{22}$$

The equation of the curve $E_{5;\lambda,\mu,1}(\frac{\lambda^2+\mu^2-1}{2})$, isomorphic to $E_{5;\lambda,\mu,1}$, looks like this:
(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 can be rewritten in terms of λ, μ as follows:

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

Identity (24) is equivalent to

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

Multiplying (25) by the (nonvanishing) number $\lambda+\mu$, we get the equivalent equation

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

The change of variables

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

transforms (26) to

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

which is an (affine model of an) elliptic curve whenever $\mathrm{char}(K)\neq5$, 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 (27) are the inequalities

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

i.e.,

$$\xi\neq0,\ \pm1,\ \frac{-1\pm\sqrt5}{2}. \tag{29}$$

This means that

$$(\xi,\eta)\notin\left\{(0,0),(\pm1,\pm1),\left(\frac{-1\pm\sqrt5}{2},0\right)\right\}. \tag{30}$$

Using (28), we can rewrite equation (22) with coefficients that are rational functions in ξ, η (rather than (λ, μ)) as follows.

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

Theorem 8.6. *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 $(\xi, \eta) \in K^2$ satisfying* (27) *and* (30) *and such that E is isomorphic to $\mathcal{E}_{5,\xi,\eta}$.*

Proof. This follows from Theorem 8.4 combined with Remark 8.5. □

Remark 8.7. In Theorem 8.6 it is *not* assumed that $\mathrm{char}(K) \neq 5$!

Corollary 8.8. *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 8.6, E is isomorphic to one of the elliptic curves $\mathcal{E}_{5,\xi,\eta}$.

Conversely, suppose that E is isomorphic to one of those 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 8.6, $E(\mathbb{F}_q)$ contains a subgroup isomorphic to $\mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$; in particular, 20 divides $|E(\mathbb{F}_q)|$. Now, it suffices to check that $|E(\mathbb{F}_q)| < 40$, but this follows from the Hasse bound (10)

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

Corollary 8.9. *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 the curves $\mathcal{E}_{5,\xi,\eta}$.*

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 8.6, E is isomorphic to one of the 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 8.6, $E(\mathbb{F}_q)$ contains a subgroup isomorphic to $\mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$; in particular, 20 divides $|E(\mathbb{F}_q)|$. The Hasse bound (10) yields

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

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 the order 8 Abelian group $E(\mathbb{F}_q)(2)$; moreover, 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 $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Consequently, $E(\mathbb{F}_q)$ is isomorphic to the direct sum

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

Corollary 8.10. *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 the curves $\mathcal{E}_{5,\xi,\eta}$.*

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 8.6, E is isomorphic to one of the elliptic curves $\mathcal{E}_{5,\xi,\eta}$.

Conversely, suppose that E is isomorphic to one of those 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 8.6, $E(\mathbb{F}_q)$ contains a subgroup isomorphic to $\mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$; in particular, 20 divides $|E(\mathbb{F}_q)|$. The Hasse bound (10) yields

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

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

Theorem 8.11. *Let K be a quadratic field, and let E be an elliptic curve over K. Then the following conditions are equivalent*:

(i) *the torsion subgroup $E(K)_t$ of $E(K)$ is isomorphic to $\mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$*;

(ii) *there exist $(\xi, \eta) \in K^2$ satisfying* (27) *and* (30) *and such that E is isomorphic to $\mathcal{E}_{5,\xi,\eta}$*.

Proof. By Theorem 4.3, if $E(K)$ contains a subgroup isomorphic to $\mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, then $E(K)_t$ is isomorphic to $\mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Now the desired result follows from Theorem 8.6. $\square$

Acknowledgments

We are grateful to Robin Chapman for helpful comments and to Oksana Podkopaeva for help with calculations. Our special thanks go to Tatiana Bandman for help with **magma**.

References

[1] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006. MR2216774

[2] J. P. Buhler, *Elliptic curves, modular forms, and applications*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, pp. 5–81. MR1860040

[3] J. W. S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966), 193–291. MR0199150

[4] D. Husemöller, *Elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 111, Springer-Verlag, New York, 2004. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen. MR2024529

[5] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221–229. MR1172689

[6] S. Kamienny and F. Najman, *Torsion groups of elliptic curves over quadratic fields*, Acta Arith. **152** (2012), no. 3, 291–305. MR2885789

[7] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149. MR931956

[8] A. W. Knapp, *Elliptic curves*, Mathematical Notes, vol. 40, Princeton University Press, Princeton, NJ, 1992. MR1193029

[9] D. S. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) **33** (1976), no. 2, 193–237. MR0434947

[10] S. Lang, *Elliptic curves: Diophantine analysis*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 231, Springer-Verlag, Berlin-New York, 1978. MR518817

[11] Á. Lozano-Robledo, *Elliptic curves, modular forms, and their L-functions*, Student Mathematical Library, vol. 58, American Mathematical Society, Providence, RI; Institute for Advanced Study (IAS), Princeton, NJ, 2011. IAS/Park City Mathematical Subseries. MR2757255

[12] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186 (1978). MR488287

[13] E. F. Schaefer, 2-*descent on the Jacobians of hyperelliptic curves*, J. Number Theory **51** (1995), no. 2, 219–232. MR1326746

[14] N. Schappacher and R. Schoof, *Beppo Levi and the arithmetic of elliptic curves*, Math. Intelligencer **18** (1996), no. 1, 57–69. MR1381581

[15] A. Silverberg, *Explicit families of elliptic curves with prescribed mod N representations*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 447–461. MR1638488

[16] A. Silverberg, *Open questions in arithmetic algebraic geometry*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, pp. 83–142. MR1860041

[17] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094

[18] J. H. Silverman and J. T. Tate, *Rational points on elliptic curves*, 2nd ed., Undergraduate Texts in Mathematics, Springer, Cham, 2015. MR3363545

[19] 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. MR0316454

[20] J. Tate, *Algebraic formulas in arbitrary characteristic*, Appendix 1, S. Lang, Elliptic functions, Second ed., Springer-Verlag, New York, 1987, pp. 299–306. MR0890960 (88c:11028)

[21] L. C. Washington, *Elliptic curves. Number theory and cryptography*, 2nd ed., Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2008. MR2404461

[22] J. Yelton, *Dyadic torsion of elliptic curves*, Eur. J. Math. **1** (2015), no. 4, 704–716. MR3426175

Department of Mathematics and Mechanics, St. Petersburg State University, Universitetsky prospekt 28, Peterhof, St. Petersburg 198504, Russia
Email address: `bekker.boris@gmail.com`

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA
Email address: `zarhin@math.psu.edu`

Received 15/MAY/2016

Translated by B. M. BEKKER