For results concerning the possibilities for the torsion subgroup over a fixed quadratic field see [318, 401]. Similarly to Mazur's theorem, here also each of these 26 groups appears as the torsion group over a quadratic field for infinitely many non-isomorphic elliptic curves. With cubic fields, the situation is different. Namely, Najman [321] proved that there is a unique curve with torsion group $\mathbb{Z}/21\mathbb{Z}$ over a cubic field. Let us mention that for each of the 26 groups from (15.43), there is an elliptic curve over a quadratic field with that torsion group and positive rank, and for all groups except $\mathbb{Z}/15\mathbb{Z}$ also with the rank ≥ 2 (see [8, 56, 320]).

15.11 Exercises

1. Let $P=(-1,2)$ and $Q=(1,-2)$ be points on the elliptic curve over $\mathbb{Q}$ given by the equation $y^2=x^3-x+4$. Determine points $P+Q$, $P-Q$, $2P$ and $2Q$ on that curve.

2. Write the elliptic curve over $\mathbb{Q}$ given by the equation

$$y^2+xy+y=x^3-x^2-5x$$

   in the short Weierstrass form.

3. Write the elliptic curve over $\mathbb{Q}$ given by the equation

$$x^3+y^3+x^2+x+1=0$$

   in the short Weierstrass form.

4. Show that the curve

$$y^2=x^3+4x^2-3x-18$$

   is singular. Determine its singular point and its rational parametrization.

5. Determine the j-invariant of the elliptic curve

$$y^2+xy+y=x^3-x^2-2.$$

6. The elliptic curve over $\mathbb{Q}$ is given by the equation

$$E:\ y^2=x^3+1875x+156250.$$

   Determine its minimal Weierstrass equation.

7. What kind of reduction (good or bad, additive or multiplicative, split or non-split) does the curve

$$E : y^2 = x^3 + 1875x + 156250$$

have for $p = 13$?

8. Let E be the elliptic curve with the equation

$$y^2 = x^3 + ax + b.$$

Let $P = (x_1, y_1)$ be a point on E, and let $2P = (x_2, y_2)$. Prove that

$$y_1^2(4x_2(3x_1^2 + 4a) - 3x_1^3 + 5ax_1 + 27b) = 4a^3 + 27b^2.$$

9. Show by an example that an elliptic curve with the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$, can have a point of finite order whose coordinates are not integers.

10. Find all points of finite order and determine the structure of the torsion group for the elliptic curve

$$y^2 = x^3 - 192240x + 32605200.$$

11. Find all points of finite order and determine the structure of the torsion group for the following elliptic curves:

a) $y^2 = x^3 + 3x + 7$,
b) $y^2 = x^3 - 19x + 30$,
c) $y^2 = x^3 - 219x + 1654$,
d) $y^2 = x^3 - 12987x - 263466$,
e) $y^2 = x^3 - 1386747x + 368636886$.

Show that in each of these examples, there are prime numbers p_1, p_2, such that $p_i \nmid 2\Delta$, for which

$$|E(\mathbb{Q})_{\text{tors}}| = \gcd(|E(\mathbb{F}_{p_1})|, |E(\mathbb{F}_{p_2})|).$$

12. Find a rational number t such that for the elliptic curve

$$E\ :\ y^2 = x(x+t)(x+t+6),$$

we have $E(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

13. A family of elliptic curves is given by

$$E_t\ :\ y^2 = x(x+t)(x+t+27).$$

Find rational numbers t_1, t_2 such that $E_{t_1}(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $E_{t_2}(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

14. Let $P \in E(\mathbb{Q})$ be a point such that $\langle P, Q\rangle = 0$ for each $Q \in E(\mathbb{Q})$. Prove that P is a torsion point.

15. Find all integer points $P = (x, y)$ on the curve

$$E\ :\ y^2 = x^3 - x^2 - 3225667994796x + 2205916672708538820,$$

such that $|x| < 10000000$. Among those points, find as large as possible set of points which are independent modulo $E(\mathbb{Q})_{\text{tors}}$, i.e. find the best possible lower bound for the rank of E.

16. Calculate the rank of the elliptic curve over $\mathbb{Q}$ given by the equation

$$y^2 = x^3 - 46x.$$

17. For the polynomial

$$p(x) = (x-4)(x-3)(x-2)(x-1)x(x+1)(x+2)(x+5),$$

determine polynomials $q(x), r(x) \in \mathbb{Q}[x]$ such that $p(x) = (q(x))^2 - r(x)$ and $\deg r \leq 3$.

18. Calculate Mazur's bound M_3 for the rank of the elliptic curve

$$E\ :\ y^2 + xy + y = x^3 - 4213613959455x + 3328416232976793662$$

with the torsion group $\mathbb{Z}/3\mathbb{Z}$.

19. Given is a point $P = (0, 2)$ on the elliptic curve $y^2 = x^3 + 2x + 4$ over the field $\mathbb{F}_{211}$. Determine the NAF representation of 110. Calculate $110P$.

20. Find an elliptic curve E over $\mathbb{F}_{17}$ such that the order of the group $E(\mathbb{F}_{17})$ is equal to 24.

21. For each of the numbers $n = 2, 3, 4, 5, 6, 7, 8, 9, 10$, find an elliptic curve E_n over $\mathbb{F}_5$ such that the order of the group $E_n(\mathbb{F}_5)$ is equal to n.

22. The elliptic curve is given by

$$E : \ y^2 = x^3 + x + 4$$

over the field $\mathbb{F}_{191}$. Determine the order of the group $E(\mathbb{F}_{191})$ by the Shanks-Mestre method using the point $P = (36, 61)$.

23. Find one anomalous and one supersingular elliptic curve over $\mathbb{F}_{23}$.

24. An elliptic curve E over the field $\mathbb{F}_{13}$ is given by the equation $y^2 = x^3 + 7x + 3$. Prove that $\alpha = (0, 4)$ is a generator of the group $E(\mathbb{F}_{13})$.

25. By using the Menezes-Vanstone cryptosystem in which the public key consists of the elliptic curve E and the generator α from the previous exercise and $\beta = (2, 8)$, encrypt the plaintext $(x_1, x_2) = (5, 11)$, with the assumption that the ephemeral key is $k = 5$.

26. The elliptic curve E over the field $\mathbb{F}_{17}$ is given by the equation $y^2 = x^3 + 5x + 2$. For the points $P = (10, 7)$ and $Q = (4, 16)$ on E, solve the elliptic curve discrete logarithm problem $Q = [m]P$ by the Pohlig-Hellman algorithm if it is known that the point P is of order 15.

27. By applying Pocklington's theorem, prove that the number $1\,048\,583$ is prime.

28. Let E be an elliptic curve over the field $\mathbb{F}_p$, where $p \equiv 3 \pmod 4$ is a prime number, given by the equation $y^2 = x^3 + x$. Determine the order of the group $E(\mathbb{F}_p)$.

29. Factorize the number $n = 403$ by using the ECM with the parameters

$$E : \quad y^2 = x^3 + 16x + 1,$$

$P = (0, 1)$ and $B = 3$.