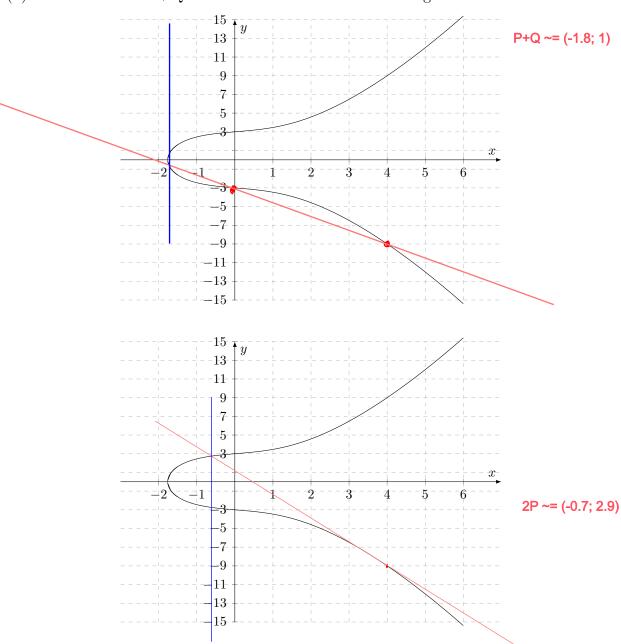
KRY: Wahlfach Kryptologie Serie 11: Diskrete Logarithmen, elliptische Kurven

Aufgabe 1 (T)

Elliptische Kurven Wir betrachten den Körper $K = \mathbb{R}$ der reellen Zahlen. Untenstehend ist die elliptische Kurve $E: y^2 = x^3 + 2x + 9$ je einmal abgebildet. Die Punkte P(4; -9) und Q(0; -3) liegen auf der Kurve.

- (a) Bestimmen Sie zeichnerisch die ungefähren Werte von P+Q und 2P.
- (b) Bestimmen Sie P+Q und 2P exakt mithilfe der Rechengesetze.



1.b) Kurve E :
$$y^2 = x^3 + 2x + 9 / P(4; -9) / Q(0; -3)$$

 $a=2$
 $b=9$
 $x1=4$
 $x2=0$
 $y1=-9$
 $y2=-3$

Falls x1 != x2:

$$m := y2-y1/x2-x1 = -3+9/-4 = -3/2 = -1.5$$

$$x3 := m^2 - x1 - x2 = (-1.5)^2 - 4 = -1.75$$

$$y3 := -m(x3 - x1) - y1 = 1.5 * ((-1.75) - 4) + 9 = 0.375$$

$$P+Q := (x3; y3) = (-1.75; 0.375)$$

Falls
$$x1 = x2$$
 und $y1 = y2 != 0$:

$$m := 3x1^2+a/2y1 = 3^4^2 + 2/2^4(-9) = -25/9$$

$$x3 := m^2 - 2x1 = (-25/9)^2 - 2^4 = -23/81$$

$$y3 := -m(x3 - x1) - y1 = 25/9 * ((-23/81) - 4) + 9 = -2114/729$$

$$2P := (x3; y3) = (-23/81; -2114/729)$$

Aufgabe 2 (T)

Wir betrachten den Körper K = GF(11) und die elliptische Kurve über K mit der Gleichung

$$E: y^2 = x^3 + 4x + 1.$$

- (a) Erstellen Sie eine Tabelle, die jedem $x \in K$ den Wert $s_x = x^3 + 4x + 1$ zuordnet.
- (b) Bestimmen Sie für jedes $s_x = x^3 + 4x + 1$, das quadratischer Rest modulo 11 ist, die Wurzeln $y_{1,2}$ und bestimmen Sie so die Menge der Punkte der elliptischen Kurve. **Hinweis:** Berechnen Sie die Wurzeln mithilfe von PARI-GP.
- (c) Berechnen Sie P(5;5) Q(7;3) mit Angabe der Zwischenschritte.
- (d) Berechnen Sie 2P(7;3) mit Angabe der Zwischenschritte.

Aufgabe 3 (T)

Bestimmen Sie mit Hilfe des Baby Step – Giant Step Algorithmus in \mathbb{Z}_{61}^* den diskreten Logarithmus $\log_{17}(42)$.

Aufgabe 4 (T)

Lösen Sie die Gleichung $78x = 246 \pmod{264}$.

Aufgabe 5 (T)

Bestimmen Sie mit Hilfe der Pollard ρ - Methode in \mathbb{Z}_{23}^* den diskreten Logarithmus $\log_5(10)$. **Hinweis:** Wählen Sie die folgende Zerlegung von \mathbb{Z}_{23}^* : $G_1 = \{1, 2, ..., 7\}, G_2 = \{8, 9, ..., 15\}, G_3 = \{16, 17, ..., 22\}.$

2. K = GF(11) / E : $y2 = x^3 + 4x + 1 -> a=4$; b=1