

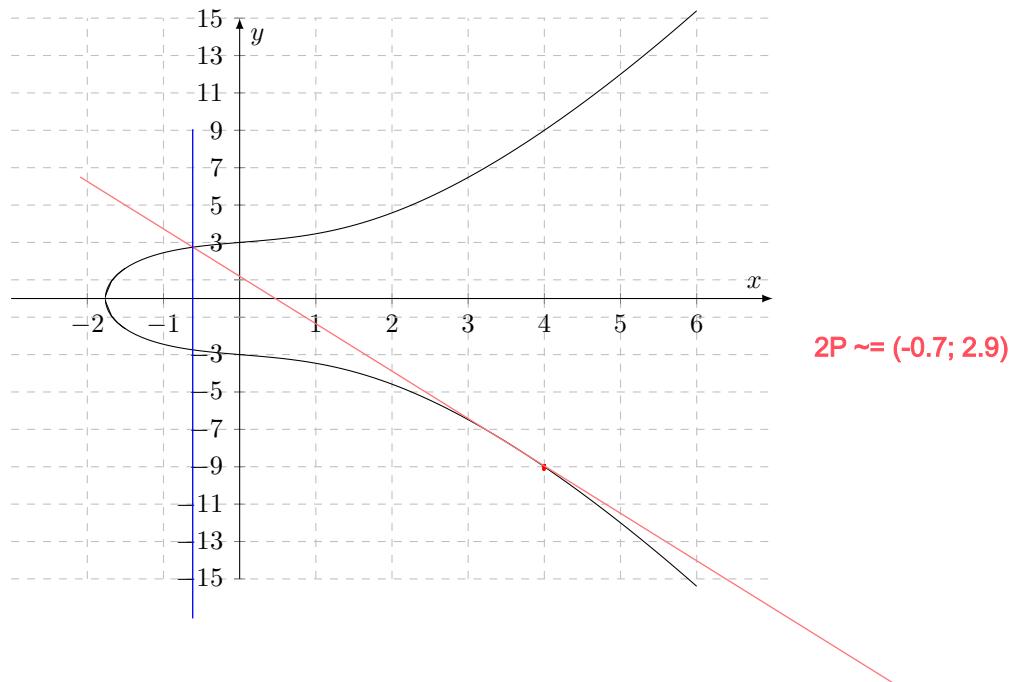
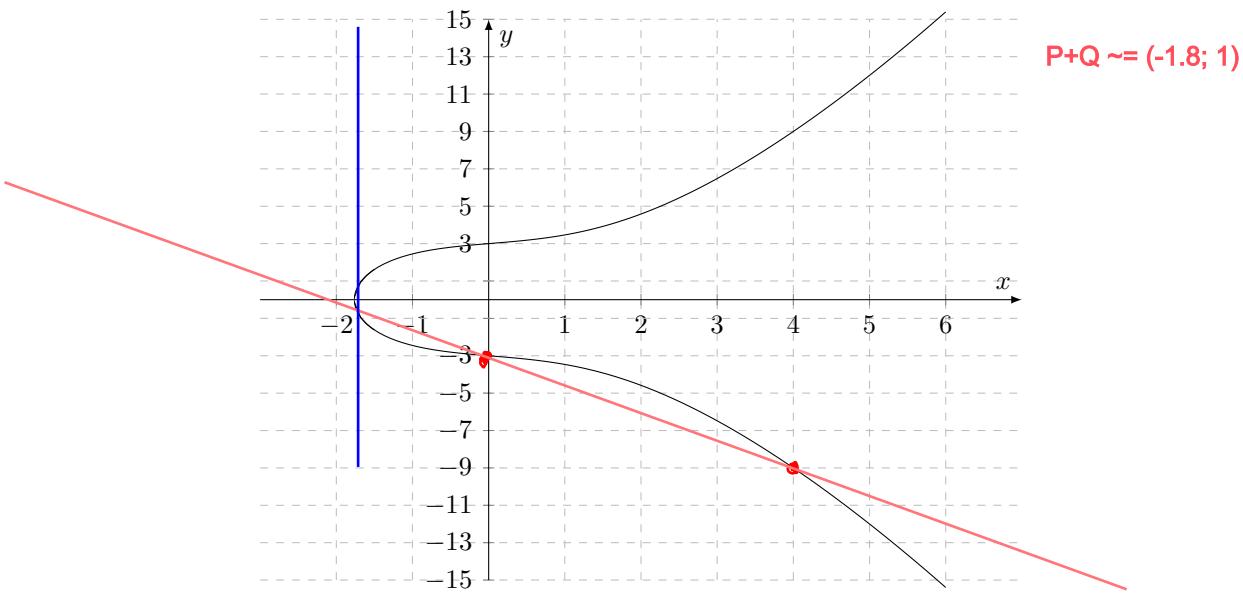
KRY: Wahlfach Kryptologie

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.

- Bestimmen Sie zeichnerisch die ungefähren Werte von $P + Q$ und $2P$.
- 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 $x_1 \neq x_2$:

$$m := y_2 - y_1 / x_2 - x_1 = -3 + 9 / -4 = -3/2 = -1.5$$

$$x_3 := m^2 - x_1 - x_2 = (-1.5)^2 - 4 = -1.75$$

$$y_3 := -m(x_3 - x_1) - y_1 = 1.5 * ((-1.75) - 4) + 9 = 0.375$$

$$P+Q := (x_3; y_3) = (-1.75; 0.375)$$

Falls $x_1 = x_2$ und $y_1 = y_2 \neq 0$:

$$m := 3x_1^2 + a / 2y_1 = 3*4^2 + 2 / 2*(-9) = -25/9$$

$$x_3 := m^2 - 2x_1 = (-25/9)^2 - 2*4 = -23/81$$

$$y_3 := -m(x_3 - x_1) - y_1 = 25/9 * ((-23/81) - 4) + 9 = -2114/729$$

$$2P := (x_3; y_3) = (-23/81; -2114/729)$$

Aufgabe 2 (T)

Wir betrachten den Körper $K = \text{GF}(11)$ 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}^* : $G_1 = \{1, 2, \dots, 7\}$, $G_2 = \{8, 9, \dots, 15\}$, $G_3 = \{16, 17, \dots, 22\}$.

2.a)b)

$$K = GF(11) / E : y^2 = x^3 + 4x + 1 \rightarrow a=4; b=1$$

$$a \in \mathbb{Z}_p \text{ hat eine Quadratwurzel} \Leftrightarrow a^{\frac{p-1}{2}} = 1 \pmod{p}$$

x	0	1	2	3	4	5	6	7	8	9	10
s_x	1	6	6	7	4	3	10	9	6	7	7
s_x^5 mod 11 = 1	TRUE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE
y1 (+sqrt mod 11)	1				9	1		8			
y2 (-sqrt mod 11)	10				2	10		3			

2.c)

$$P(5; 5) - Q(7; 3)$$

$$P - Q = P + (-Q)$$

$$-Q = (7; -3) \pmod{11} = (7; 8)$$

$$P(5; 5) + -Q(7; 8)$$

$$m = 8-5/7-5 \pmod{11} = 3/2 \pmod{11} = 7$$

$$gp > \text{Mod}(3/2, 11) \rightarrow \text{Mod}(7, 11)$$

$$x_3 = 7^2-5-7 \pmod{11} = 4$$

$$gp > \text{Mod}(7^2-5-7, 11) \rightarrow \text{Mod}(4, 11)$$

$$y_3 = -7*(4-5)-5 \pmod{11} = 2$$

$$gp > \text{Mod}(-7*(4-5)-5, 11) \rightarrow \text{Mod}(2, 11)$$

$$\Rightarrow P+(-Q) = (4; 2)$$

3.

$$Z^*_{-61}; \log_{17}(42)$$

$$\rightarrow g=17; a=42; n=61; m=\text{roundUp}(\sqrt{61})=8$$

Babysteps: 0-7

$$(0; 17^0) \pmod{61} = (0; 1)$$

$$(1; 17^1) \pmod{61} = (1; 17)$$

$$(2; 17^2) \pmod{61} = (2; 45)$$

$$(3; 17^3) \pmod{61} = (3; 33)$$

$$(4; 17^4) \pmod{61} = (4; 12) \leqslant$$

$$(5; 17^5) \pmod{61} = (5; 21)$$

$$(6; 17^6) \pmod{61} = (6; 52)$$

$$(7; 17^7) \pmod{61} = (7; 30)$$

Giantsteps:

$$h=17^{-8} \pmod{61} = 25$$

$$(0; 42*25^0) \pmod{61} = (0; 42)$$

$$(1; 42*25^1) \pmod{61} = (1; 13)$$

$$(2; 42*25^2) \pmod{61} = (2; 20)$$

$$(3; 42*25^3) \pmod{61} = (3; 12) \leqslant$$

$$a^*(g^{-8})^3 = g^4$$

$$a = g^{8*3+4} = g^{28}$$

4.

$$78x = 246 \pmod{264}$$

Vereinfachung der Gleichung:

$$\text{gp} > \text{gcd}(78, 264) = 6$$

$$78/6 = 13$$

$$246/6 = 41$$

$$264/6 = 44$$

$$13x = 41 \pmod{44}$$

Multiplikative Inverse von 13

$$a = 13^{-1} \pmod{44} = 17$$

$$\text{gp} > \text{Mod}(13^{-1}, 44) \rightarrow \text{Mod}(17, 44)$$

$$x = a * 41 + b * 44 \pmod{264} \mid b = \{0, 1, 2, 3, 4, 5\}$$

$$b=0$$

$$\text{gp} > \text{Mod}(17 * 41, 264) = 169$$

$$b=1$$

$$\text{gp} > \text{Mod}(17 * 41 + 44, 264) = 213$$

$$b=2$$

$$\text{gp} > \text{Mod}(17 * 41 + 2 * 44, 264) = 257$$

$$b=3$$

$$\text{gp} > \text{Mod}(17 * 41 + 3 * 44, 264) = 37$$

$$b=4$$

$$\text{gp} > \text{Mod}(17 * 41 + 4 * 44, 264) = 81$$

$$b=5$$

$$\text{gp} > \text{Mod}(17 * 41 + 5 * 44, 264) = 125$$

5.

$$Z^{*23}; \log_5(10)$$

$$G1=\{1, \dots, 7\}; G2=\{8, \dots, 15\}; G3=\{16, \dots, 22\};$$

$$g=5; a=10; p=23$$

$$x_i = a^r * g^s \pmod{p}$$

$$x_0 = 1 \rightarrow r=0, s=0$$

$$\Rightarrow 1 \text{ Element von } G1 \Rightarrow x_1 = x_0 * a = 10$$

$$x_1 = 10 \rightarrow r=1, s=0$$

$$\Rightarrow 10 \text{ Element von } G2 \Rightarrow x_2 = x_1^2 \pmod{23} = 8$$

$$x_2 = 8 \rightarrow r=2, s=0$$

$$\Rightarrow 8 \text{ Element von } G2 \Rightarrow x_3 = x_2^2 \pmod{23} = 18$$

$$x_3 = 18 \rightarrow r=4, s=0$$

$$\Rightarrow 18 \text{ Element von } G3 \Rightarrow x_4 = g * x_3 \pmod{23} = 21$$

$$x_4 = 21 \rightarrow r=4, s=1$$

$$\Rightarrow 21 \text{ Element von } G3 \Rightarrow x_5 = g * x_4 \pmod{23} = 13$$

$$x_5 = 13 \rightarrow r=4, s=2$$

$$\Rightarrow 13 \text{ Element von } G2 \Rightarrow x_6 = x_5^2 \pmod{23} = 8$$

$$x_6 = 8 \rightarrow r=8, s=4$$

$$\Rightarrow \text{Duplikat}$$

$$10^2 * 5^0 = 10^8 * 5^4 \pmod{23}$$

$$= 10^{-6} = 5^4 \pmod{23}$$

$$10 = 5^x \Rightarrow 5^{-6} * x = 5^4 \pmod{23}$$

$$-6x = 4 \pmod{22}$$

$$\text{gcd}(6, 22) = 2$$

$$-3x = 2 \pmod{11}$$

$$(-3)^{-1} \pmod{11} = 7$$

$$7^2 \pmod{22} = 14$$

$$7^2 + 11 \pmod{22} = 3$$

$$5^3 \pmod{23} = 10 \Rightarrow x=3$$