

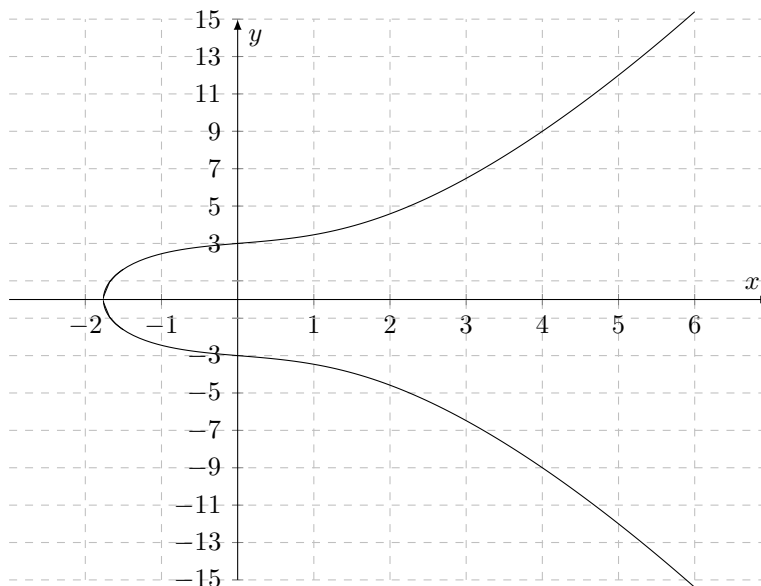
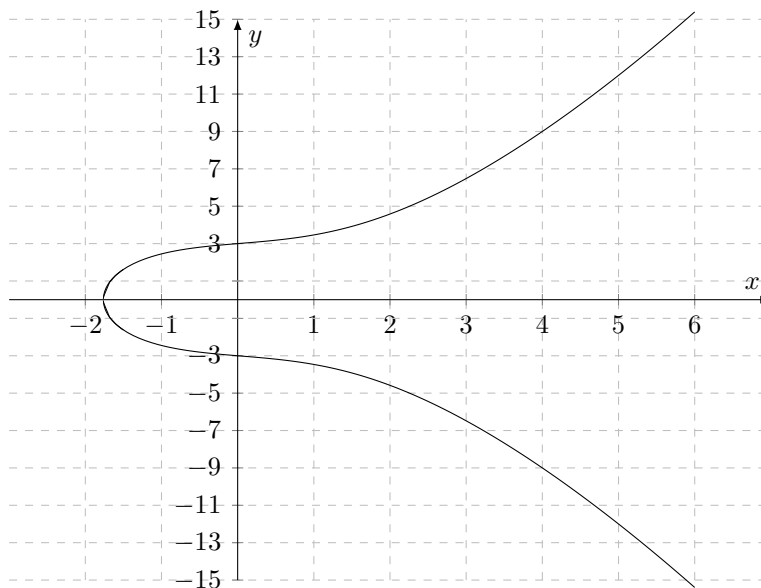
## KRY: Wahlfach Kryptologie

### 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.



**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  $\rho$  - Methode in  $\mathbb{Z}_{23}^*$  den diskreten Logarithmus  $\log_5(10)$ .

**Hinweis:** Wählen Sie die folgende Zerlegung von  $\mathbb{Z}_{23}^*$ :  $G_1 = \{1, 2, \dots, 7\}$ ,  $G_2 = \{8, 9, \dots, 15\}$ ,  $G_3 = \{16, 17, \dots, 22\}$ .