

Zusatz-Übungsblatt zur Vorlesung  
Kryptologie**Übung 1**

Wählen Sie sich auf der umseitig abgebildeten elliptischen Kurve drei Punkte  $P_1$ ,  $P_2$  und  $P_3$  und bestimmen Sie zeichnerisch  $P_1 + (P_2 + P_3)$  und  $(P_1 + P_2) + P_3$ .

**Übung 2**

Welche Punkte besitzt die elliptische Kurve bzgl.

$$y^2 = x^3 - 3x - 1$$

über  $\mathbb{Z}_7$ ?

**Übung 3**

Betrachtet wird die elliptische Kurve über  $\mathbb{Z}_5$  bzgl.

$$y^2 = x^3 - x + 1.$$

Zeigen Sie durch Nachrechnen, dass gilt:

$$((0, 1) + (4, 4)) + (0, 4) = (0, 1) + ((4, 4) + (0, 4)).$$

**Übung 4**

Eine Zahl  $a \in \mathbb{Z}_p$  heißt *quadratischer Rest* modulo  $p$  genau dann, wenn es ein  $x \in \mathbb{Z}_p$  gibt mit  $a = x^2 \pmod{p}$ .

Zeigen Sie: Ist  $p$  eine Primzahl  $> 2$ , so gibt es genau  $\frac{p+1}{2}$  quadratische Reste in  $\mathbb{Z}_p$ .

