5. Übungsblatt

Abgabe: Mittwoch, 10.6.09

Aufgabe 1 Seien a, b in $\mathbb{Z}$ und n in $\mathbb{N}$. Zeigen Sie:

a) Die Kongruenz
$$ax \equiv b \bmod n$$
ist genau dann lösbar, wenn $d = \mathrm{ggT}(a, n)$ ein Teiler von b ist.

b) Gilt $d \mid b$, so gibt es genau d Lösungen x mit $0 \leq x \leq n-1$.

Aufgabe 2 Sei $x \neq x'$ binäre Folgen endlicher Länge und seien $x_1 \dots x_t$ bzw. $x'_1 \dots x'_{t'}$ die zugehörigen Bitfolgen mittels derer nach der Konstruktion aus der Vorlesung die Hash-Werte von x und x' bestimmt werden. Zeige: Ist $t \leq t'$, so existiert ein $0 \leq i < t$ mit $x_{t-i} \neq x'_{t'-i}$.

Aufgabe 3 Zeigen Sie, dass die drei Nullstellen von $x^3+ax+b \in K[x]$ genau dann paarweise verschieden sind, wenn $4a^3 + 27b^2 \neq 0$ ist.

Aufgabe 4 Gegeben sei die elliptische Kurve $E : y^2 = x^3 - x$.

a) Berechnen Sie $|E(\mathbb{Z}_5)|$.

b) Zeigen Sie, dass $E(\mathbb{Z}_5)$ genau ein Element der Ordnung 2, aber kein Element der Ordnung 4 hat