Prof. Dr. M. Kreuzer
P. Ackermann

Abgabe: 20.06.2005, 14h

Kryptografie
Übungsblatt 9

Aufgabe 27:
Gegeben sei ein Körper K und eine kubische Kurve über K mit der Gleichung $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Zeigen Sie, dass diese Gleichung durch eine Koordinatentransformation auf die folgende Gestalt gebracht werden kann:

a) $y^2 = x^3 + ax + b$ (mit $a, b \in K$), falls $\mathrm{char}(K) \notin \{2, 3\}$ gilt,
b) $y^2 = x^3 + ax^2 + bx + c$ (mit $a, b, c \in K$ und $ab = 0$), falls $\mathrm{char}(K) = 3$ gilt,
c) $y^2 + ay = x^3 + bx + c$ oder $y^2 + xy = x^3 + dx^2 + e$ (mit $a, b, c, d, e \in K$), falls $\mathrm{char}(K) = 2$ gilt.

Aufgabe 28:
Gegeben sei der folgende Satz:

Drei Geraden G_1, G_2, G_3 mögen eine kubische Kurve C in neun Punkten $P_1, \ldots, P_9$ schneiden. Schneiden drei weitere Geraden H_1, H_2, H_3 die Kurve C dann ebenfalls in neun Punkten $Q_1, \ldots, Q_9$ und gilt $P_i = Q_i$ für $i = 1, \ldots, 8$, so folgt $P_9 = Q_9$.

Verwenden Sie diesen Satz, um das Assoziativgesetz für die Addition von Punkten auf einer elliptischen Kurve zu beweisen.
Hinweis: Behandeln Sie zuerst den Fall, dass einer der drei Punkte der unendlich ferne Punkt ist.

Aufgabe 29:
Sei $K = \mathbb{Q}$ oder $K = \mathbb{Z}/p\mathbb{Z}$ mit $p \notin \{2, 3\}$. Schreiben Sie eine Funktion `EllipticPoint(...)`, die ausgehend von den Parametern $a, b \in K$ einer elliptischen Kurve $E(K)$ über K einen Punkt $(x, y) \in E(K)$ berechnet.