Institut für Informatik
Komplexität und Kryptografie
Prof. Dr. Johannes Köbler

Sommersemester 2006

Übungen zur Kryptologie 2

6. Aufgabenblatt

Aufgabe 1

Betrachten Sie die mittels

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

über den reellen Zahlen definierte elliptische Kurve E.

a) Skizieren Sie zeichnerisch den Verlauf von E.

b) Berechnen Sie die Summe $P + Q$ für $P = (3, 4)$ und $Q = (2, 0)$.

c) Berechnen Sie die Punkte $2P = P + P$ und $2Q = Q + Q$.

Aufgabe 2

Die Punkte der *projektiven Ebene* werden durch die Ursprungsgeraden

$$g(X, Y, Z) = \{(\lambda X, \lambda Y, \lambda Z) \mid \lambda \in \mathbb{R}\},\ (X, Y, Z) \in \mathbb{R}^3 - \{(0, 0, 0)\}$$

gebildet. Es gilt also $g(X, Y, Z) = g(X', Y', Z')$, falls ein $\lambda \in \mathbb{R} - \{0\}$ existiert mit $X' = \lambda X$, $Y' = \lambda Y$ und $Z' = \lambda Z$.

a) Überlegen Sie, wie sich die affine Ebene $\mathbb{R}^2$ in die projektive Ebene einbetten lässt. *Hinweis:* Verwenden Sie nur projektive Punkte der Form $g(X, Y, 1)$.

b) Zeigen Sie, dass von dieser Einbettung genau die projektiven Punkte der Form $g(X, Y, 0)$ nicht erfasst werden. Welche Punkte müsste man zum $\mathbb{R}^2$ hinzunehmen, damit diese Einbettung zu einem Isomorphismus wird? Geben Sie eine geometrische Interpretation dieser Punkte.

c) Im $\mathbb{R}^2$ sei eine Kurve durch eine Gleichung der Form $F(x, y) = y^2 - x^3 - ax - b = 0$ definiert. Wie lässt sich hieraus eine Kurvengleichung $\tilde{F}(X, Y, Z) = 0$ für die Einbettung $\{g(x, y, 1) \mid F(x, y) = 0\}$ dieser Kurve in die projektive Ebene gewinnen?

d) Welche projektiven Punkte der Form $g(X, Y, 0)$ erfüllen ebenfalls die Gleichung $\tilde{F}(X, Y, Z) = 0$?

Aufgabe 3

Geben Sie eine geometrische Bedingung dafür an, dass ein Punkt P auf einer elliptischen Kurve über $\mathbb{R}$ die Ordnung 2, 3 oder 4 hat.

Aufgabe 4

Sei E eine durch die Gleichung $F(x, y) = 0$ im $\mathbb{R}^2$ definierte Kurve, wobei F die Form $F(x, y) = y^2 - x^3 - ax - b$ hat. Zeigen Sie, dass folgende Bedingungen äquivalent sind.

a) Das Polynom $p(x) = x^3 + ax + b$ hat eine mehrfache Nullstelle,

b) $4a^3 = -27b^2$,

c) Es ex. ein Punkt $(x_0, y_0) \in E$, für den die partiellen Ableitungen $\frac{\delta F}{\delta x}(x_0, y_0)$ und $\frac{\delta F}{\delta y}(x_0, y_0)$ beide 0 sind. (Ein solcher Punkt heißt *singulär*.)

Aufgabe 5

Zeigen Sie, dass eine über

$$y^2 = x^3 + ax + b$$

definierte elliptische Kurve nicht zyklisch ist, wenn das Polynom $x^3 + ax + b$ drei verschiedene Nullstellen in $\mathbb{Z}_p$ hat.

Aufgabe 6

Bestimmen Sie die Anzahl der Punkte der durch

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

definierten elliptischen Kurve über $\mathbb{F}_q$, falls $q \equiv_6 5$ ist.

Aufgabe 7 (10 Punkte)

Sei E die über $\mathbb{Z}_{71}$ durch

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

definierte elliptische Kurve E.

a) Bestimmen Sie die Anzahl der Punkte von E.

b) Zeigen Sie, dass E nicht zyklisch ist.

c) Bestimmen Sie alle Punkte der Ordnung 1, 2, 3 und 4, sowie einen Punkt maximaler Ordnung in E.