Übungen zur Kryptologie 2 Sommersemester 2008

Johannes Köbler/Sebastian Kuhnert

Übungsblatt 7

Aufgabe 49

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) Es gilt $4a^3 = -27b^2$.

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 50

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 51

Zeigen Sie, dass eine über $\mathbb{Z}_p$ mittels

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

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

Aufgabe 52

Bestimmen Sie die Anzahl der Punkte der durch

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

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

Aufgabe 53

Eine elliptische Kurve E über $\mathbb{F}_q$ ($q = 2^n$) enthält neben dem Punkt O alle Lösungen $(x,y) \in \mathbb{F}_{2^n}$ einer Gleichung der Form

$$y^2 + cy = x^3 + ax + b \text{ oder } y^2 + xy = x^3 + ax^2 + b.$$

Leiten Sie für beide Gleichungen Formeln für die Koordinaten von $-P$ und $P + Q$ in Abhängigkeit der Koordinaten von $P = (x_1, y_1)$ und $Q = (x_2, y_2)$ her.
Hinweis: Bestimmen Sie hierzu wie in der Vorlesung die Koordinaten des Schnittpunktes der durch P und O (bzw. durch P und Q) definierten Geraden mit der Kurve über $\mathbb{R}$ und beachten Sie die Besonderheiten der Arithmetik in $\mathbb{F}_{2^n}$.

Aufgabe 54

Sei E_q die durch $y^2 + y = x^3$ über $\mathbb{F}_q$ ($q = 2^n$) definierte elliptische Kurve.

a) Sei $P = (x,y) \in E_q$. Bestimmen Sie die Koordinaten von $-P$ und von $2P$.

b) Bestimmen Sie die Ordnung aller Punkte P von E_{16}.
Hinweis: Berechnen Sie die Koordinaten von $4P$.

c) Bestimmen Sie die Anzahl der Punkte von E_4 und von E_{16}.
Hinweis: Zeigen Sie $\#E_{16} = \#E_4$ und benutzen Sie den Satz von Hasse.

Aufgabe 55

Bestimmen Sie die Anzahl der Punkte der durch $y^2 + y = x^3$ definierten elliptischen Kurve E_q über $\mathbb{F}_q$, falls $q \equiv_3 2$ ist.

Aufgabe 56

a) Bestimmen Sie die NFA-Darstellung der Zahl 87.

b) Bestimmen Sie mit Hilfe des Algorithmus DoubleAddSub das Vielfache $87P$ des Punktes $P = (2,6)$ auf der elliptischen Kurve E, die über $\mathbb{Z}_{127}$ durch $y^2 = x^3 + x + 26$ definiert ist.

Aufgabe 57

Bestimmen Sie die Anzahl l_i aller natürlichen Zahlen, die eine NAF-Darstellung der Form $(c_{i-1}, \ldots, c_0)$ mit $c_{i-1} = 1$ haben. Zeigen Sie hierzu folgende Rekursion und finden Sie eine explizite Formel für l_i.

$$l_i = \begin{cases} 1, & i \le 2, \\ 2(l_1 + \cdots + l_{i-2}) + 1, & i \ge 3. \end{cases}$$

Aufgabe 58

Was wären die Folgen, wenn man beim ECDSA-Signaturverfahren $y = 0$ oder $z = 0$ zulassen würde.

Aufgabe 59 (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.