Übungsblatt 5

Aufgabe 35 ***mündlich***

- 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.
- Zeigen Sie, dass eine elliptische Kurve $y^2 = x^3 + ax + b$ über $\mathbb{F}_q$ nicht zyklisch ist, wenn das Polynom $x^3 + ax + b$ drei verschiedene Nullstellen in $\mathbb{F}_q$ hat.

Aufgabe 36 Die Ursprungsgeraden ***mündlich***

$$g(X,Y,Z) = \left\{(\lambda X, \lambda Y, \lambda Z) \;\middle|\; \lambda \in \mathbb{R}\right\},\ (X,Y,Z) \in \mathbb{R}^3 - \{(0,0,0)\}$$

bilden die Punkte der *projektiven Ebene*. 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 durch $F(x,y) = y^2 - x^3 - ax - b = 0$ eine Kurve definiert. Wie lässt sich hieraus eine Kurvengleichung $\tilde{F}(X,Y,Z) = 0$ für die Einbettung $\left\{g(x,y,1) \;\middle|\; F(x,y) = 0\right\}$ dieser Kurve in die projektive Ebene gewinnen?

(d) Für welche projektiven Punkte der Form $g(X,Y,0)$ gilt ebenfalls $\tilde{F}(X,Y,Z) = 0$?

Aufgabe 37 Wieviele Punkte haben folgende ell. Kurven über $\mathbb{F}_q$? ***mündlich***

(a) $y^2 = x^3 - 1$ im Fall $q \equiv_6 5$ und

(b) $y^2 + y = x^3$ im Fall $q \equiv_3 2$.

Aufgabe 38 ***mündlich***

Eine elliptische Kurve E über $\mathbb{F}_q$ $(q = 2^n)$ enthält neben dem Punkt $\mathcal{O}$ 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 $\mathcal{O}$ (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 39 Sei E_q die elliptische Kurve $y^2 + y = x^3$ über $\mathbb{F}_q$ $(q = 2^n)$. ***mündlich***

(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 40 ***mündlich***

(a) Bestimmen Sie die NAF-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 41 ***mündlich***

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 42 ***mündlich***

Ein Dokument x soll mit dem RSA-Verfahren sowohl verschlüsselt als auch signiert werden. Beschreiben Sie, worauf hierbei zu achten ist, damit die Nachricht nicht abgefangen und unbemerkt mit der Signatur eines Angreifers versehen werden kann.

Aufgabe 43 ***mündlich***

Sei g ein Erzeuger von $\mathbb{Z}_p^*$, p prim (d.h. $\mathbb{Z}_p^* = \{1, \ldots, p-1\} = \{g^i \bmod p \mid i = 1, \ldots, p-1\}$). Bestimmen Sie die Ordnung $\mathrm{ord}(g^i) = \min\{j \ge 1 \mid (g^i)^j \equiv_p 1\}$ von g^i in $\mathbb{Z}_p^*$.

Aufgabe 44 Sei E die elliptische Kurve $y^2 = x^3 - x$ über $\mathbb{Z}_{71}$. ***10 Punkte***

(a) Bestimmen Sie die Anzahl der Punkte von E.

(b) Bestimmen Sie alle Punkte der Ordnung 1, 2, 3 und 4, sowie einen Punkt maximaler Ordnung in E. Ist E zyklisch?