Humboldt-Universität zu Berlin
Prof. Dr. Johannes Köbler

Kryptologie - SoSe 2018
31. Mai 2018

Übungsblatt 6

Aufgabe 38 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 39 ***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 Gleichungen der Form $y^2+cy = x^3+ax+b$ 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 40 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 41 Sei E die elliptische Kurve $y^2 = x^3 + x + 26$ über $\mathbb{Z}_{127}$. ***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.

Aufgabe 42 ***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.

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

Aufgabe 43 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?