Vorlesung „Kryptographie II“ (Sommersemester 2025)

Übungsblatt 12 (18.7.2025)

Aufgabe 56: Sei p eine Primzahl mit $p \equiv 1 \bmod 4$ und $E_{a,0}$ die durch $y^2 = x^3 + ax$ über $\mathbb{F}_p$ definierte elliptische Kurve für $a \in \mathbb{F}_p^*$. Zeige:

(1) Für $a, a' \in \mathbb{F}_p^*$ gilt die Äquivalenz:

$$a' = u^4 a \text{ für ein } u \in \mathbb{F}_p^* \quad \Longleftrightarrow \quad a^{\frac{p-1}{4}} = {a'}^{\frac{p-1}{4}}.$$

(2) Für $a, a' \in \mathbb{F}_p^*$ gilt die Äquivalenz:

$$E_{a,0} \text{ und } E_{a',0} \text{ sind isomorph über } \mathbb{F}_p \quad \Longleftrightarrow \quad a^{\frac{p-1}{4}} = {a'}^{\frac{p-1}{4}}.$$

(3) Es gilt

$$|\{a^{\frac{p-1}{4}} : a \in \mathbb{F}_p^*\}| = 4.$$

(4) Die über $\mathbb{F}_p$ definierten elliptischen Kurven mit j-Invariante 1728 zerfallen in 4 Isomorphieklassen über $\mathbb{F}_p$.

Sei nun $p = 509$. (Statt mit $p = 509$ kann man die Aufgabe mit jeder Primzahl $p \equiv 1 \bmod 4$ durchführen.)

(5) Gib für jede Isomorphieklasse der über $\mathbb{F}_p$ definierten elliptischen Kurven mit j-Invariante 1728 einen Repräsentanten an, also 4 Kurven $E_{a_i,0} : y^2 = x^3 + a_i x$, $i = 1, 2, 3, 4$.

(6) Bestimme $|E_{a_i,0}(\mathbb{F}_p)|$ und $|E_{a_i,0}(\mathbb{F}_p)| - (p+1)$ für $i = 1, 2, 3, 4$.

(7) Bestimme $m, n \in \mathbb{N}$ mit $p = m^2 + n^2$, beispielsweise mit dem Algorithmus zum Zwei-Quadrate-Satz.

(8) Vergleiche die Ergebnisse in (6) und (7). Lässt sich eine Vermutung aufstellen?

Aufgabe 57: Bestimme für die Gitter

$$\Lambda_1 = \mathbb{Z} \cdot 2 + \mathbb{Z} \cdot (1 + \sqrt{-5}) \quad \text{und} \quad \Lambda_2 = \mathbb{Z} \cdot 2 + \mathbb{Z} \cdot (1 + \sqrt{-7})$$

den Endomorphismenring $\mathrm{End}(\Lambda_i) = \{\alpha \in \mathbb{C} : \alpha\Lambda_i \subseteq \Lambda_i\}$.

Aufgabe 58: Für $p = 233$ wird durch $y^2 = x^3 + x$ eine elliptische Kurve E über $\mathbb{F}_p$ definiert.

(1) Bestimme $|E(\mathbb{F}_p)|$.

(2) Bestimme die Struktur von $E(\mathbb{F}_p)$ als abelsche Gruppe, d.h. $d_1, \ldots, d_r \in \mathbb{N}$ mit $d_1 \mid d_2$, $d_2 \mid d_3$, $\ldots$, $d_{r-1} \mid d_r$ und $E(\mathbb{F}_p) \simeq Z_{d_1} \times \cdots \times Z_{d_r}$.

(3) Bestimme zwei natürliche Zahlen m_1 und m_2 mit

$$p + 1 - 2\sqrt{p} < m_1 < m_2 < p + 1 + 2\sqrt{p},$$

sodass

$$m_1 \cdot P = m_2 \cdot P = O \text{ für alle } P \in E(\mathbb{F}_p)$$

gilt.

Datei: kii_u12.tex. Version vom 17.7.2025

Aufgabe 59: Sei E eine elliptische Kurve über $\mathbb{F}_p$, $P \in E(\mathbb{F}_p)$, $e_A \in \mathbb{N}$ und $Q_A = e_A \cdot P$. Sei $N = |E(\mathbb{F}_p)|$ mit $N = n_1 \dots n_r$, wobei $n_1, \dots, n_r$ paarweise teilerfremd sind, und $N_i = \frac{N}{n_i}$ für $i = 1, \dots, r$.

(1) Zeige: Für $i = 1, \dots, r$ gibt es ein x_i mit

$$N_i \cdot Q_A = x_i \cdot N_i \cdot P \quad \text{und} \quad 0 \leq x_i \leq n_i - 1.$$

(2) Mit dem chinesischen Restsatz findet man ein $x \in \mathbb{Z}$ mit $x \equiv x_i \bmod n_i$ für $i = 1, \dots, r$ und $0 \leq x \leq N - 1$. Zeige, dass dann gilt

$$Q_A = x \cdot P.$$

(Anwendung: Sind die n_i's klein, kann man x_i beispielsweise durch Probieren finden und damit dann den diskreten Logarithmus von Q_A zur Basis P bestimmen.)

Aufgabe 60: Anne benutzt eine Variante der ElGamal-Verschlüsselung mit elliptischen Kurven. Zugrunde liegt die durch $y^2 = x^3 - 30x - 56$ über $\mathbb{F}_p$ definierte elliptische Kurve E mit

$$p = 340282366920938463463374607431745713481$$

und ein Punkt

$$P = (5, 151274519653029985997762667114917526012) \in E(\mathbb{F}_p).$$

Es ist außerdem bekannt, dass gilt

$$|E(\mathbb{F}_p)| = 340282366920938463435852718069021841100.$$

Der öffentliche Schlüssel von Anne ist der Punkt

$$Q_A = (291590769884559095943296524956252909848, 168169858601782381090826520956063046209),$$

den Anne mit ihrem privaten Schlüssel $e_A \in \mathbb{N}$ als $Q_A = e_A \cdot P \in E(\mathbb{F}_p)$ berechnet hat.
Karin will eine Nachricht, die nur aus Großbuchstaben und Leerzeichen besteht, an Anne schicken. Sie teilt die Nachricht in Blöcke der Länge 19 auf, in jedem Block ersetzt sie A durch 01, B durch 02, ..., Z durch 26 und jedes Leerzeichen durch 00. Es entstehen zwei Zahlen a_1, a_2. Karin wählt nun zwei Zufallszahlen z_1, z_2 und berechnet damit

$$R_i = z_i \cdot P = (x_{R_i}, y_{R_i}) \in E(\mathbb{F}_p), \quad S_i = z_i \cdot Q_i = (x_{S_i}, y_{S_i}) \in E(\mathbb{F}_p), \quad t_i = a_i + x_{S_i} \bmod p.$$

Karin schickt an Anne die Zahlentripel $(x_{R_i}, y_{R_i} \bmod 2, t_i)$ für $i = 1, 2$:

$$(330876176871207193972420510066687583 06, 1, 225679372127487540565397625036020851579),$$

$$(909065629816319442209125077589376563 61, 0, 286729791488297508163918458677598654477).$$

Was will Karin Anne mitteilen? (Hinweis: Aufgabe 59)