Vorlesung „Kryptographie II“ (Sommersemester 2025)

Übungsblatt 9 (27.6.2025)

Aufgabe 41:

(1) Sei E eine über einem Körper K (der Charakteristik $\neq 2, 3$) durch $y^2 = x^3 + ax + b$ definierte elliptische Kurve und $(x_1, y_1), \ldots, (x_n, y_n) \in E(K)$. Zeige:

(a) Es gilt

$$\begin{pmatrix} x_1 & 1 \\ x_2 & 1 \\ \vdots & \vdots \\ x_n & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} y_1^2 - x_1^3 \\ y_2^2 - x_2^3 \\ \vdots \\ y_n^2 - x_n^3 \end{pmatrix}.$$

(b) Die Matrix

$$\begin{pmatrix} x_1 & 1 & y_1^2 - x_1^3 \\ x_2 & 1 & y_2^2 - x_2^3 \\ \vdots & \vdots & \vdots \\ x_n & 1 & y_n^2 - x_n^3 \end{pmatrix}$$

hat Rang ≤ 2 und jede 3×3-Untermatrix hat Determinante 0.

(2) Die folgenden vier Punkte P_i

$$\begin{aligned} P_1 &= (410977650387461885166918264382, 1171732399374379425829326543 2), \\ P_2 &= (438549448898086231254041345807, 306116929809774958561556686820), \\ P_3 &= (591122728927400712901339648638, 519977520554277876993896158514), \\ P_4 &= (137383245866090536750778529466, 541709075181038805910489375572). \end{aligned}$$

sind Punkte einer über einem endlichen Körper $\mathbb{F}_p$ definierten elliptischen Kurve E mit einer Gleichung $y^2 = x^3 + ax + b$. Leider sind p, a und b irgendwie verlorengegangen. Rekonstruiere p, a und b.

Aufgabe 42: Karl und Paul verwenden die VIGENERE-Verschlüsselung zum Nachrichtenaustausch. Zur Schlüsselerzeugung haben Karl und Paul eine Primzahl p, eine elliptische Kurve E über $\mathbb{F}_p$ und einen Punkt $P \in E(\mathbb{F}_p)$ vereinbart. Mit $n = \operatorname{ord}(P)$ und $(x_i, y_i) = i \cdot P \in E(\mathbb{F}_p)$ besteht der Schlüssel dann aus der Zahlenfolge

$$x_1, y_1, x_2, y_2, \ldots, x_{n-1}, y_{n-1}.$$

Paul erhält von Karl folgende Nachricht:

```
QNZUFB JIEC,
TYP CSLK TYK MAIAEXVZTZ MOOK TTG UWSA DPOYRK FQGPQY-QBUAGBZHI EMR WZVIXYV KLQ
ATGAZZPIVLRW OQWOWC SQMOKGTXGAF. SXXJJ WKXW VKJ, HJO KCCGNXL PJDUOHHBUXRZP IQO
WVRPFMMFLLAS DMGHQH UVI.
GBJHW PKYOIWK, ASET
```

Entschlüssle den Text. (Hinweis: `CVFGXYRVAREFRPUFHAQMJNAMVT`)

Datei: kii_u9.tex. Version vom 26.6.2025

Aufgabe 43: Über $K = \mathbb{F}_{29}$ ist $E_{a,b} : y^2 = x^3 + ax + b$ mit

$$(a, b) \in \{(2, 6), (4, 7), (8, 9), (8, 14)\}$$

eine elliptische Kurve mit

$$|E_{a,b}(\mathbb{F}_{29})| = 32.$$

Bestimme jeweils die Struktur von $E(\mathbb{F}_{29})$ als abelsche Gruppe.

1. Hinweis: Bis auf Isomorphie gibt es folgende abelsche Gruppen der Ordnung 32:

$Z_{32}, \quad Z_{16} \times Z_2, \quad Z_8 \times Z_4, \quad Z_8 \times Z_2 \times Z_2, \quad Z_4 \times Z_4 \times Z_2, \quad Z_4 \times Z_2 \times Z_2 \times Z_2, \quad Z_2 \times Z_2 \times Z_2 \times Z_2.$

2. Hinweis: In Sage kann man beispielsweise die elliptische Kurve $y^2 = x^3 + 2x + 6$ durch `E=EllipticCurve(GF(29),[2,6])` definieren, mit `E.points()` erhält man die über $\mathbb{F}_{29}$ definierten Punkte, wobei ein Punkt (x, y) in Sage als $(x : y : 1)$ geschrieben wird, der Punkt O ist in Sage $(0 : 1 : 0)$.)

Aufgabe 44: Sei p eine ungerade Primzahl mit $p \equiv 2 \bmod 3$, $b \in \mathbb{F}_p^*$ und E die durch $y^2 = x^3 + b$ über $\mathbb{F}_p$ definierte elliptische Kurve. Zeige:

(1) Es ist $\frac{2p-1}{3} \in \mathbb{N}$ und

$$\left(z^3\right)^{\frac{2p-1}{3}} = \left(z^{\frac{2p-1}{3}}\right)^3 = z \text{ für alle } z \in \mathbb{F}_p.$$

(2) Es gilt

$$E(\mathbb{F}_p) \setminus \{O\} = \{((y^2 - b)^{\frac{2p-1}{3}}, y) : y \in \mathbb{F}_p\}.$$

(3) Es gilt $|E(\mathbb{F}_p)| = p + 1$.

Aufgabe 45: Sei K ein Körper und

$$C = \{(x, y) \in K \times K : y^2 = x^3\}.$$

Zeige:

(1) Die Abbildungen

$$\phi : K \to C, \quad t \mapsto (t^2, t^3)$$

und

$$\psi : C \to K, \quad (x, y) \mapsto \begin{cases} 0 & \text{für } x = 0, \\ \frac{y}{x} & \text{für } x \neq 0 \end{cases}$$

sind wohldefiniert und invers zueinander.

(2) Sind $t_1, t_2, t_3 \in K \setminus \{0\}$ paarweise verschieden, so gilt die Äquivalenz:

$$\phi(t_1), \phi(t_2), \phi(t_3) \text{ liegen auf einer Geraden} \quad \Longleftrightarrow \quad \frac{1}{t_1} + \frac{1}{t_2} + \frac{1}{t_3} = 0.$$

Hinweis: Für 3 Punkte $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in K \times K$ gilt:

$$(x_1, y_1), (x_2, y_2), (x_3, y_3) \text{ liegen auf einer Geraden} \quad \Longleftrightarrow \quad \begin{vmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{vmatrix} = 0.$$