

Übungsblatt 5

Aufgabe 36 Sei E die elliptische Kurve $y^2 = x^3 - 3x - 2$ über \mathbb{R} . **mündlich**

- Skizzieren Sie zeichnerisch den Verlauf von E .
- Berechnen Sie die Summe $P + Q$ für $P = (3, 4)$ und $Q = (2, 0)$.
- Berechnen Sie die Punkte $2P = P + P$ und $2Q = Q + Q$.

Aufgabe 37 Die Ursprungsgeraden **mündlich**

$$g(X, Y, Z) = \{(\lambda X, \lambda Y, \lambda Z) \mid \lambda \in \mathbb{R}\}, (X, Y, Z) \in \mathbb{R}^3 - \{(0, 0, 0)\}$$

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 $Z' = \lambda Z$.

- Überlegen Sie, wie sich die affine Ebene \mathbb{R}^2 in die projektive Ebene einbetten lässt. (*Hinweis*: Verwenden Sie nur projektive Punkte der Form $g(X, Y, 1)$.)
- 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.
- 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 $\{g(x, y, 1) \mid F(x, y) = 0\}$ dieser Kurve in die projektive Ebene gewinnen?
- Für welche projektiven Punkte der Form $g(X, Y, 0)$ gilt ebenfalls $\tilde{F}(X, Y, Z) = 0$?

Aufgabe 38 **mündlich**

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.

- Das Polynom $p(x) = x^3 + ax + b$ hat eine mehrfache Nullstelle.
- Es gilt $4a^3 = -27b^2$.
- Es ex. ein Punkt $(x_0, y_0) \in E$, für den die partiellen Ableitungen $\frac{\partial F}{\partial x}(x_0, y_0)$ und $\frac{\partial F}{\partial y}(x_0, y_0)$ beide 0 sind. (Ein solcher Punkt heißt *singulär*.)

Aufgabe 39 **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{Z}_p nicht zyklisch ist, wenn das Polynom $x^3 + ax + b$ drei verschiedene Nullstellen in \mathbb{Z}_p hat.

Aufgabe 40 Wieviele Punkte haben folgende ell. Kurven über \mathbb{F}_q ? **mündlich**

- $y^2 = x^3 - 1$ im Fall $q \equiv_6 5$ und
- $y^2 + y = x^3$ im Fall $q \equiv_3 2$.

Aufgabe 41 **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

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

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

- Sei $P = (x, y) \in E_q$. Bestimmen Sie die Koordinaten von $-P$ und von $2P$.
- Bestimmen Sie die Ordnung aller Punkte P von E_{16} . (*Hinweis*: Berechnen Sie die Koordinaten von $4P$.)
- 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 43 **mündlich**

- Bestimmen Sie die NAF-Darstellung der Zahl 87.
- 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 44 **mündlich**

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

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

Aufgabe 45 Sei E die elliptische Kurve $y^2 = x^3 - x$ über \mathbb{Z}_{71} . **10 Punkte**

- Bestimmen Sie die Anzahl der Punkte von E .
- Bestimmen Sie alle Punkte der Ordnung 1, 2, 3 und 4, sowie einen Punkt maximaler Ordnung in E . Ist E zyklisch?