Mathematische Methoden in der Kommunikationstheorie

(Sommersemester 2018)

Dr. Tobias Moede
t.moede@tu-bs.de
Universitätsplatz 2, Raum 515
0531 391-7516

Alexander Cant, M.Sc.
a.cant@tu-bs.de
Universitätsplatz 2, Raum 515
0531 391-7516

Technische Universität Braunschweig

Übungsblatt 6

(Abgabe: 15.05.2018 in der VL)

Aufgabe 1. (Rationale Punkte auf elliptischen Kurven I)
Gegeben sei die elliptische Kurve E definiert durch

$$y^2 = x^3 + 3x.$$

Bestimmen Sie den Isomorphietyp der Gruppe $E(\mathbb{F}_7)$.

Aufgabe 2. (Rationale Punkte auf elliptischen Kurven II)
Für einen endlichen Körper F_q sei das *Legendre-Symbol* definiert durch

$$\left(\frac{x}{\mathbb{F}_q}\right) = \begin{cases} +1, & \text{falls } t^2 = x \text{ eine Lösung } t \in \mathbb{F}_q^* \text{ hat,} \\ -1, & \text{falls } t^2 = x \text{ keine Lösung } t \in \mathbb{F}_q^* \text{ hat,} \\ 0, & \text{falls } x = 0. \end{cases}$$

Beweisen Sie, dass für eine elliptische Kurve E definiert durch $y^2 = x^3 + ax + b$ gilt:

$$|E(\mathbb{F}_q)| = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + ax + b}{\mathbb{F}_q}\right).$$

Bestimmen Sie dann mit der Formel $|E(\mathbb{F}_7)|$ für die elliptische Kurve E über $\mathbb{F}_7$, die (wie in Aufgabe 1) gegeben ist durch

$$y^2 = x^3 + 3x.$$

Aufgabe 3. (Gitter I)

(a) Seien $L, L' \subseteq \mathbb{R}^n$ Gitter mit $L \supseteq L'$. Zeigen Sie, dass der Index $|L/L'|$ endlich ist und dass $\det(L') = |L/L'| \cdot \det(L)$ gilt.

(b) Zeigen Sie, dass Gitter diskret (in der gewöhnlichen Topologie) sind. Das heißt: Ist $L \subseteq \mathbb{R}^n$ ein Gitter und $x \in L$, dann existiert eine offene Menge $U \subseteq \mathbb{R}^n$ mit $U \cap L = \{x\}$.

Aufgabe 4. (Gitter II)
Sei $L \subseteq \mathbb{R}^3$ das Gitter mit der Basis $B = \{(42, -38, 65)^T, (103, 87, -10)^T, (-13, 27, 10)^T\}$.

(a) Zeigen Sie, dass $B' = \{(129, 33, -30)^T, (1778, -142, 395)^T, (-910, 90, -230)^T\}$ auch eine Basis von L ist und bestimmen Sie die Basiswechselmatrix von der Basis B zur Basis B'.

(b) Bestimmen Sie die Hadamard-Quotienten von B und B'.

(c) Nutzen Sie den Algorithmus von Babai mit den Basen B und B', um Vektoren $v, v' \in L$ zu finden, die möglichst nah an $w = (170, -51, -90)^T$ liegen. Vergleichen Sie die Ergebnisse.