

Diskrete Mathematik

Blatt 12, 07.07.2006, Abgabe 14.07.2006

Aufgabe 1. Bestimme alle Punkte der elliptischen Kurve $E_{1,1}(\mathbf{Z}_{11})$ und prüfe, ob die Kurve zyklisch ist.

Aufgabe 2. Sei q prim.

Zeige: $|E_{0,b}(\mathbf{Z}_q)| = q + 1$ für $q = 2 \pmod{3}$, $b \in \mathbf{Z}_q^*$.

Hinweis: $x \mapsto x^3$ ist Bijektion von \mathbf{Z}_q für $q = 2 \pmod{3}$.

Aufgabe 3. Zeige die Äquivalenz folgender Aussagen für $\mathbf{x}_1, \dots, \mathbf{x}_m \in \mathbf{R}^n$:

1. $\mathbf{x}_2 - \mathbf{x}_1, \dots, \mathbf{x}_m - \mathbf{x}_1 \in \mathbf{R}^n$ sind linear unabhängig.
 2. $(1, \mathbf{x}_1), \dots, (1, \mathbf{x}_m) \in \mathbf{R}^{n+1}$ sind *linear unabhängig*.
- ($\mathbf{x}_1, \dots, \mathbf{x}_m$ heißen *affin unabhängig*, wenn 1. gilt.)

Aufgabe 4. Betrachte die dualen LP-Aufgaben

$$(P) \quad \max\{\mathbf{c}^t \mathbf{x} \mid A\mathbf{x} \leq \mathbf{b}\}$$

$$(D) \quad \min\{\mathbf{b}^t \mathbf{u} \mid A^t \mathbf{u} = \mathbf{c}, \mathbf{u} \geq 0\}.$$

Konstruiere je ein Beispiel, so dass

1. (P) unbeschränkt (D) unzulässig
2. (D) unbeschränkt (P) unzulässig
3. (P) und (D) unzulässig.

Je 6 Punkte pro Aufgabe.