Vorlesung Angewandte Probleme von Algebra und Geometrie

Prof. Dr. M. Zähle (2h), Übung: E. Schneider (2h), Wintersemester 2013/2014

In Teil 1 der Vorlesung werden ausgewählte Probleme der Konvexgeometrie mit Anwendungen in der linearen Optimierung vorgestellt. Teil 2 liegt auf einem Grenzgebiet zwischen Algebra und Zahlentheorie. Insbesondere zeigen wir, wie die Theorie der primen Restklassengruppen bei modernen Verschlüsselungsmethoden angewendet wird und beschreiben diese Verfahren.
Die Lehrveranstaltung ist für Bachelor Mathematik, Master Wirtschaftsmathematik sowie Lehramt (Gym.)/Vertiefung geeignet. (Teil 1 könnte in Absprache mit der Vorlesung 'Polyedergeometrie' zu einem Lehramtsmodul kombiniert werden.)

Inhalt:

1 Konvexe Mengen

1.1 Affine und euklidische Geometrie

Wiederholung wichtiger Grundlagen

1.2 Konvexität

Charakterisierung konvexer Mengen im affinen Raum; Ebenen und Halbräume, Ellipsoidkörper als Beispiele

1.3 Durchschnitt, konvexe Hülle und konvexe Polyeder

konvexe Hülle als Durchschnitt und als Menge der Konvexkombinationen, Simplizes als spezielle konvexe Polyeder, baryzentrische Koordinaten, konvexe Hülle als Vereinigung von erzeugten Simplizes

1.4 Stützhyperebenen (im euklidischen Fall)

Existenz von Stützhyperebenen an beschränkte konvexe Mengen, abgeschlossene konvexe Hülle als Durchschnitt von Stützhalbräumen

1.5 Extremalpunkte

Begriffsbildung, Beispiele Simplex und Ellipsoidkörper, Extremalpunkte und konvexe Hülle – Satz von Krein-Milman, Extremalpunkte in Stützhyperebenen, Extremalpunkte und konvexe Polyeder

1.6 Anwendung in der linearen Optimierung

allgemeines Verfahren zur Minimierung eines linearen Funktionals unter linearen Nebenbedingungen; Simplexverfahren; Beispiele

2 Elementare Zahlentheorie

2.1 Teilbarkeit in $\mathbb{Z}$ und Primzahlen

Teilbarkeitseigenschaften; Teilbarkeit mit Rest; Euklidischer Algorithmus zur Bestimmung des größten gemeinsamen Teilers; Primzahlzerlegung

2.2 Restklassenringe

Körpereigenschaft von $\mathbb{Z}_p$ für $p \in \mathbb{P}$; Nullteiler in $\mathbb{Z}_n$; Kleiner Fermatscher Satz

2.3 Die primen Restklassengruppen und die Eulersche φ-Funktion

Charakterisierung von $\mathbb{Z}_n^*$; prime Restsysteme; Bestimmung von $\varphi(p),\ p \in \mathbb{P}$; Satz von Euler; $\varphi(m \cdot n),\ \varphi(p^\alpha),\ \varphi(n)$ mittels Primzahlzerlegung; $\sum_{d|n} \varphi(d) = n$

2.4 Verschlüsselungsmethoden

Anwendung der Theorie der primen Restklassengruppen: lineare Methode, exponentielle Methode, RSA-Methode mit Unterschrift

2.5 Die Ordnung von primen Restklassen und Primitivwurzeln

$\operatorname{ord}_n a,\ \operatorname{ord}_n(a^k)$; $\mathbb{Z}_n^* = [a]$ für Primitivwurzeln a, Kongruenz von Polynomen als Hilfsmittel: Moduln mit Primitivwurzeln sind $1, 2, 4, p^k$ und $2p^k$ mit $p \in \mathbb{P} \setminus \{2\},\ k \in \mathbb{N}$