

Diskrete Mathematik II

Roberto Avanzi (nach Alexander May)

Fakultät für Mathematik
Ruhr-Universität Bochum

Sommersemester 2010

Organisatorisches

- Vorlesung: **Mo 12-14** in HIA , **Di 10-11** in ND 2/99
(3+1 SWS, 6.75 CP)
- Übung: **Di 11-13** in NA 5/64
 - ▶ Assistent: **Enrico Thomae**, Korrektor: **Ilya Ozerov**
 - ▶ Übung ist **zweiwöchentlich**: gerade/ungerade Woche.
 - ▶ Übungsaufgaben werden korrigiert und benotet.
 - ▶ Musterlösungen werden veröffentlicht.
 - ▶ Gruppenabgaben bis 3 Personen.
 - ▶ Bonussystem:
bis 10%, bzw etwa 2/3-Notenstufe
Gilt nur, wenn man die Klausur besteht!
Wird sonst (ab 40% der Klausur) nun anteilig berechnet.
- Klausur: voraussichtlich Ende August.

Themengebiete

1 Kodierungstheorie

- ▶ Komprimierende Codes
- ▶ Fehlererkennende Codes
- ▶ Ausfalltolerante Codes
- ▶ + Anwendungen: Kommunikation, Internet, CD, Kryptographie

2 Algorithmische Zahlentheorie

- ▶ Quadratische Reste
- ▶ + Anwendungen: Zufallszahlengenerator, Identity-Based Encryption

3 Elliptische Kurven

- ▶ Arithmetik
- ▶ + Anwendung: Kryptographie

4 Komplexitätstheorie

- ▶ Klassen P und NP
- ▶ Reduktionen
- ▶ + Anwendung: Sicherheitsbeweise in der Kryptographie

Weiterführende Referenzen

- Steven Roman, “Introduction to Coding and Information Theory”, Springer Verlag, 1996
- Michael R. Garey, David S. Johnson, “Computers and Intractability”, Freeman, 2000
- J. Blömer, “Einführung in Algorithmen und Komplexität”, Vorlesungsskript Universität Paderborn, 2002
- N. Koblitz, “A Course in Number Theory and Cryptography”, Springer Verlag, 1994
- R. Avanzi, Skript zur Vorlesung “Zahlentheorie”.