Leibniz Universität Hannover
Fakultät für Mathematik und Physik

20. Januar 2022

SEMINARANKÜNDIGUNG

für das Sommersemester 2022

Thema: Endliche Körper, Primzahltests und Faktorisierung

Veranstalter: Dr. Víctor González Alonso

Überblick: Primzahlen spielen eine sehr wichtige Rolle in der Kodierung und Verschlüsselung von Informationen. Zum Beispiel: die Sicherheit des mittlerweile klassischen RSA-Verschlüsselungsverfahren basiert auf die Schwierigkeit des Faktorisierungsproblems. Das heißt, es ist bisher kein Algorithmus bekannt, der die Primfaktorzerlegung einer beliebigen ganzen Zahl effizient berechnet. Ein sicheres RSA-Verfahren braucht aber zwei große Primzahlen. Man braucht also effiziente Methoden um zu entscheiden, ob eine ganze Zahl eine Primzahl ist: die Primzahltests.

In diesem Seminar werden wir mehrere Primzahltests und Faktorisierungsmethoden besprechen. Dazu werden wir auch einige Eigenschaften von endlichen Körper beweisen und Grundlagen der Komplexitätstheorie einführen.

Zielgruppe: Das Seminar richtet sich vor allem an Studierende des Fächerübergreifenden Bachelors.

Literatur: Grundlage für die Vorträge sind einzelne Kapitel folgender Bücher:

1. H. Kurzweil, *Endliche Körper*, 2. Auflage, Springer (2008).
2. P. Ribenboim, *Die Welt der Primzahlen*, 2. Auflage, Springer (2011).
3. N. Koblitz, *A Course in Number Theory and Cryptography*, Springer (1994).

Voraussetzungen: Kenntnisse aus Lineare Algebra I und Algebra I

Anmeldung: Bis Ende März per E-Mail (gonzalez@math.uni-hannnover.de). Eine Vorbesprechung findet Mitte März statt (der genaue Termin wird bei Stud.IP angekündigt). Bei Fragen können Sie sich gerne über diese E-Mail-Adresse an mich wenden.