PROSEMINAR: PRIMZAHLEN UND FAKTORISIERUNG FÜR DIE KRYPTOGRAFIE

PROF. DR. G. BÖCKLE, K. FISCHER **WS 2016/17**

Das Studium der Primzahlen, d.h. der ganzen Zahlen $p \geq 2$, die sich nicht in mehrere solche Faktoren zerlegen lassen, war Jahrhunderte lang Antrieb und Inspiration für Forschung in der Mathematik.

Durch die umfassende Digitalisierung der Kommunikation in den vergangenen Jahrzehnten rücken nun diese Aspekte der Zahlentheorie in den Fokus von Anwendern: Kryptographen verschlüsseln ihre Emails, Rechnernetze knacken Primzahlrekorde und Internetseiten authentifizieren sich mit SSL.

Das Proseminar erarbeitet die Theorie, die hinter diesen Entwicklungen steht, nimmt dabei aber eine effiziente, algorithmische Sichtweise ein: Schnelle Arithmetik in $\mathbb{Z}/n\mathbb{Z}$, Laufzeitanalyse und probabilistische Verfahren werden ebenso behandelt wie das Zahlkörpersieb, das in der algebraischen Zahlentheorie anzusiedeln ist. Die Themen im einzelnen sind:

- Komplexitätsanalyse, Beispiele §2+3
- Schnelle Arithmetik: DFT, Schönhage-Strassen §9 (*evtl. 2 Vorträge*)
- Pseudoprimzahlen und Miller-Rabin §§3.3-3.5
- Mersenne-Zahlen und der Lukas-Lehmer-Test §4.2
- AKS-Test: 'PRIMES is in P' (*evtl. 2 Vorträge*)
- Faktorisierungsverfahren I: Pollard-Rho und Baby-Step-Giant-Step §5
- Faktorisierungsverfahren II: glatte Zahlen und Quadratisches Sieb §6.1
- Hintergrund: Zahlkörper und Ganzheitsringe
- Faktorisierungsverfahren III: Zahlkörpersieb §6.2
- Der Index-Kalkül §6.4
- Asymmetrische Kryptographie: RSA und DH §8.1

Die Quellenangaben beziehen sich auf das Buch von Crandall und Pomerance.

Termin: Die Veranstaltung wird als **Block im Februar 2017** abgehalten. Voraussichtlich zu Beginn der Semesterferien.

Vorbesprechung/Themenvergabe: Am Dienstag, **18. Oktober 2016**, um 13:00 Uhr in SR3. Bei Interesse tragen Sie sich bitte in **Müsli** ein.

Nützliche Vorkenntnisse: Lineare Algebra 2 (wird erwartet), *elementare Zahlentheorie oder Algebra 1 (hilfreich)*

Literatur: R. Crandall and C. Pomerance, *Prime numbers – A computational perspective*, 2nd ed., Springer, 2005