Universität Karlsruhe
Mathematisches Institut II
Professor Dr. C.–G. Schmidt
Dr. Hendrik Kasten

29. Januar 2008

Proseminar SS 2008: Primzahlen

Seit der Antike sind Primzahlen ein fester aber auch schwierig zu durchschauender Bestandteil der Mathematik. So schrieb beispielsweise der große Carl Friedrich Gauß 1801 in seinen *Disquisitiones Arithmeticae*:

> Dass die Aufgabe, die Primzahlen von den zusammengesetzten zu unterscheiden und letztere in ihre Primfaktoren zu zerlegen, zu den wichtigsten der gesamten Arithmetik gehört und die Bemühungen und den Scharfsinn sowohl der alten als auch der neueren Geometer in Anspruch genommen hat, ist so bekannt, dass es überflüssig wäre, darüber viele Worte zu verlieren. [...] Ausserdem dürfte es die Würde der Wissenschaft erheischen, alle Hülfsmittel zur Lösung jenes so eleganten und berühmten Problems fleissig zu vervollkommnen.

Bekannte Algorithmen wie das Sieb des Eratosthenes haben *exponentielle* Laufzeit, im Beispiel ist dies $O(2^{\log_2 n})$. Kann aber die Primalität vielleicht mit einer anderen Methode effizient entschieden werden? Diese Frage wird im Rahmen der modernen Komplexitätstheorie mathematisch durch die Forderung einer *polynomialen* Laufzeit konkretisiert: Gibt es einen deterministischen Algorithmus, der mit einem festen Exponenten κ für jede natürliche Zahl n in $O(\log^\kappa n)$ Rechenschritten entscheidet, ob diese prim ist oder nicht; kurz:

> Ist PRIMES in $\mathcal{P}$?

Im Jahr 2002 wurde diese Frage von Manindra Agrawal, Neeraj Kayal und Nitin Saxena positiv beantwortet. Dabei verwendete ihr Algorithmus nur elementare Methoden, wie sie bereits im Grundstudium der Mathematik gelehrt werden (können). Das wollen wir uns in diesem Proseminar zunutze machen und werden uns im Laufe des Semesters genug Zahlentheorie aneignen, um in den letzten Vorträgen den Originalartikel behandeln zu können.

Dafür werden wir zunächst einige wichtige Konzepte aus der elementaren Zahlentheorie einführen, wie den Chinesischen Restsatz, Carmichaelzahlen oder das Legendre-Symbol; später werden wir klassische Primzahltests und Faktorisierungsmethoden kennenlernen. Außerdem wollen wir uns im Hinblick auf unser Ziel natürlich auch damit beschäftigen, wie sich aus diesen theoretischen Ergebnissen konkrete Algorithmen bestimmen lassen, die wir auf ihre Laufzeit untersuchen können.

Voraussetzungen: Lineare Algebra I

Anmeldung: bei Frau Hoffmann in Zimmer 308

Vorbesprechung: findet am Donnerstag, dem 7. Februar 2004, um 14 Uhr im S 31 statt.

Kontakt: Sie können uns erreichen unter

Prof. Dr. C.–G. Schmidt
Zimmer 309
Tel.: 0721/608-3040
Claus.Schmidt@math.uni-karlsruhe.de

Hendrik Kasten
Zimmer 307
Tel.: 0721/608-3312
Hendrik.Kasten@math.uni-karlsruhe.de