Fachbereich Mathematik

Mathematisches Kolloquium

Im Rahmen des Kolloquiums spricht: **GD–Prof. Dr. Oleg Bogopolski**
z. Z. Universität Dortmund

über das Thema: **A short proof of Agrawal–Kayal–Saxena theorem: "PRIMES is in P"**

Abstract: In seinem ersten Buch "Disquisitiones Arithmeticae" (1801), hat C.F. Gauß geschrieben: "*Das Problem des Unterscheidens von Primzahlen und zusammengesetzten Zahlen, und das Zerlegen von großen Zahlen in ihre Primfaktoren, ist eine der wichtigsten und interessantesten Aufgaben der Arithmetik.*" Jetzt können wir dazu sagen, dass die zwei Probleme eine zentrale Stelle nicht nur in der algorithmischen Zahlentheorie, sondern auch in der Kryptographie einnehmen. In dem Vortrag wird das erste Problem besprochen:

Wie kann man schnell erkennen, ob eine gegebene natürliche Zahl eine Primzahl ist?

Es gibt einen sehr schnellen Miller–Rabin Primzahlentest, der es ermöglicht die Zahlen mit 10 000 Ziffern zu untersuchen. Dieser Test ist probabilistisch, deshalb gibt er nicht immer richtige Antworten. 2002 haben die drei indischen Mathematiker Manindra Agrawal, Neeraj Kayal und Nitin Saxena einen Artikel "PRIMES is in P" veröffentlicht. Der AKS–Test ist deterministisch und polynomial. Das heißt, dass er immer richtige Antworten gibt und in einer polynomialen Zeit läuft.
In dem Vortrag wird eine einfache Erklärung des AKS–Tests gegeben und es werden neue Hypothesen besprochen.

Termin: Montag, **13. November 2006, 17:00 Uhr**
Ort: Hörsaal, M E28
Kaffee/Tee: 16:30 Uhr, Raum M 614/616

Zu diesem Vortrag laden die Dozenten der Mathematik ein.