SS 09

Seminar der WE AℓZAGK

Do 8:30 - 10:00 in MZH 7200

Die Verfahren zur PrimzahlErkennung sind mittlerweile so weit entwickelt worden, daß es eine Routineaufgabe ist, bei Zahlen von einigen Tausend Dezimalstellen den Nachweis zu führen, daß sie Primzahlen sind.
Von besonderem theoretischen Interesse ist dabei das Resultat einer Gruppe indischer Wissenschaftler

> *M. Agrawal, N. Kayal, N. Saxena*: „Primes is in P“
> Annals of Math. 160 (2004), 781-793

die zum ersten Mal einen Primzahltest vorstellten, dessen Laufzeit polynomial ist: die Behandlung einer Zahl n erfordert eine Laufzeit von höchstens $(\log n)^{12+o(1)}$.
Natürlich gibt es inzwischen eine ganze Reihe von Verbesserungen, zuletzt:

> *J.-M. Couveignes, T. Ezome, R. Lercier*:
> “Elliptic periods and primality proving„,
> arXiv: 0810.2853v3 (7.02.2009).

Im SS 09 werden wir uns zunächst orientieren an

> *R. Schoof*: „Four primality testing algorithms“
> in „Algorithmic Number Theory“, MSRI Publications 44 (2008)

und dann den o.g. Artikel von Couveignes et al studieren, unter wesentlicher Benutzung von

> *J.M. Couveignes, R. Lercier*: „Elliptic periods for finite fields“
> in „Finite Fields and their Applications“, Juni 2008.

Es können Seminarscheine zum Bereich II erworben werden. Näheres bei:

J. Gamst, Di., 10:00-12:00 in MZH 7110
gamst@math.uni-bremen.de