WS 2011/12

Seminar der WE AℓZAGK

Di 8:30 - 10:00 in MZH 7200

Unser Gegenstand im kommenden Semester sind
Algebraische Dynamische Systeme

Für uns wird ein Dynamisches System zunächst einfach gegeben sein durch eine Abbildung T:M $\to$ M einer Menge M in sich, bei der man sich für Fixpunkte oder allgemeiner periodischen Punkte x von T interessiert, d.h mit $T^n(x) = x$.
Unter diesen Gesichtspunkt kann man einige Faktorisierungsverfahren subsumieren.
Bei der Pollardschen „Rho-Methode“ z.B, mit der die Primfaktoren einer Zahl n=pq gefunden werden sollen, hat man $M = \mathbb{Z}/n\mathbb{Z}$, und T ist gegeben durch ein Polynom mit ganzen Koeffizienten.
Mit einem Startwert x_0 bildet man die Folge $x_i = T^i(\alpha_0)$ und erreicht schliesslich einen Zyklus $x_k, x_{k+1}, x_{k+l} = x_k$.
Man berechnet daher die ggT$(x_i - x_j, n)$ und hofft, dass die Periodizität schon mod p oder mod q auftritt, sodass der obige ggT dann ein echter Teiler von n ist.
Die ersten Vorträge beziehen sich auf neuere Arbeiten zur Periodenlänge von $x \to x^2 + c$ über $\mathbb{F}_q$ oder $\mathbb{Z}/n\mathbb{Z}$ mit n=pq.
Im weiteren Verlauf des Seminars behandeln wir einen Übersichtsartikel von H. Niederreiter und I. Shparlinski und skizzieren dann einen allgemeinen Rahmen der Theorie nach einem Buch von J. Silverman
Wenn Zeit bleibt, sehen wir uns auch Anwendungen in der diophantischen Analysis nach einem Kurs von M. Waldschmidt an.
Literaturangaben und Vortragsplan findet man auf der AℓZAGK Seite.
Es können Seminarscheine zu Bereich I oder zu Bereich II erworben werden.

Näheres bei:

- Jens Gamst, Di 10-12 Uhr in MZH 7110, mail: *gamst@math.uni-bremen.de*
- Michael Hortmann, nach Vereinb. in MZH 6160, mail: *michael.hortmann@math.uni-bremen.de*