SS 2011

Seminar der WE Aℓ ZAGK

Di 8:30 - 10:00 Uhr in MZH 7200

Im kommenden Semester beschäftigen wir uns an Hand der Habilitationsschrift von C. Diem:

> „On the arithmetic and the discrete logarithm problem in class groups of curves“

mit einem Algorithmus für das Diskrete Logarithmus Problem auf elliptischen Kurven über Erweiterungskörpern endlicher Körper $\mathbb{F}_q$, der subexponentielle Laufzeit hat.

Der Algorithmus ordnet sich in den allgemeinen Rahmen der „IndexKalkülMethode“ ein, wir beginnen daher mit grundsätzlichen Bemerkungen zu dieser Methode und dem Resultat, daß man damit das Diskrete Logarithmus Problem in $\mathbb{F}_p^*$ in subexponentieller Laufzeit lösen kann.

Im weiteren Verlauf des Seminars folgen wir im wesentlichen dem Abschnitt 3.5 der Schrift von C. Diem. Die dafür nötigen Kenntnisse über elliptische Kurven und aus der Algebraischen Geometrie werden ohne Beweise hingenommen.

Ein Vortragsplan mit Literaturliste findet sich auf der AℓZAGK Seite.

Näheres bei

Jens Gamst, Di 10-12 Uhr in MZH 7110, mail: *gamst@math.uni-bremen.de*