ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Abteilung für Reine Mathematik

Seminar:	**Elliptische Kurven**
Dozent:	**Dr. Urs Hartl**
Zeit/Ort:	**Mo 14-16 Uhr, SR403**
Vorbesprechung:	**Montag 9.2.2004, 14:00 Uhr, Raum 425, Eckerstraße 1**
Web-Seite:	http://home.mathematik.uni-freiburg.de/hartl/Lehre.html

---

Inhalt:
Dieses Seminar schließt sich an die Vorlesung „Algebraische Geometrie II" aus dem Wintersemester 2003/2004 an, die einen Einstieg in die Theorie der elliptischen Kurven, sowie die Theorie der Schemata bot.
Das Studium von elliptischen Kurven soll nun hier fortgesetzt werden. Wir werden uns dabei insbesondere mit folgenden Themenbereichen beschäftigen:

- elliptische Kurven über den komplexen Zahlen,
- Reduktion von elliptischen Kurven,
- rationale Punkte auf elliptischen Kurven,
- Anwendung elliptischer Kurven in der Kryptographie.

Literatur:

1. J. Silverman: The Arithmetic of Elliptic Curves, LNM 106, Springer 1985.
2. A. Werner: Elliptische Kurven in der Kryptographie, Springer 2002.

Typisches Semester:	ab 6. Semester
Studienschwerpunkt:	Algebra
Notwendige Vorkenntnisse:	Algebraische Geometrie I, II (Teil: Elliptische Kurven)
Sprechstunde Dozent:	Mo 10-11 Uhr und nach Vereinbahrung