Syllabus: MAS 6396

Department of Mathematical Sciences
Charles E. Schmidt College of Science
Florida Atlantic University

Spring, 2007. MAS 6396, Elliptic Curves

Instructor
Rainer Steinwandt, Office SE 280
Phone: (561) 297-3353
Email: rsteinwa@fau.edu

Class Time and Place
Monday, Wednesday, Friday: 10:00 – 10:50 p.m., SE 215.

Office Hours
Monday, Wednesday, Friday: 2:00 p.m. – 3:30 p.m. or by appointment. Also, feel free to come to the office anytime—whenever time permits, questions and discussions are welcome. (If there should be any timing conflicts, like inevitable meetings during regular office hours, this will be announced beforehand in class, whenever possible.)

Course Web Site
http://www.math.fau.edu/~srainer/EllipticCurveClass/

Required Text and Materials
Most of the material will be taken from the book *Elliptic Curves: Number Theory and Cryptography* (Lawrence C. Washington, Chapman & Hall/CRC, 2003). If supplementary material is necessary, this will be distributed in class or on the course web site as needed.

Course Objectives
The course assumes familiarity with elementary concepts from algebra, as covered by an introductory algebra course, for instance. After completion of this course you should be acquainted with the basic definitions and results from the theory of elliptic curves. You should understand and be able to explain essential algebraic properties of elliptic curves over fields of different characteristics. Moreover, after completion of this course, you should know how to perform basic algorithmic tasks related to elliptic curves—like computing in a group defined by an elliptic curve, evaluating a Weil pairing or counting the number of points on an elliptic curve.
**Lecture Schedule**

Where possible, suggestions of course participants for topics of particular interest will be taken into account. The topics I intend to cover are listed below, and the exposition will mainly follow the respective part of Washington’s book mentioned in the above section on required texts and materials. The exact time frame per item varies (also in dependence of previous knowledge of the course participants), but a typical time frame is two weeks per item.

1. Basic theory of elliptic curves
2. Torsion points
3. Elliptic curves over finite fields
4. Elliptic curves over the rational numbers
5. Complex multiplication
6. Divisors
7. Zeta functions

**Assessment Procedures**

There will be two homework projects $X_1$, $X_2$ and one exam $X_3$. Both homework projects and the exam will be assigned in class and collected on the date specified on the assignment. The scheduled assignment dates and maximum number of points for the items $X_1$, $X_2$ and $X_3$ are listed in the following table.

<table>
<thead>
<tr>
<th>Item</th>
<th>Date</th>
<th>Max. points</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_1$</td>
<td>Sep 17, 2007</td>
<td>35</td>
</tr>
<tr>
<td>$X_2$</td>
<td>Oct 22, 2007</td>
<td>35</td>
</tr>
<tr>
<td>$X_3$</td>
<td>Nov 28, 2007</td>
<td>30</td>
</tr>
</tbody>
</table>

Homework projects or an exam returned after the specified deadline will not be accepted and graded with 0 points.

Both homework projects and the exam will be returned in class or can be picked up during office hours at the instructor’s office. At the end of the course, the final grades will be available at the instructor’s office (room SE 280). Please keep your exam and documentation of homework projects, so that a possible disagreement about your grade can be resolved.

Your overall grade in the course is derived from your cumulative performance as follows:

1. The points from the items $X_1$, $X_2$ and $X_3$ are added, yielding a final number of points $0 \leq P \leq 100$.
2. Your grade is derived from $P$ according to the following table.
<table>
<thead>
<tr>
<th>Value of $P$</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt; 94</td>
<td>A</td>
</tr>
<tr>
<td>&gt; 90 – 94</td>
<td>A−</td>
</tr>
<tr>
<td>&gt; 87 – 90</td>
<td>B+</td>
</tr>
<tr>
<td>&gt; 83 – 87</td>
<td>B</td>
</tr>
<tr>
<td>&gt; 80 – 83</td>
<td>B−</td>
</tr>
<tr>
<td>&gt; 75 – 80</td>
<td>C+</td>
</tr>
<tr>
<td>&gt; 65 – 75</td>
<td>C</td>
</tr>
<tr>
<td>&gt; 60 – 65</td>
<td>C−</td>
</tr>
<tr>
<td>&gt; 57 – 60</td>
<td>D+</td>
</tr>
<tr>
<td>&gt; 53 – 57</td>
<td>D</td>
</tr>
<tr>
<td>≥ 50 – 53</td>
<td>D−</td>
</tr>
<tr>
<td>&lt;50</td>
<td>F</td>
</tr>
</tbody>
</table>

**Make-up Tests and Extra Credit**
If you cannot attend the exam or hand in a homework project due to a relevant reason like significant health problems or being involved in a major traffic accident, you can make up the respective item. Extra credit work is not possible.

**Course Procedure**
The course is conducted in lecture/discussion style.

**Students with Disabilities**
In compliance with the Americans with Disabilities Act (A.D.A.) – Students who require special accommodations due to a disability to properly execute coursework must register with the Office for Students with Disabilities (OSD) located in Boca – SU 133 (561-297-3880), in Davie – MOD I (964-236-1222), or in Jupiter – SR 117 (561-799-8585) and follow all OSD procedures.

**Incomplete Grades**
A grade of $I$ (incomplete) will only be given under certain conditions and in accordance with the academic policies and regulations put forward in FAU’s *Graduate Policies and Procedures Manual* (see http://www.fau.edu/graduate/pubs/pol.pdf). The student has to show exceptional circumstances why requirements cannot be met. A request for an incomplete grade has to be made in writing with supporting documentation, where appropriate.

**Classroom Etiquette and Academic Integrity**
Please refer to the guidelines for good practice in graduate education in FAU’s *Graduate Policies and Procedures Manual* (see http://www.fau.edu/graduate/pubs/pol.pdf).