Number Theory, Finite Fields and Their Applications

Course Syllabus

Basic information

<table>
<thead>
<tr>
<th>Program of study</th>
<th>Applied Computing in Engineering and Science (Master’s Degree)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Semester</td>
<td>Third (Year 2)</td>
</tr>
<tr>
<td>Course credits</td>
<td>6 ECTS</td>
</tr>
<tr>
<td>Language</td>
<td>English level B1 / Intermediate</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>B.Sc. degree in Mathematics or Computer Science</td>
</tr>
</tbody>
</table>

Course Instructor

N.N. Osipov, D.Sc. in Mathematics, Web-pages:

https://scholar.google.ru/citations?user=P5Nn8-UAAAAJ&hl=en
http://www.mathnet.ru/eng/person/31746

Professor of Applied Mathematics and Computer Security Department, Siberian Federal University, Krasnoyarsk, Russia
Office: School of Space and Information Technology, office 3-11
E-mail: nosipov@rambler.ru

Required knowledge

The students who take this course should have basic knowledge of elementary number theory, linear and abstract algebra. Programming skills in any computer algebra system (e.g., Reduce, Maple, Mathematica, etc.) would help, but is not required.

Preliminary Reading:


Computing

Access to one of the computing algebra systems mentioned above is required in order to do the computer assignments. SFU has a license for educational use of Maple CAS.

Teaching

The course will be taught in lecture format along with class examples and demonstrations. Problem Sets (or Individual Tasks) will be assigned. At the end of semester the qualification (oral examination) will take place.

Course description

An exposition of major problems in computational number theory with emphasis on practical algorithms and their computational complexity. An application of finite field theory to cryptography and coding theory.
Course goal

The course is aimed to introduce some important and widely used algorithms in computational number theory and finite fields theory with their applications (cryptography, coding theory).

Course objectives

The objectives of the course are:

1. to give students a detailed description of the main modern algorithms in computational number theory;
2. to implement all the algorithms and methods introduced in the course on a computer using a computer algebra system;
3. to make students familiar with basic properties and techniques of finite fields and their application to cryptography and coding theory.

Learning Outcomes

At the end of the course, the student will be able:

- to use the modern algorithms in computational number theory for searching information in targeted areas (cryptography, coding theory);
- to use symbolic software packages to perform number-theoretic computations;
- to apply these methods to academic and simple practical instances.

Outline of content

1. Algorithms for primality testing
2. Algorithms for integer factorization
3. Finite fields and polynomials
4. Algorithms for discrete logarithms
5. Public-key cryptography
6. Algebraic coding theory

Collaborative Work

Many people learn more effectively when they study in small groups and cooperate in various other ways on homework. We are very much in favor of this kind of cooperation so long as all participants actively involve themselves in all aspects of the work. When you hand in a paper with your name on it we assume that you are certifying it as your (joint) work and that you were involved in all aspects of it. Even if you work with others you should do its writing separately, and you should indicate the names of any collaborators for each part of it. However, we encourage you to make the final project a team effort with a joint presentation and write up, so please try to find collaborators early in the term for this work.

Course assessment

Note: Assessments subject to change. Below there is a tentative version of assessments. The final version will appear prior to start of the course.
<table>
<thead>
<tr>
<th>Assessment Type</th>
<th>Number per semester</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem Sets</td>
<td>6</td>
<td>50%</td>
</tr>
<tr>
<td>Essay</td>
<td>1</td>
<td>20%</td>
</tr>
<tr>
<td>Final Exam</td>
<td>1</td>
<td>30%</td>
</tr>
</tbody>
</table>

### Attendance Policy

Students are expected to attend classes regularly, since the consistent attendance offers the most effective opportunity open to all students to gain command of the concepts and materials of the course. Meanwhile, excuses of various origin are permissible, in such a case students take a consultation and do the necessary class-work at home (or at their own). Such “hidden extramural” activity must not exceed a quarter of the total course time.

### References


### Academic Honor Policy / Academic Honesty:

The Siberian Federal University is built upon a strong foundation of integrity, respect and trust. All members of the university have a responsibility to be honest and the right to expect honesty from others. Any form of academic dishonesty is unacceptable to our community.

### Note

The Course Instructor reserves the right to make changes to this syllabus as necessary prior to start of the course.