Syllabus for the course "Number Theory"

Area of Specialisation: 01.06.01 Mathematics and Mechanics
Doctoral programs in

01.01.02 Differential Equations, Dynamic Systems and Optimal Management
01.01.03 Mathematical Physics
01.01.04 Geometry and Topology
01.01.05 Probability Theory and Mathematical Statistics
01.01.06 Mathematical Logics, Algebra and Theory of Numbers

Approved by the Academic Council of the Doctoral School in Mathematics
on 24th October, 2017

Moscow - 2017

Syllabus

1. Course Description
    a. Title of a Course: Number Theory
    b. Pre-requisites: basic abstract algebra (linear algebra, rings, groups, the Galois
    c. theory) and elementary complex analysis
    d. Course Type: optional
    e. Abstract

The beginnings of number theory can be traced to Diophantine equations: polynomial equations such that only the integer solutions are sought or studied. Surprisingly this is a highly structured part of mathematics: there are general results and conjectures, which have many concrete nontrivial corollaries. Number theory uses tools from algebra, analysis, and topology.

2. Learning Objectives

The course covers some of the most important results obtained by the beginning of the 20th century.

3. Learning Outcomes

Students will learn the basics of contemporary number theory

4. Course Plan

• Finite fields
• Integers represented by binary quadratic forms
• Quadratic reciprocity law
• Division rings over number fields
• The ideal class group
• Dirichlet's theorem on units in number fields
• Local fields
• Hasse-Minkowski theorem
• Dirichlet's theorem on primes in arithmetic progressions
• Analytic class number formula

5. Reading List
    a. Required

    R. Ash, A Course In Algebraic Number Theory

    https://faculty.math.illinois.edu/~r-ash/ANT.html

    b. Optional

Algebraic Number Theory, a Computational Approach, http://www.freetechbooks.com/algebraic-number-theory-a-computational-approach-t992.html

6. Grading System

The final grade is computes as 0.5(homeworks)+0.5(final exam). The grade is rounded to the nearest integer; half-integers are rounded up.

7. Guidelines for Knowledge Assessment

Examples of homework problems:

1. (a) Let $K \supset \mathbb{Q}$ be a finite extension, $O_K \subset K$ the maximal order, r_2 the number of complex (not real) embeddings $K \hookrightarrow \mathbb{C}$ up to complex conjugation, $K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R}$. Prove that

$$Vol(K_{\mathbb{R}}/O_K) = 2^{-r_2}\sqrt{Disc(K/\mathbb{Q})}.$$

Here $Disc(K/\mathbb{Q})$ stands for the discriminant of the extension. (Note, the $\mathbb{R}$-algebra $K_{\mathbb{R}}$ is isomorphic to $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ and that the induced from $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ volume form does not depend on the choice of this isomorphism. Therefore the expression $Vol(K_{\mathbb{R}}/O_K)$ makes sense.)
(b) Prove that every finite extension $K \supset \mathbb{Q}$ of degree greater than 1 is ramified at least over one prime. [1] (Hint: Use the Minkowski Lemma and part (a).)

2. Let $p > 2$ be a prime number, μ_p a p-th primitive root of 1 in $\mathbb{C}$.
(a) Show $\mathbb{Z}[\mu_p] \subset \mathbb{Q}(\mu_p)$ is the maximal order and that the extension $\mathbb{Q}(\mu_p) \supset \mathbb{Q}$ is unramified except over prime p.
(b) For each $l \neq p$ compute the Frobenius element $F_l \in Gal(\mathbb{Q}(\mu_p)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/p)^*$.

3. (a) Let $f(x)$ be a monic polynomial of degree n with integral coefficients which has no multiple complex roots, D the discriminant of $f(x)$, and let $K \supset \mathbb{Q}$ be the splitting field of $f(x)$. The Galois group $Gal(K/\mathbb{Q})$ acts on the set of roots of $f(x)$ and this action defines an embedding $Gal(K/\mathbb{Q}) \subset S_n$.
(a) Show that if p does not divide D then K is unramified over p.
(b) Assume that p does not divide D. Let $\overline{f}(x) = \overline{f}_1(x) \cdots \overline{f}_l(x)$ be the factorization of the reduction of $f(x)$ modulo p into a product of irreducible polynomials. Let d_i be the degree of $\overline{f}_i(x)$. Prove the cycle type of the Frobenius element F_p regarded as a conjugacy class in S_n is $(d_1, \cdots, d_l)$.

8. Methods of Instruction

Introductory talks, problem sessions and self-study.

9. Special Equipment and Software Support (if required)

No requirements.

Competences to be developed: UK-1, 2, 5, PK-1, OPK-1, 2 (according to *01.06.01 Mathematics and Mechanics* Educational Standard).