School of Mathematics

Module MA2317 — Introduction to number theory 2010-11
(SF & JS Mathematics, JS & SS Two-subject Moderatorship)

Lecturer: Dr. Vladimir Dotsenko

Requirements/prerequisites: basics of linear algebra and group theory from the first year (MA1212, MA1214).

Duration: Michaelmas term, 11 weeks

Number of lectures per week: 3 lectures including tutorials per week

Assessment: 30%*continuous assessment + 70%*final exam mark or 100%*final exam mark, whichever is higher

ECTS credits: 5

End-of-year Examination: 2 hour examination in Trinity term.

Description:

The ultimate goal of this course is to introduce the students to most of the basic concepts of number theory, at the same time demonstrating interactions of number theory with other areas of maths and giving an overview of number-theoretic methods and results of contemporary mathematics. This ambitious goal is achieved through combining rigorous proofs with only hints on proofs and even just vague ideas in some cases, the latter being more of a roadmap for future studies rather than an examinable material. The course will be accompanied by bi-weekly tutorials in the form of problem-solving sessions. The only prerequisites are basic linear algebra (vector spaces, dimensions) and group theory from the first year. Recommended reading consists of (selected chapters from) books [1,2,3,4,5] below.

1. Euclid's algorithm. Linear Diophantine equations and Frobenius's problem. Fundamental theorem of arithmetic.

2. Infinitude of primes. Number theory meets analysis: Bertrand's postulate, more on distribution of primes, primes in arithmetic sequences.

3. Modular arithmetic. Fermat's little theorem. Euler's theorem. Chinese Remainder Theorem. Quadratic residues. Quadratic reciprocity law.

4. Number theory meets computer science and cryptography: the Agrawal–Kayal–Saxena primality test and the Rivest–Shamir–Adleman algorithm.

5. Euler's totient function. Number theory meets combinatorics: Möbius inversion and its applications.

6. Polynomials over a field. Gauss's lemma. Eisenstein's criterion. Dumas's criterion.

7. Cyclotomic polynomials and applications: primes in the arithmetic sequence $a_n = dn+1$; Wedderburn's little theorem.

8. Algebraic numbers. Liouville's theorem and examples of transcendent numbers.

9. Number theory meets algebraic geometry: Pythagorean triples. More on Diophantine equations: $n = 4$ case of Fermat's last theorem, Markov's equation etc.

10. Fermat's last theorem for polynomials. What breaks for integers? (Mistakes of Cauchy and Lamé, Kummer's ideal numbers.) The *abc*-conjecture.

11. Number theory meets topology: p-adic numbers, Ostrowski's theorem, Hensel's lemma and applications.

References

[**1**] H. Davenport, *The higher arithmetic*, Cambridge University Press, Cambridge, 2008.

[**2**] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press, Oxford, 2008.

[**3**] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990.

[**4**] Serge Lang, *Math talks for undergraduates*, Springer-Verlag, New York, 1999.

[**5**] Victor V. Prasolov, *Polynomials*, Algorithms and Computation in Mathematics, vol. 11, Springer-Verlag, Berlin, 2004.

Learning Outcomes: On sucessful completion of this module, students will be able to:

- apply the Euclidean algorithm to solve linear Diophantine equations in the case of integers, Gaussian integers, and polynomials;
- reproduce various proofs of the infinitude of primes, and their minor modifications;
- use modular arithmetic to derive theoretical results (e.g. every number is congruent modulo 9 to the sum of its digits, Fermat's little theorem, Euler's theorem);
- apply the Chinese Remainder Theorem to theoretical (e.g. values of the Euler function) and practical (e.g. systems of simultaneous linear congruences) problems;
- apply the Quadratic Reciprocity Law to compute various Legendre symbols, and use theorems on quadratic residues to prove particular cases of Dirichlet's theorem for primes in arithmetic sequences;
- demonstrate that a given polynomial is irreducible over integers;
- prove that a given number is algebraic, and use Liouville's theorem to analyse the Diophantine approximations of a given number (in particular, prove that a given number is transcendental);

- classify all Pythagorean triples (and solutions to similar equations), and use the infinite descent method to prove that a given equation has no integer solutions;
- apply Hensel's lemma to solve polynomial congruences modulo prime powers.

December 9, 2010