

# MA2317: INTRODUCTION TO NUMBER THEORY

VLADIMIR DOTSENKO

**Overview.** 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 transcendental 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.

**Homeworks, assessment etc.** There will be several home assignments, each for a week or two weeks, depending on the topic covered. The final mark for the course will be 30% of the continuous assessment plus 70% of the final exam mark, or the final exam mark, whichever is higher.

## 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.