Number Theory

MATH 30200

Lecturer: Professor Alexander Gorodnik
Email: <a.gorodnik@bristol.ac.uk>
Office: Howard House 5a

Course Webpage: http://www.maths.bris.ac.uk/~mazag/nt/

Class Times: Monday 5-6pm at Chemistry Building: West Block Lecture Theatre 4
Wednesday 9-10am at Maths Building: SM1
Friday 2-3pm at Maths Building: SM1

Office hours: Monday 4-5pm and by appointment

Prerequisites: MATH11511 "Number Theory and Group Theory"
MATH11006 "Analysis 1"

Course Description: Number theory is a thriving and active area of research whose origins are amongst the oldest in mathematics; some questions asked over two thousand years ago have not been fully answered yet. Despite this ancient heritage, it has surprisingly contemporary applications, underpinning the internet data security that lies at the heart of the Digital Age. Although at the core of number theory one finds the basic properties of the integers and rational numbers, the subject has developed coherently in many directions as it has been influenced by (and indeed as it in turn influences) partner disciplines. Almost every conceivable mathematical discipline has played a role in this development, and indeed this web of interactions encompasses Algebra and Algebraic Geometry, Analysis, Combinatorics, Probability, Logic, Computer Science, Mathematical Physics, and beyond.

At the end of the unit you will acquire a command of the basic tools of number theory as applicable to the investigation of congruences, arithmetic functions, Diophantine equations and beyond. In addition, you will become familiar with the underlying themes and current state of knowledge of several branches of Number Theory and its interaction with partner disciplines.

Syllabus: Topics covered will include:

1. Revision of the basic properties of the integers including the Euclidean algorithm.
2. Number-theoretic functions, especially the Möbius and Euler functions. Averages and maximum values.
3. Congruences, including the theorems of Fermat, Euler, and Lagrange, and computational applications. The RSA cryptosystem.
4. Primitive roots and the structure of the residues modulo m.
5. Polynomial congruences to prime powers. Hensels lemma and the p-adic numbers.
6. The quadratic residue symbols of Lagrange and Jacobi. Quadratic reciprocity.
7. The solution of quadratic equations in integers.

8. Introduction to one or more of the following topics, depending on time available: Diophantine approximation and transcendence, continued fractions, Dirichlets theorem on primes in arithmetic progressions, Diophantine equations and elliptic curves.

Homework: Homework problems will be assigned and collected bi-weekly. The first homework assignment is collected in Week 2. Although the homeworks are not a part of the course assessment, it is essential to do them regularly to prepare for the exam.

Math Cafe: A convenient place to work on the number theory homeworks is Math Cafe on Tuesday 9-10am at Portacabin 4, run by Demmas Salim <ds13187@bristol.ac.uk>.

Course Assessment: The final assessment mark for the unit is calculated from a standard 2.5-hour written closed-book examination in May-June. Calculators are NOT permitted in this examination. Raw scores on the examinations will be determined according to the marking scheme written on the examination paper. The marking scheme, indicating the maximum score per question, is a guide to the relative weighting of the questions. The pass mark for this unit is 40.

References: There is no unique recommended text for this course. Useful references are:

1. Alan Baker, A concise introduction to the theory of numbers. Cambridge University Press, 1984.

2. Ivan Niven, Herbert S. Zuckerman and Hugh L. Montgomery, An introduction to the theory of numbers. Fifth edition. John Wiley & Sons, Inc., 1991.

3. H. E. Rose, A course in number theory. Second edition. Oxford Science Publications. The Clarendon Press, Oxford University Press, 1994.

4. J. H. Silverman, A friendly introduction to number theory. Third edition. Prentice Hall, 2005.