ELEMENTARY NUMBER THEORY

JEANINE VAN ORDER

Scope

The course will be a motivated introduction to the theory of numbers, with historical perspective, aimed at undergraduate and graduate students alike. The lectures will be given in Portuguese, and aimed primarily at undergraduate students (of all backgrounds). The main text will be Baker's monograph [1], cross-referenced with various instructive examples and problems from [3], [4], [5], and also [2]. Extra references will be presented for general culture and further self-study, together with non-examinable material on diophantine equations, p-adic numbers, and some applications to cryptography. There will also be weekly problems sets, as well as a written final exam.

Topics outline

Each topic should take two or three lectures to cover, and the tentative plan leaves flexibility to devote more time to certain topics according to the interests and strengths of the students.

(1). Divisibility. Foundations, the division algorithm, the Euclidean algorithm, the greatest common divisor, the fundamental theorem of arithmetic, some properties of prime numbers, and some open problems.

(2). Arithmetic functions. The function $[x]$, multiplicative functions, the Euler φ function, the Möbius function and the inversion formula, the functions $\tau(n)$ and $\sigma(n)$, average orders, perfect numbers, and the Riemann zeta function.

(3). Congruences. Definitions, the Chinese Remainder Theorem, theorems of Fermat and Euler, Wilson's theorem, Lagrange's theorem, primitive roots, and indices.

(4). Quadratic residues. The Legendre symbol, Euler's criterion, Gauss' lemma, the law of quadratic reciprocity, and the Jacobi symbol.

(5). Quadratic forms. Survey of equivalence relations, reduction, representations by binary quadratic forms, sums of two squares, and sums of four squares.

(6). Quadratic fields. Survey of algebraic number fields, quadratic fields, units, primes and their decompositions, Euclidean domains, and the Gaussian number field.

(7). Diophantine approximation. Survey of Dirichlet's theorem, continued fractions, rational approximation, quadratic irrationals, Liouville's theorem, transcendental numbers, and Minkowski's theorem.

(8). Further topics (non-examinable). (i) Diophantine equations: The Pell equation, the Thue equation, the Mordell equation, the Fermat equation – leading to work of Kummer and other modern developments. The congruent number problem. (ii) A motivated introduction to p-adic numbers: norms, Ostrowski's theorem, the product formula, the p-adic numbers as completions, the p-adic integers, Hensel's lemma, and the Hasse-Minkowski theorem. (iii) Applications to cryptography, e.g. primality testing, RSA encryption, and topics in elliptic curve cryptography such as elliptic codes.

References

[1] A. Baker, *A concise introduction to the theory of numbers*, Cambridge University Press (1984).

[2] J.-P. Serre, *Cours d'arithmétique*, Presses Universitaires de France (1977).

[3] M.R. Murty, *Problems in Analytic Number Theory*, Grad. Texts in Math., Springer **206** (2001).

[4] M.R. Murty and J. Esmonde, *Problems in Algebraic Number Theory*, Grad. Texts in Math., Springer **190** (2004)

[5] D.B. Zagier, *Zetafunktionen und quadratische Körper: Eine Einführung in die höhere Zahlentheorie*, Springer (1981).