

# Number Theory Final Exam topics

Márton Erdélyi, 2026

## 1. Order, primitive roots, quadratic residues

Order, primitive roots and discrete logarithm. Quadratic residues, Legendre and Jacobi symbol. Quadratic reciprocity. Cryptographic applications (the RSA algorithm).

## 2. Primes and their distribution

Riemann's zeta function. Prime Number Theorem, asymptotic for the  $n$ th prime. Dirichlet theorem. There is an arbitrary large gap between consecutive primes. Bertrand postulate/Chebyshev's theorem. Sum of reciprocals of primes and twin primes.

## 3. Gaussian integers and unique factorization

Divisors, units, primes and irreducibles in a domain. Gcd and Euclidean algorithm. Unique factorization. Characterization of Gaussian primes. Euclidean domains.

## 4. Diophantine equations

Parametrization of the Pythagorean triples. Fermat's last theorem in general and the case for the exponent 3 or 4. Representation of integers as sum of squares: theorems on sums of 2, 3 and 4 squares.

## 5. Combinatorial number theory

Schur's theorem. The van der Waerden theorem. The theorem of Szemerédi on arithmetic progressions. The Chevalley-Warning theorem. The Erdős-Ginzburg-Ziv theorem.