## Számelmélet 2/2/0/v/5

Tárgyfelelős: Rónyai Lajos
További oktatók: Wettl Ferenc, Lukács Erzsébet

Oszthatóság, euklideszi algoritmus, a számelmélet alaptétele. Kongruenciák, lineáris kongruenciák és lineáris diofantikus egyenletek, Euler-, Fermat- és Wilson-tétel, műveletek maradékosztályokkal. Magasabb fokú kongruenciák, primitív gyök, diszkrét logaritmus, hatványmaradék. Chevalley-tétel és alkalmazásai. Legendre-szimbólum, kvadratikus reciprocitás, Jacobi-szimbólum. Prímszámok eloszlása, Fermat- és Mersenne-prímek. Prímtesztek. Számelméleti függvények: Euler-függvény, Möbius-függvény, Möbius-féle inverziós formula. Diofantikus egyenletek, pitagoraszi számhármasok. Gauss-egészek, számok négyzetösszegként való előállításai. A számelmélet alkalmazásai, RSA algoritmus.

Irodalom:
Freud R., Gyarmati E.: Számelmélet. Tankönyvkiadó, 2000.
I. Niven, H. S. Zuckerman: Bevezetés a számelméletbe. Műszaki Könyvkiadó, 1978.
I. M. Vinogradov: A számelmélet alapjai. Tankönyvkiadó, 1968.

## Number theory 2/2/0/v/5

Course coordinator: Lajos Rónyai
Other instructors: Ferenc Wettl, Erzsébet Lukács

Divisibility, Euclidean algorithm, the fundamental theorem of number theory, congruences, linear congruences and linear diophantine equations, Euler's, Fermat's and Wilson's theorems, operations with residue classes. Congruences of higher degrees, primitive root, discrete logarithm, power residue. Chevalley's theorem and its applications. Legendre symbol, quadratic reciprocity, Jacobi symbol. Distribution of prime numbers, Fermat and Mersenne primes. Prime tests. Arithmetic functions: Euler function, Möbius function, Möbius inversion theorem. Diophantine equations, Pythagorean triples. Gaussian integers, decomposition of numbers into quadratic sums. Applications of number theory, the RSA algorithm.

References:
Freud R., Gyarmati E.: Számelmélet. Tankönyvkiadó, 2000.
I. Niven, H. S. Zuckerman: Bevezetés a számelméletbe. Műszaki Könyvkiadó, 1978.
I. M. Vinogradov: A számelmélet alapjai. Tankönyvkiadó, 1968.