## Algebrai és aritmetikai algoritmusok 3/1/0/f/5

Tárgyfelelős: Nagy Attila
További oktatók: Horváth Erzsébet, Wettl Ferenc, Ivanyos Gábor

Alapvető módszerek: műveletek egész számokkal, polinomokkal, mátrixokkal. A véges Fourier-transzformáció és alkalmazásai, a bilineáris bonyolultság elemei. Kínai maradéktétel, moduláris aritmetika. Prímtesztelés. Algoritmusok egész számok felbontására és a diszkrét logaritmus-feladatra. Kriptográfiai alkalmazások. Polinomok hatékony felbontása véges testek és algebrai számtestek felett. Elliptikus görbék, alapvető algoritmusok, ezek alkalmazásai. Moduláris algoritmusok és interpoláció. Hermite, Cauchy, Padé approximáció. Gröbner bázisok.
Irodalom:
Iványi Antal: Informatikai algoritmusok (Algebra, Komputer algebra, Számelmélet fejezetek)

## Algebraic and arithmetical algorithms 3/1/0/f/5

Course coordinator: Attila Nagy
Other instructors: Erzsébet Horváth, Ferenc Wettl, Gábor Ivanyos

Fundamental methods: operations with integers, polynomials, matrices. Fast Fourier transformation and applications. Elements of bilinear complexity. Chinese remainder theorem, modular arithmetic. Primality testing. Algorithms for factoring integers, and for discrete logarithms. Applications to cryptography. Efficient decomposition of polynomials over finite fields and algebraic number fields. Elliptic curves, their basic algorithms, applications. Modular algorithms and interpolation. Hermite, Cauchy, Padé approximation. Gröbner bases.

Reference:
Antal Iványi: Informatics algorithms (Sections: Algebra, Comuter algebra, Number theory)