Programtervező Informatikus MSc
Modellalkotó Informatikus szakirány

ELTE IK, Komputeralgebra Tanszék
Tantárgyi dokumentáció

TÁRGY NEVE: Algebrai geometriai számítások EA

TÁRGY KÓDJA: IPM-08modAGSZE

Összes kredit: 2

Összes óraszám: 2

Óra típusa	**előadás**	**gyakorlat**	**konzultáció**
Kredit	2		
Heti óraszám	2		
Számonkérés módja	K		

Tematika:

I. Algebrai alapok:

1. Csoportelmélet: 1.1. Véges Abel-csoportok alaptétele, 1.2. Kongruenciák, 1.3. Redukált maradékosztályok csoportja Z_m, 1.4. Kvadratikus kongruenciák, 1.4.1. Legendre-szimbólum, 1.4.2. Jacobi-szimbólum, 1.4.3. Kvadratikus reciprocitás, 1.5. Diszkrét logaritmus probléma különböző algebrai struktúrákban, 1.6. Karakterek, 1.6.1. Dirichlet karakterek.
2. Testek: 2.1. Test karakterisztikája, 2.2. Algebrai testbővítések, 2.3. Véges testek, 2.4. Kvadratikus testek.

II. Prímszámok:

3. Általánosított Riemann-sejtés, 3.1. Prímszámok eloszlása, 3.2. Riemann sejtései, 4. Szita algoritmusok, 5. Prímtesztek, 5.1. Valószínűségi prímtesztek, pszeudoprímek, 5.2. Egzakt prímtesztek, 5.3. Különleges prímek, prímkombinációk, 6. Prímfaktorizáció.

III. Elliptikus görbék:

7.1. Alapgondolatok, 7.1.1. Csoport törvény, 7.1.2. Projektív koordináták, 7.1.3. Elliptikus görbék (mod n), 7.2. Torziós pontok, 7.3. Elliptikus görbék véges test felett, 7.4. Prímtfaktorizáció elliptikus görbékkel, 7.5. Prímtesztelés elliptikus görbékkel, 7.6. Elliptikus görbék és kriptográfia, 8. Az ECPP tökéletesítése.

Irodalom:

Lawrence C. Washington: *Elliptic Curves* (Number theory and Cryptography)
Előkészületben: Farkas G., Kátai I.: *Algebrai geometriai számítások jegyzet*

Ajánlott irodalom:

David M. Bressoud: *Factorization and Primality Testing*
Paulo Ribenboim: *The Little Book of Bigger Primes*