SZÁMÍTÓGÉPES SZÁMELMÉLET

Vizsgatételek

1. Primek eloszlása. Ikerprímek. Bateman és Horn sejtése. Eratosztenész szitája.
2. Moduláris inverz euklideszi algoritmussal és bináris euklideszi algoritmussal. Általános szita, a szitálás dúsító hatása. Programozási problémák.
3. Próbaosztás. A prímosztók eloszlása. A prímosztók számának határeloszlása. Fermat módszere. Pollard ρ módszere.
4. Fermat tétele, Euler tétele, kínai maradéktétel. Gyors hatványozás. Pollard $p-1$ módszere és finomításai.
5. Fermat teszt. $\mathbb{Z}/n\mathbb{Z}$ nem nulla elemei ciklikus csoportot alkotnak, ha n prím. Legendre- és Jacobi-szimbólum, kiszámításuk és a kapcsolódó tételek: Euler tétele, Gauss reciprocitási tétele.
6. Soloway–Strassen-teszt, Miller–Rabin-teszt. Miller tétele. Lucas-teszt és finomításai.
7. Lucas-sorozatok és kiszámításuk. Riesel-teszt, Lucas–Lehmer-teszt. Williams $p+1$ módszere.
8. Fermat-számok, Mersenne-számok, egyéb speciális alakú prímek keresése. Példa prímtesztelésre és faktorizálásra. Prímszámkódolás.
9. Számok és polinomok aritmetikája. Gyors algoritmusok: Karacuba módszere, FFT-módszerek.
10. Elliptikus függvények, elliptikus integrálok. Számolás elliptikus görbéken.
11. Faktorizálás elliptikus görbékkel. Faktorizálás szita módszerekkel.
12. Prímtesztelés ellliptikus görbékkel.
13. Polinomfaktorizálás.

Typeset by $\mathcal{AMS}$-TEX