Tematika az Algebrai geometriai számítások c. tárgyhoz

2014. tavaszi félév

1. **Valószínűségi prímtesztek**
   Fermat-teszt. Soloway-Strassen teszt, Miller-Rabin teszt.

2. **Determinisztikus prímtesztek**
   Lucas teszt. Pocklington-Lehmer teszt, Proth teszt.

3. **Faktorizáció**
   Próbaosztás, Pollard ρ, Pollard $p-1$, Fermat faktorizációk, kvadratikus szita.

4. **Diszkrét logaritmus probléma**
   A diszkrét logaritmus probléma. Generikus algoritmusok, brute-force, Baby-step, giant-step algoritmus, Pollard ρ, Pohling-Hellman. Indexkalkulus.

5. **Elliptikus görbék, alapok**
   A görbék fogalma, rövid Weierstrasse egyenlet. Szinguláris görbék. Általános Weierstrasse egyenlet, és kapcsolata a rövid Weierstrasse egyenlettel. Csoportművelet a görbén. Projektív koordináták.

6. **Elliptikus görbék véges testek fölött**
   Görbék véges testek fölött. Hasse-Weil tétel. Görbék elemszáma. Frobenius leképzés a görbén. Torziópontok. Szuperszinguláris görbék. Bilineáris leképzések a torziócsoportból.

7. **Elliptikus görbék, diszkrét logaritmus probléma:**
   Diszkrét logaritmus probléma görbéken. MOV támadás. Kriptográdiai alkalmazások: Diffie-Hellman kulcscsere. Példa, mikor a DDHP könnyű. 3 személyes kulcscsere protokoll.

8. **Elliptikus görbék, titkosítási eljárások**
   ElGamal és ECDSA aláírás. ID alapú titkosítás.

9. **Elliptikus görbék, görbék mod n**
   Görbék mod n. Faktórizáció és determinisztikus prímteszt elliptikus görblkkel.