
Diszkrét modellek alkalmazásai

2. Minta ZH

1. Oldd meg a következő szimultán kongruencia-rendszert! (10 pont)

$$4x \equiv 2 \pmod{3}$$

$$9x \equiv 7 \pmod{11}$$

$$9x \equiv 6 \pmod{21}$$

2. Keress generátorokat modulo 11!

Mennyi lesz $\log_6 3, \log_4 7, \log_8 5, \log_2 9$ modulo 11? (10 pont)

3. Egy RSA titkosításnál legyen a két titkos prím $p = 29, q = 37$ és a titkosító exponens $e = 55$. Mi lesz a titkos kulcs? (d) (8 pont)

4. Egy RSA titkosításnál legyen a két titkos prím $p = 5, q = 17$ és a titkosító exponens $e = 19$. Ha a titkosított üzenet $c = 18$, akkor mi volt az eredeti üzenet? (10 pont)

5. Számítsd ki az Euklideszi algoritmussal az alábbi polinomok legnagyobb közös osztóját \mathbb{Z}_7 felett! (12 pont)

$$f(x) = -7x^6 + x^5 - 4x^4 + 16x^3 + 21x^2 - 11x + 8$$

$$g(x) = 5x^4 + 7x^3 - 19x^2 + 10x - 3$$