Diszkrét logaritmus

Feladatsor

Diszkrét modellek alkalmazásai

Matematikai kérdések

1. Számítsuk ki a következő moduláris hatványokat:
a) $2^{10} \bmod 3$; b) $3^7 \bmod 5$; c) $4^{123} \bmod 5$; d) $5^5 \bmod 7$.

2. Alakítsuk át a^{19}-t a gyorshatványozás módszerével.

3. Definiáljuk egy szám rendjét modulo m. Mennyi 3 rendje modulo 4?

4. Írjuk fel a kis Fermat-tételt. Adjunk rá egy példát egy 10 és 15 közötti modulussal.

5. Írjuk fel a Lagrange-tételt. Adjunk rá egy példát egy 10 és 15 közötti modulussal.

6. Definiáljuk a primitív gyök fogalmát. Primitív gyök-e a 2 modulo 3?

7. Definiáljuk a diszkrét logaritmus fogalmát. Mennyi $\operatorname{ind}_3 4 \pmod 5$?

8. Hogyan számítja ki a két fél a Diffie–Hellman-kulcscsere közös titkát?

9. Melyik matematikai problémát kellene megoldani a Diffie–Hellman-kulcscsere feltöréséhez?

Programozási feladatok

10. Írjunk függvényt, amely kiszámítja $a^n \bmod m$-et

a) ismételt szorzással, majd a végén *egyszeri* maradékképzéssel;

b) ismételt szorzással, *lépésenkénti* maradékképzéssel;

c) gyorshatványozással.

Ellenőrizzük az eredményt a `power_mod()` beépített függvénnyel.

11. Keressünk az $a = 6$ alapra és az $m = 11$ modulusra olyan n kitevőt, amelyre

a) az előző feladat a) része nem fut le gyorsan, de b) és c) igen;

b) az előző feladat a) és b) része nem fut le gyorsan, de c) igen.

12. Írjunk függvényt, amely kiszámítja egy adott $a \in \mathbb{Z}$ rendjét modulo p. Teszteljük az első néhány p prímszámra, és azon belül minden lehetséges a maradékra. Minden esetben ellenőrizzük, hogy a hatvány megfelel a rend definíciójának, valamint hogy az eredmény teljesíti a Lagrange-tételt.

13. Számítsuk ki a-nak a g-alapú diszkrét logaritmusát modulo p

a) lineáris kereséssel; b) a baby-step giant-step algoritmussal.

Teszteljük különböző p prímszámokra, g primitív gyökökre és előre kiszámolt hatványértékekre. Futtassuk le a $p = 12345678923$, $g = 2$ és $a = 9718522932$ értékekre is. Lefutnak-e ugyanezen p-re és g-re, de egy véletlen a-ra 1 és $p-1$ között?

14. Szimuláljuk a Diffie–Hellman-kulcscserét, azaz írjunk programot, amely mindkét fél műveleteit végrehajtja, majd kiszámítja a közös titkot mindkét módon, és ellenőrzi, hogy egyeznek-e. Próbáljuk ki egyrészt a $p = 23$ és a $g = 5$, másrészt a $p = 12345678923$ és a $g = 5$ értékekre.

15. a) Implementáljuk a következő pszeudovéletlenszám-generátort:

$$x_n := 48271^n x_0 \bmod 2147483647,$$

ahol x_0 tetszőleges kezdőszám. A generáláshoz olyan függvényt írjunk, amely az előző értékből (x_{n-1}) generálja a következő számot (x_n), az x_0 és az n ismerete nélkül.

b) Mennyire "véletlenek" az előállított számok? Ideális esetben a generált számok minden bitje 50%-50% valószínűséggel lesz 1 vagy 0. Generáljunk 1000 véletlen számot (x_1-től x_{1000}-ig), és készítsünk statisztikát a számok bitjeiről (kettes számrendszerbeli számjegyeiről), például:

```
 0. bit: 500 (0), 500 (1)
 1. bit: 491 (0), 509 (1)
[...]
30. bit: 511 (0), 489 (1)
```

(A kisebb számoknak, amelyeknek nincs 31 bitjük, a hiányzó bitjeit 0-nak tekintsük.)