

Moduláris aritmetika

(feladatsor)

Diszkrét modellek alkalmazásai

1. Egy bankszámlaszám kétszer vagy háromszor nyolc számjegyből áll. Minden helyes számlaszám megfelel a következő szabálynak: ha a számjegyeit megszorozzuk rendre az $1, 3, 7, 9, 1, 3, 7, 9, \dots$ számokkal, akkor ezek összege 0-ra végződik. Ez igaz külön az első 8 számjegyre és a maradék 8 vagy 16 számjegyre is.
 - a) Írjunk függvényt, amely eldönti, hogy egy számlaszám helyes-e (ezen szabály alapján).
 - b) Helyes-e a 10402196-50526765-81771006 szám? Ha nem, melyik részében van a hiba?
 - c) Meg tudjuk mondani, hogy melyik számjegy a hibás?
 - d) Írjunk függvényt, amely kap egy (potenciálisan hibás) számlaszámot és egy sorszámot, hogy melyik számjegy a hibás, és visszaadja a helyes bankszámlaszámot.
2. Írjunk függvényt, amely megoldja az $ax \equiv b \pmod{m}$ lineáris kongruenciát adott $a, b \in \mathbb{Z}$ és $m \in \mathbb{N}^+$ számokra. A visszatérési érték az összes megoldás listája legyen 0 és $m-1$ között. Kétféleképpen oldjuk meg:
 - a) kimerítő kereséssel (brute force);
 - b) a tanult módszerrel. (Ne használjuk a Sage egyenletmegoldó függvényeit, viszont az egyéb számelméleti függvényeket használhatjuk.)
 - c) Oldjuk meg a $30517578125x \equiv 33729082272 \pmod{99999999999}$ kongruenciát. Melyik módszer működik?
3. Írjunk függvényt, amely kiszámítja az $a \in \mathbb{Z}_m$ multiplikatív inverzét adott $m \in \mathbb{N}^+$ -ra. Ne használjuk a Sage egyenletmegoldó függvényeit és moduláris aritmetikáját, ill. ne használjunk kimerítő keresést. A bemenő és kimenő számok egész számok legyenek (ne maradékosztályok). Ha nem létezik az inverz, akkor a visszatérési érték semmi (**None**) legyen. Számítsuk ki 123456789 inverzét modulo 79590490282399.
4. Implementáljuk a kínai maradéktételt két kongruenciára, azaz írjunk egy függvényt, amely kiszámítja az $x \equiv a \pmod{m}$ és az $x \equiv b \pmod{n}$ kongruenciák közös megoldását. Legyen a paraméterezése hasonló, mint a `crt()` négy paramétere, viszont a `crt()`-vel ellentétben az eredményt maradékosztályként adjuk vissza, a megfelelő modulussal. Ha nincs megoldás, akkor **None** legyen a visszatérési érték. (Ne használjuk a `crt()`-t és a Sage egyéb egyenletmegoldó függvényeit.)