Kongruenciák

Feladatsor

Diszkrét modellek alkalmazásai

Matematikai kérdések

1. Definiáljuk a kongruencia fogalmát. Mutassuk be a definíciót egy példán az $m = 8$ modulusra.

2. Melyek igazak az alábbiak közül:
a) $1 \equiv 6 \pmod 3$, b) $3 \equiv 9 \pmod 6$, c) $10 \equiv 2 \pmod 4$, d) $2 \equiv -2 \pmod 5$?

3. Írjuk fel a maradékoszályokat modulo 3.

4. Mi a teljes maradékrendszer? Írjunk rá *két* példát modulo 6.

5. Oldjuk meg az alábbi lineáris kongruenciákat:
a) $3x \equiv 5\ (8)$; b) $6x \equiv 6\ (15)$; c) $12x \equiv 9\ (18)$; d) $21x \equiv 14\ (35)$; e) $100x \equiv 40\ (260)$.

6. Definiáljuk a moduláris inverz fogalmát. Adjunk rá egy példát, ahol a modulus $m = 5$.

7. Mikor létezik egy szám moduláris inverze? Mely számok invertálhatók modulo 8?

8. Számítsuk ki az alábbi a-k inverzét modulo m, ha van (mikor melyik módszerrel egyszerűbb?):
a) $a = 1, m = 3$; b) $a = 2, m = 3$; c) $a = 2, m = 5$; d) $a = 7, m = 10$; e) $a = 3, m = 6$;
f) $a = 2, m = 99$; g) $a = 17, m = 50$; h) $a = 27, m = 100$; i) $a = 34, m = 55$.

9. Oldjuk meg az alábbi kongruenciarendszereket:

a) $\begin{cases} x \equiv 2 \pmod 7 \\ x \equiv 5 \pmod 8; \end{cases}$ b) $\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 2 \pmod 5; \end{cases}$ c) $\begin{cases} x \equiv 3 \pmod{10} \\ x \equiv 5 \pmod 6; \end{cases}$

d) $\begin{cases} x \equiv 8 \pmod{10} \\ x \equiv 4 \pmod{15}; \end{cases}$ e) $\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 4 \\ x \equiv 1 \pmod 5. \end{cases}$

Programozási feladatok

10. Hány prímszám van 2800000-ig, amely kongruens 7-tel modulo 235?

11. 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) próbálgatással; b) a bővített euklideszi algoritmussal.

A visszatérési érték az összes megoldás listája 0 és $m-1$ között. Teszteléshez használhatjuk az 5-ös feladat kongruenciáit. Ezenkívül oldjuk meg a következő kongruenciát is:

$$30517578125x \equiv 33729082272 \pmod{999999999999}.$$

12. Írjunk függvényt, amely kiszámítja egy adott $a \in \mathbb{Z}$ szám inverzét modulo $m \in \mathbb{N}^+$ az alábbi módszerekkel. Ha nem invertálható, akkor `None`-t adjunk vissza.

a) Oldjuk meg egyszerű kereséssel (de ne keressük tovább, mint ameddig feltétlenül szükséges).
b) Oldjuk meg a bővített euklideszi algoritmussal.
c) Teszteljük a megoldásokat $m = 2$-től 100-ig minden modulusra és minden lehetséges számra.
d) Invertáljuk $a = 3$-at egyre nagyobb modulusokra: $m = 10, 100, 1000, \ldots$. Melyik módszerrel tudunk tovább menni?

13. a) Írjunk függvényt, amely eldönti, hogy egy bankszámlaszám helyes-e (az ellenőrzőösszeg alapján). Helyesek-e a következő számlaszámok:

- 10402196-50526765-81771006,
- 10700505-70347915-51300009?

b) Írjunk függvényt, amely kap egy (potenciálisan hibás) bankszámlaszámot és egy sorszámot 1-től 24-ig, hogy melyik számjegye hibás. Feltételezhetjük, hogy ez az egyetlen hibás számjegye (ha van egyáltalán). Adjuk vissza a helyes bankszámlaszámot. Oldjuk meg a feladatot két lényegesen különböző módon. Teszteléshez induljunk ki egy ismert helyes számlaszámból, és változtassuk meg (külön-külön) minden egyes számjegyét minden lehetséges módon.

14. Implementáljuk a kínai maradéktételt két kongruenciára, azaz írjunk függvényt, amely kiszámítja az $x \equiv a \pmod{m}$ és az $x \equiv b \pmod{n}$ kongruenciák közös megoldását. A `crt()`-hez hasonlóan négy paramétert várjon: a, b, m, n, de azzal ellentétben a visszatérési érték az (x, r) pár legyen, ahol x a (legkisebb nemnegatív) megoldás, és r a megoldás modulusa. Ha nincs megoldás, akkor `None`-t adjunk vissza. (Ne használjuk a `crt()`-t és a Sage egyéb egyenletmegoldó függvényeit.) Teszteljük a megoldást a 9-es feladat megfelelő példáira, és ellenőrizzük, hogy a megoldás valóban teljesíti az eredeti kongruenciákat.