Számelmélet

Bevezetés a számításelméletbe 1
10. gyakorlat

Definíció

Legyenek $a, b, m \in \mathbb{Z}$, $m > 0$ tetszőlegesek. Azt mondjuk, hogy a kongruens b-vel modulo m, ha $m \mid b - a$ (azaz a és b azonos maradékot ad m-mel osztva). Ennek a jele $a \equiv b \pmod{m}$.

Tétel

Legyenek $a, b, c, d, m, k \in \mathbb{Z}$, $m > 0$, $k \geq 1$ tetszőlegesek. Ha $a \equiv b \pmod{m}$ és $c \equiv d \pmod{m}$, akkor az alábbiak teljesülnek.

1. $a + c \equiv b + d \pmod{m}$
2. $a - c \equiv b - d \pmod{m}$
3. $ac \equiv bd \pmod{m}$
4. $a^k \equiv b^k \pmod{m}$

Tétel

Legyenek $a, b, c, m \in \mathbb{Z}$, $m > 0$ tetszőlegesek, és legyen $d = (c, m)$. Ekkor

$$ac \equiv bc \pmod{m} \qquad \Longleftrightarrow \qquad a \equiv b \pmod{\frac{m}{d}}.$$

Tétel

Az $ax \equiv b \pmod{m}$ lineáris kongruencia akkor és csak akkor oldható meg, ha $(a, m) \mid b$. A kongruencia megoldáshalmaza (a, m) darab maradékosztály modulo m.

Ekvivalens átalakítások

- Mindkét oldalhoz hozzáadunk ugyanannyit.
- Az egyik oldalhoz hozzáadjuk m egy többszörösét.
- A modulushoz relatív prímmel szorzunk.
- Ha mindkét oldal osztható ugyanazzal a számmal, akkor ezzel a számmal leoszthatunk, de a modulust a fenti tétel szerint változtatnunk kell.

Tétel

Az $ax + by = c$ egyenletnek akkor és csak akkor létezik egész megoldása, ha $(a, b) \mid c$.

1. Milyen maradékot ad

   (a) 70^{70} 23-mal osztva;

(b) 55^{100} 48-cal osztva;

(c) 1025^{1005} 1023-mal osztva?

2. Oldjuk meg az alábbi lineáris kongruenciákat, illetve lineáris diofantikus egyenleteket!

   (a) $3x \equiv 2 \pmod 5$

   (b) $32x \equiv 12 \pmod{82}$

   (c) $13x \equiv 1 \pmod{28}$

   (d) $91x \equiv 252 \pmod{35}$

   (e) $43x + 25y = 98$

   (f) $64x + 26y = 4$

3. Egy egész szám 109-cel vett osztási maradéka 5-tel kisebb, mint a szám 18-szorosának a 109-cel vett osztási maradéka. Milyen maradékot adhat ez a szám 109-cel osztva?

4. Az n pozitív egész számra $43n - 1$ utolsó két számjegye megegyezik $2n + 2$ utolsó két számjegyével. Mi ez a két számjegy?

5. A 2×2015-ös A mátrixban az i-edik sor és a j-edik oszlop kereszteződésében álló elem legyen a $62 \cdot i \cdot j$ szám 2015-ös maradéka minden $1 \leq i \leq 2$, $1 \leq j \leq 2015$ esetén. Van-e A-nak olyan oszlopa, amelyben az első elem éppen 1-gyel kisebb a másodiknál? Ha igen, akkor milyen sorszámú oszlopokra teljesül ez?

6. Abszurdisztán pénzneme a lop, takarékossági okokból csak két címletet használnak: a 7 és a 19 lopost.

   (a) Hányféleképp tudjuk kifizetni a 101 lopos mozijegyet, ha a pénztárban még egyáltalán nincs pénz (vagyis nem tudnak visszaadni), nálunk azonban minden címletből 50 darab van?

   (b) Most másodikok vagyunk a pénztárnál és az első vásárló egy jegyet vett (vagyis ennek az ára van a pénztárban). Ezúttal hányféleképp tudunk fizetni, ha a többi körülmény változatlan?

   (c) Igaz-e, hogy bármely (egész) összeg kifizethető a két címlet segítségével (esetleg úgy, hogy valamelyikből visszakapunk)?