

Számelméleti algoritmusok
BEVEZETÉS A SZÁMÍTÁSELMÉLETBE 1
4. gyakorlat
2025.

1. Milyen maradékot ad

- (a) 73-mal osztva $3^{147} + 70^{147}$;
- (b) 25-tel osztva $46^{47^{48}}$;
- (c) 121-gyel osztva $42^{41^{40}}$;
- (d) 3^{2011} -nel osztva $100^{3^{2011}}$?

2. Hány olyan 504-nél nemnagyobb, pozitív egész szám van, amelynek van 504-gyel osztva 1 maradékot adó többszöröse?

3. Határozzuk meg

- (a) 899 és 493;
- (b) 346 és 158;
- (c) 24961 és 9483

legnagyobb közös osztóját.

4. Milyen maradékot ad

- (a) 79-cel osztva 3^{45} ;
- (c) 623-mal osztva 5^{300} ;
- (b) 91-gyel osztva 3^{169} ;
- (d) 155-tel osztva 5^{85} ?

5. Határozzuk meg a $10x \equiv 24 \pmod{m}$ lineáris kongruencia megoldásait modulo m , ahol

- (a) $m = 15$, illetve
- (b) $m = 16$.

6. Hány olyan szám van 1 és 10000 között, mely osztható 7-tel és 8-cal is, a 22-vel vett osztási maradéka pedig 10?

7. Jumurdzsák először örült a tiszti kinevezésnek, de hamarosan elment a kedve az egésztől. Mindjárt az első összezsápolásban jópáran elestek a rábízott 50-fős csapatból, amit még elviselt volna, csak hogy köztük volt a pénztáros is, így már a második héten Jumurdzsáknak kellett kiosztania a zsoldot, ami cseppet sem volt egyszerű feladat. Minden alárendeltjének 26 akcse járt hetente (neki magának pedig 2 arany), de a főnökség persze nem bajlódott akcsékkal, aranyban adta át Jumurdzsáknak a csapat heti zsoldját (1 arany = 60 akcse). Fel kellett tehát váltania az aranyakat a zsold kiosztása előtt, ráadásul még a visszamaradó nyamvadt 2 akcsét sem tarthatta meg. – Így jár, aki elveszti a talizmánját – sóhajtott keserűen. Hányan estek el (a második hétig) Jumurdzsák alárendeltjei közül?

8. Legyen $n = 20181210$. Az előadáson tanult megfelelő algoritmus alkalmazásával határozzuk meg $45n + 12$ és $35n + 9$ legnagyobb közös osztóját.
9. Legyen $n = 123456$. Az előadáson tanult megfelelő algoritmus alkalmazásával határozzuk meg $12n + 6$ és $9n + 4$ legnagyobb közös osztóját.
10. Határozzuk meg a

$$\max_{n \in \mathbb{Z}^+} \text{lko}(21n + 6, 6n + 4)$$

értéket.

11. Döntsük el az alábbi a számokról, hogy az m számoknak árulójuk vagy cinkosuk-e, esetleg egyik sem.

(a) $m = 33$ és $a = 6$

(c) $m = 21$ és $a = 8$

(b) $m = 13$ és $a = 2$

(d) $m = 21$ és $a = 5$

12. A $C: x \mapsto x^{77} \pmod{221}$ kódoló függvénnyel a $0, 1, \dots, 84$ „üzeneteket” lehet kódolni.

(a) Mennyi $C(2)$ értéke? A megoldáshoz használjuk az előadáson tanult megfelelő algoritmust.

(b) Határozzuk meg a C -hez tartozó D dekódoló függvényt és ellenőrizzük $D(y)$ értékét $y = C(2)$ -re.

13. Bizonyítsuk be, hogy 561 Carmichael-szám.