

1. A tanult Euklideszi algoritmus segítségével határozzuk meg az összes olyan egészt 0 és 301 között, aminek a 222-szerese 34 maradékot ad 302-vel osztva. (ZH, 2022. október 18.)

2. A $C : x \mapsto x^{43} \pmod{91}$ kódoló függvénnyel a $0, 1, \dots, 90$ „üzeneteket” lehet kódolni.

a) Mennyi $C(20)$ értéke? A megoldáshoz használjuk az előadáson tanult megfelelő algoritmust (és kivételesen számológépet is).

b) Határozzuk meg a C -hez tartozó D dekódoló függvényt és ellenőrizzük $D(y)$ értékét $y = C(20)$ -ra.

3. Az előadáson tanult megfelelő algoritmusok alkalmazásával oldjuk meg az alábbi feladatokat. A megoldáshoz (kivételesen) használjunk számológépet.

a) Milyen maradékot ad 3^{86} 79-cel osztva?

b) Mely x egészekre teljesül a $119x \equiv 2 \pmod{514}$ kongruencia?

c) Mely x egészekre teljesül a $158x \equiv 10 \pmod{346}$ kongruencia?

4. Legyen $n = 987654321$. Az előadáson tanult megfelelő algoritmus alkalmazásával határozzuk meg $98n + 27$ és $76n + 21$ legnagyobb közös osztóját. (ZH, 2020. december 21.)

5. – Mi legyen ebédre?

– Hát, mondjuk...

– Vigyázz, az ellenség lehallgatja a beszélgetést! Használd a $C : x \mapsto x^{11} \pmod{51}$ kódoló függvényt úgy, hogy az angol ábécé betűit sorban a $1, 2, \dots, 26$ számokkal helyettesítéd!

– Mármint...

– Ne értetlenkedj! $A = 1, B = 2, C = 3$, satöbbi, végül $Z = 26$. Ékezeteket ne használj és ne törődj azzal, hogy 50-ig a többi számnak már nincs jelentése. Szóval mi legyen a kaja?

– 2, 1, 6.

Készítsünk dekódoló függvényt és fejtsük meg vele, hogy mi lesz az ebéd.

6. Az előadáson tanult megfelelő algoritmusok alkalmazásával oldjuk meg az alábbi feladatokat. A megoldáshoz (kivételesen) használjunk számológépet.

a) Milyen maradékot ad 5^{300} 623-mal osztva?

b) Mi 352 és 155 legnagyobb közös osztója?

c) Mely x egészekre teljesül a $155x \equiv 7 \pmod{352}$ kongruencia?

d) Mely x egészekre teljesül a $122x \equiv 5 \pmod{166}$ kongruencia?

e) Mely x egészekre teljesül a $122x \equiv 6 \pmod{166}$ kongruencia?

7. Döntsük el az alábbi számokról, hogy 165-nek árulója, cinkosa vagy egyik sem. (A megoldáshoz használjunk számológépet és a megfelelő, tanult algoritmusokat.)

a) 13

b) 23

c) 33

8. Határozzuk meg 3^{100000} (vagyis három a százezrediken) utolsó 4 számjegyét. (ZH, 2022. december 19.)

9. Legyen $n = 20181210$. Az előadáson tanult megfelelő algoritmus alkalmazásával határozzuk meg $45n + 12$ és $35n + 9$ legnagyobb közös osztóját. (ZH, 2018. december 10.)

10. Elfogtunk egy gyanús üzenetet: 159,111,5,140,39,68,6. Tudjuk, hogy a feladó az üzenet karaktereit egyszerűen az ASCII kódjukkal helyettesítette, majd ezekre az $x \rightarrow (x^{29} \pmod{161})$ kódoló függvényt alkalmazta. (Ezzel a függvénnyel tehát a $0, 1, \dots, 160$ számokat lehet kódolni, de csak az első 128-nak van valódi jelentése.) Használjuk ki, hogy a feladó túl kicsi számokat választott a kód generálásakor: készítsünk dekódoló függvényt és fejtsük meg vele az üzenetet.

11*. Bizonyítsuk be, hogy 561 ($= 3 \cdot 11 \cdot 17$) Carmichael-szám.