Zh az anyag számelmélet részéből (1. zh, 2021-11-02)

A névsorban (vezetéknév alapján) K-Zs kezdőbetűsöknek.

A rendelkezésre álló idő 120 perc. Minden segédeszköz használható, mindaddig, amíg a munkát a hallgató önállóan végzi.

1. [papíron, 9 pont]
A bővített euklideszi algoritmus segítségével
keressük meg az alábbi (a,b) számpárok legnagyobb közös osztóját, *d*-t. A bővített változatot használjuk, tehát olyan *s, t* egészeket is adjunk meg, melyekkel d = as + bt.

A) a = 37, b = 14
B) a = 176, b = 64
C) a = 301, b = 89

2. [papíron, 9 = 4 + 2 + 3 pont]
Az alábbi problémák megoldását adjuk meg a tanult alakban, vagy adjunk meg indoklást arra, miért nincs megoldás. Az előző feladatban kapott *d, s, t* értékeket is használhatjuk.

A) Oldjuk meg az egészek körében a 37x + 14y = 400 egyenletet. Mik a pozitív megoldások?

B) Oldjuk meg a következő kongruenciát:

$$64x \equiv 32 \pmod{176}$$

C) A kínai maradéktétel segítségével adjuk meg az alábbi kongruenciarendszer megoldását:

$$x \equiv 3 \pmod{11}$$
$$x \equiv 5 \pmod{43}$$

3. [számítógéppel, 9 pont]
Legyen p prímszám. Azt mondjuk, hogy egy S egy egész szám „duplaköb mod p”, ha van olyan x egész, melyre:

2*x^3 ≡ S (mod p)

Például 5 duplaköb mod 7, mert 2*3^3 ≡ 5 (mod 7).
Keressük meg programmal a legkisebb olyan páratlan pozitív p prímet, melyre létezik 5 egymást követő szomszédos duplaköb mod p.

4. [papíron vagy géppel vagy vegyesen, 9 pont]

Számítsuk ki a 1023^1025^1027 hatvány maradékát
A) modulo 100,
B) modulo 41,
C) modulo 103.

5. [gépen, 9 pont]

Legyen x tetszőleges egész, melyre LNKO(x, 187) = 1. Képezzük a következő sorozatot:
a0 = x mod 187
a1 = x^3 mod 187
a2 = a1^3 mod 187
a3 = a2^3 mod 187
…
a(n) = a(n-1) ^3 mod 187
vagyis minden elem az előzpő köbe modulo 187.
Létezik (legalább egy) olyan K szám, melyre a következő teljesül:
Ha n > 200, akkor a(n+K) = a(n). Keressük meg x-hez a legkisebb ilyen pozitív K számot egy függvénnyel. Hogyan változik x-től függően a K érték?