

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

A névsorban (vezetéknév alapján) A-J kezdőbetűseknek.

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)  $a = 31, b = 12$

B)  $a = 174, b = 62$

C)  $a = 291, b = 83$

### 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  $31x + 12y = 400$  egyenletet. Mik a pozitív megoldások?

B) Oldjuk meg a következő kongruenciát:

$$62x \equiv 34 \pmod{174}$$

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

$$x \equiv 7 \pmod{21}$$

$$x \equiv 5 \pmod{41}$$

### 3. [számítógéppel, 9 pont]

Legyen  $p$  prímszám. Azt mondjuk, hogy egy  $S$  egy egész szám „köbszám mod  $p$ ”, ha van olyan  $x$  egész, melyre:

$$x^3 \equiv S \pmod{p}$$

Például 6 köbszám mod 7, mert  $3^3 \equiv 6 \pmod{7}$ .

Keressük meg programmal a legkisebb olyan páratlan pozitív  $p$  prímet, melyre létezik 5 egymást követő szomszédos köbszám 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  $\text{LNKO}(x, 187) = 1$ . Képezzük a következő sorozatot:

$$a_0 = x \bmod 187$$

$$a_1 = x^2 \bmod 187$$

$$a_2 = a_1^2 \bmod 187$$

$$a_3 = a_2^2 \bmod 187$$

...

$$a(n) = a(n-1)^2 \bmod 187$$

vagyis minden elem az előző négyzete 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 függvénnel. Hogyan változik  $x$ -től függően a  $K$  érték?