

I. zárthelyi (minta)

gépes rész

- Összpontszám: 35 pont.
- Használható: Sage, a tárgy honlapja, saját jegyzet, saját órai munka, Sage honlapja.
- Nem használható: egyéb internet, más személy, mesterséges intelligencia.
- Minden feladat megoldását írással ki.
- A megoldások ne legyenek túl lassúak (pár másodpercen belül fussanak le).
- A megoldásokat egyetlen `.sage` fájlban töltsük fel (nem `.zip`).

3. Keressük meg 1000-ig azokat a szomszédos prímszámokat, amelyek távolsága nagyobb, mint előttük bármely más szomszédos prímszámé: $(2, 3), (3, 5), (7, 11), (23, 29), \dots$ (8 p)

4. Két különböző pozitív egész szám, a és b *barátságos számok* [*amicable numbers*], ha bármelyikük valódi osztóinak összege megegyezik a másik számmal, azaz $s(a) = b$ és $s(b) = a$. Például 220 és 284 egy barátságos számpár. Írjuk ki 3000-ig az összes barátságos számpárt (mindegyik párt pontosan egyszer). Ne használjuk a Sage matematikai függvényeit. (9 p)

5. Oldjunk meg egyszerre több $ax \equiv b \pmod{m}$ alakú lineáris kongruenciát, ahol a és m *relatív prímek* és rögzített értékek, b pedig minden kongruenciában különböző.

- Használjuk ki, hogy több hasonló kongruenciát oldunk meg egyszerre, azaz ne külön-külön, egymástól függetlenül oldjuk meg őket.
- A függvény három paramétert vár: a -t, m -et és a lehetséges b -k listáját, és visszaadja a megoldások listáját, amelyek 0 és $m-1$ között vannak, és a b -k listájának felelnek meg.
- Ne használjuk a Sage matematikai függvényeit.
- Teszteljük a függvényt a $\{3x \equiv 0 \pmod{10}, 3x \equiv 1 \pmod{10}, \dots, 3x \equiv 9 \pmod{10}\}$ kongruenciákra, valamint a következőkre:

$$\{1101200990981x \equiv b \pmod{1234567654321} \mid b = 0, 1, \dots, 9\}.$$

(9 p)

6. Törjük fel a Diffie–Hellman-kulcscserét (ha lehetséges), azaz írjunk függvényt, amely a kulcscsere nyilvánosan látható adataiból diszkrét logaritmussal kiszámítja a közös titkot. Teszteljük a függvényt több különböző paraméteren (amelyeknek ismerjük a megoldását), köztük a $p = 23$ és a $p = 12345678923$ modulusokra is. (9 p)