II. 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 írassuk ki.
- A megoldások ne legyenek túl lassúak (pár másodpercen belül fussanak le).
- A megoldásokat egyetlen `.sage` fájlban töltsük fel (nem `.zip`).

3. a) Írjunk függvényt, amely adott n-re kiszámítja a $p_n = x^{n-1} + \ldots + x^2 + x + 1 \in \mathbb{Z}[x]$ polinomot. (Az eredmény típusa polinom legyen.)
b) Írjuk ki azon n-eket 1-től 20-ig, melyekre a fenti p_n irreducibilis. Mik ezek a számok? *(9 p)*

4. a) Módosítsuk az RSA implementációját úgy, hogy a nyilvános kitevő $e = 65537$ legyen, és ha így az RSA feltételei nem teljesülnek, akkor generáljunk új prímszámokat. A prímszámok $L = 2^{50}$ alatti véletlen számok legyenek. Titkosítsunk így egy tetszőleges üzenetet.
b) Törjük fel az RSA-t a Sage prímfaktorizációs függvénye segítségével, azaz állítsuk vissza az üzenetet a fent titkosított értékből csak a nyilvános kulcs használatával. (Megjegyzés: a fenti L elég kicsi ahhoz, hogy ez működjön.) *(9 p)*

5. Ebben a feladatban R legyen egy *kommutatív egységelemes gyűrű*, amelyet az elemek listájával adunk meg. (Tehát **nem** Sage struktúrát várnak, pl. `Zmod(7)`, hanem az elemek listáját, pl. `list(Zmod(7))`.) Az elemekről **semmi mást** ne használjunk, csak a gyűrű két műveletét (`a + b` és `a * b`) és egyenlőségvizsgálatot (`a == b` és `a != b`), valamint azt az absztrakt tényt, hogy kommutatív egységelemes gyűrűt alkotnak. (Tehát azt sem tudjuk, hogy melyik az egységelem.)
a) Írjunk függvényt, amely megkapja R-et és annak két $a, b \in R$ elemét, és eldönti, hogy $a \mid b$.
A függvény segítségével írassuk ki az összes $a \in \mathbb{Z}_{10}$ elemet, amely osztható a $\overline{4} \in \mathbb{Z}_{10}$ elemmel.
b) Írjunk függvényt, amely megkapja R-et, és visszaadja az *egységek* listáját R-ben.
A függvény segítségével írassuk ki $\mathbb{Z}_{10}$ egységeit. *(9 p)*

6. Írassuk ki minden legfeljebb tíz elemből álló véges test fölött azt a polinomot, amelynek a test minden eleme gyöke (mindegyik egyszeres, és nincsenek további faktorai). *(8 p)*