NÉV: NEPTUN:

ELTE IK Diszkrét modellek alkalmazásai (BSc, 18, F) A feladatsor

1. zárthelyi dolgozat

I. rész (hagyományos, papíron megoldandó feladatok)

Felhasználható idő: 30 perc

1. feladat 15 pont

Legyen adott egy olyan számítógép-architektúra, ahol a gépi szó 4 bites, tehát a számítógépünk az $I_1 = [0; 2^4 - 1] = [0; 15]$ intervallum egészeivel képes gyors egész aritmetikát végezni. Erre az aritmetikára építve valósítsunk meg az architektúránkon olyan egész aritmetikát (összeadás, kivonás, szorzás), amellyel az $I_2 = [0; 251]$ intervallumban is tudunk számolni.

Ábrázoljuk ebben az aritmetikában az egészeket I_1-beli modulo 4, 7 és 9 maradékainak rendszereként, majd végezzük el ebben az aritmetikában a $118 + 5 \cdot (110 - 89)$ műveletsort.

II. rész (programozási feladatok)

Felhasználható idő: 90 perc

2. feladat 4 pont

Írjon függvényt, amely a paraméterben kapott egészek listájának egy olyan másolatával tér vissza, amely nem tartalmazza a szintén paraméterként kapott egész számot.

3. feladat 10 pont

Egy a természetes számot Leyland-számnak nevezünk, ha a felírható $x^y + y^x$ alakban, ahol $1 < y \leq x$. Írjon függvényt, amely egy paraméterként kapott természetes számról eldönti, hogy Leyland-szám-e. Ha a vizsgált szám Leyland-szám, akkor a függvény térjen vissza a lehetséges (x,y) párok listájával; amennyiben nem az, akkor üres listával. Mutassa meg egy SageMath programmal, hogy a [2; 500] intervallumban nincs olyan Leyland-szám, amely legalább kétféleképpen írható fel.

4. feladat 10 pont

A moduláris számábrázolás szokásos jelöléseivel legyen $a, b \in \mathbb{Z}$ két szám, a_i, b_i a moduláris számábrázolásbeli számjegyeik, tehát
$a = (a_1, a_2, ..., a_k)$, $b = (b_1, b_2, ..., b_k)$,
$m_1, m_2, ..., m_k$ páronként relatív prím modulusok, $M = m_1 \cdot m_2 \cdot \ldots \cdot m_k$. Moduláris számábrázolásban az osztás a következő módon végezhető el:

Ha $lnko(b, M) = 1$ akkor $\dfrac{a}{b} = \left(\dfrac{a_1}{b_1} \mod m_1,\ \dfrac{a_2}{b_2} \mod m_2,\ ...,\ \dfrac{a_k}{b_k} \mod m_k \right)$

Írjon $RNS\_div(moduli, a, b)$ függvényt, amely moduláris számábrázolásban elvégzi az a/b osztást. Ha az osztás nem végezhető el, a függvény dobjon $ValueError$ kivételt.
Végezze el a 143/11 osztást, ahol a moduláris számábrázolásbeli használt modulusok $2, 3, 5, 7$ legyen.

5. feladat 11 pont

Legyen

$a = 64634626235213500000000000000000000436222222222222222222222222222222222222222222222222222299999999$

$b = 43464120000032562352350000000000000000000000000000532634742373467436000000000000000000000236236233$

Végezze el az $a - b$ kivonást moduláris számábrázolással úgy, hogy a számjegyek reprezentánsai (residues) legnagyobb megengedett modulusa 500000. Az a és b pontos értéke megtalálható a zh munkafüzetében. SageMath forráskóddal indokolja, hogyan választott alkalmas modulusokat.

2020. november 5.

Koch-Gömöri Richárd, kgomoririchard@inf.elte.hu, kgomori.richard@gmail.com