14. feladatsor: Moduláris számábrázolás, RSA-titkosítás

1. feladat (*)
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 $I_2 = [0; 1100]$ intervallumban is tudunk számolni.

Ábrázoljuk ebben az aritmetikában az egészeket I_1-beli modulo $7, 11$ és 15 maradékainak rendszereként, majd végezzük el ebben az aritmetikában a $16 + 52$, $52 - 16$, $16 \cdot 52$ műveleteket.

2. feladat (*)
Legyen adott egy olyan számítógép-architektúra, ahol a gépi szó 3 bites, tehát a számítógépünk az $I_1 = [0; 2^3 - 1] = [0; 7]$ intervallum egészeivel képes gyors egész aritmetikát végezni. Erre az aritmetikára építve valósítsunk meg az architektúránkon olyan egész aritmetikát (összeadás, kivonás, szorzás), amellyel az $I_2 = [0; 200]$ intervallumban is tudunk számolni.

Ábrázoljuk ebben az aritmetikában az egészeket I_1-beli modulo 2, 3, 5 és 7 maradékainak rendszereként, majd végezzük el ebben az aritmetikában az $5 \cdot (6 \cdot 32 - 159)$ műveletsort.

3. feladat (*)

4. feladat (*)

5. feladat (*)

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