

3. feladat 12 pont

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.

Megoldás

$$5 = (5 \bmod 2, 5 \bmod 3, 5 \bmod 5, 5 \bmod 7) = (1, 2, 0, 5)$$

$$7 = (7 \bmod 2, 7 \bmod 3, 7 \bmod 5, 7 \bmod 7) = (0, 0, 1, 6)$$

$$32 = (32 \bmod 2, 32 \bmod 3, 32 \bmod 5, 32 \bmod 7) = (0, 2, 2, 4)$$

$$159 = (159 \bmod 2, 159 \bmod 3, 159 \bmod 5, 159 \bmod 7) = (1, 0, 4, 5)$$

$$c = 5 \cdot (6 \cdot 32 - 159) = (1 \cdot (0 \cdot 0 - 1) \bmod 2, 2 \cdot (0 \cdot 2 - 0) \bmod 3, 0 \cdot (1 \cdot 2 - 4) \bmod 5, 5 \cdot (6 \cdot 4 - 5) \bmod 7) = (-1 \bmod 2, 0 \bmod 3, 0 \bmod 5, 95 \bmod 7) = (1, 0, 0, 4)$$

$-1 \bmod 2 = 1$ mert m -el osztva $0 \leq \text{maradék} < m$ és $-1 + 2 = 1$, tehát $-1 \bmod 2 = 1$. Hasonlóan $95 - 13 \cdot 7 = 4$ ezért $95 \bmod 7 = 4$.

Azt kaptuk tehát, hogy $c = (1, 0, 0, 4)$. Ki kell számítani tehát azt a $c \in \mathbb{Z}$ számot, amely 2-vel osztva 1, 3-mal osztva 0, 5-tel osztva 0, 7-tel osztva 4 maradékot ad. Erre alkalmas eszköz a kongruencia-egyenlet rendszer:

$$x \equiv 1 \pmod{2}$$

$$x \equiv 0 \pmod{3}$$

$$x \equiv 0 \pmod{5}$$

$$x \equiv 4 \pmod{7}$$

A modulusok páronként relatív prímek ($m_1 = 2, m_2 = 3, m_3 = 5, m_4 = 7$), alkalmazható a kínai maradéktétel: létezik megoldás modulo $M = 2 \cdot 3 \cdot 5 \cdot 7 = 210$ és ez a megoldás egyértelmű (azaz csak egyetlen maradékosztály elégíti ki).

$$\text{Legyen } M_1 = \frac{210}{2} = 105, M_2 = \frac{210}{3} = 70, M_3 = \frac{210}{5} = 42, M_4 = \frac{210}{7} = 30.$$

Meg kell oldani az $M_i \cdot y \equiv 1 \pmod{m_i}$ kongruenciákat:

I

$$105y \equiv 1 \pmod{2}$$

$$\text{megoldás: } y \equiv 1 \pmod{2}$$

II

$$70y \equiv 1 \pmod{3}$$

$$\text{megoldás: } y \equiv 1 \pmod{3}$$

III

$$42y \equiv 1 \pmod{5}$$

$$\text{megoldás: } y \equiv 3 \pmod{5}$$

IV

$$30y \equiv 1 \pmod{7}$$

$$\text{megoldás: } y \equiv 4 \pmod{7}$$

A kongruencia-rendszer megoldása:

$$c \equiv 1 \cdot 105 \cdot 1 + 0 \cdot 70 \cdot 1 + 0 \cdot 42 \cdot 3 + 4 \cdot 30 \cdot 4 \pmod{210} \equiv 165 \pmod{210}$$

Innen a végeredmény: $c = 165$

Koch-Gömöri Richárd, kgomori.richard@gmail.com