Adatábrázolás

Definíció. Az egy gépi szóban ábrázolható egészeket *egyszeres pontosságú egészeknek* nevezzük.

Az egészek reprezentálásának lehetőségei:

(1) Helyiértékes

$$n = \sum_{i=0}^{k-1} d_i B^i$$

(a) (B-1) beférjen egy gépi szóba

(b) d_i jegyek egyszeres pontosságúak

(c) $[d_0, d_1, \ldots d_{k-1}]$ lineáris listát láncolt listaként vagy tömbként implementáljuk

(2) Moduláris

Az n egész megfelelő számú, egyszeres pontosságú, páronként relatív prím modulusokkal vett moduláris képeinek lineáris listájaként adható meg.

Megjegyzés. Összeadás, szorzás és osztás elvégzése gyorsabb.

Példa. 32 bites számítógépünk

$$I_1 = [0, 2^{32} - 1]$$

intervallum egészeivel tud számolni, legyen $I_2 = [0, 10^4]$ és $B = 10^4$.

$$n_1 = 12345678909876543210 1234567890,$$

$$n_2 = 2110,$$

$$n_1 = [7890, 3456, 1012, 5432, 9876, 7890, 3456, 12],$$

$$n_2 = [2110],$$

$$n_1 + n_2 = [0, 3457, 1012, 5432, 9876, 7890, 3456, 12].$$

Legyen

$$\prod_{i=1}^{6} m_i > 10^{50}$$

$$m_1 = 4294967291, m_2 = 4294967279,$$

$$m_3 = 4294967231, m_4 = 4294967197,$$

$$m_5 = 4294967189, m_6 = 4294967161,$$

ekkor

$$n_1 \equiv 2009436698 \pmod{m_1},$$

$$n_{\equiv} 961831343 \pmod{m_2},$$

$$n_1 \equiv 4253639097 \pmod{m_3},$$

$$n_1 \equiv 1549708 \pmod{m_4},$$

$$n_1 \equiv 2459482973 \pmod{m_5},$$

$$n_1 \equiv 3373507250 \pmod{m_6},$$

$$n_2 \equiv 2110 \pmod{m_1}, (i \leq i \leq 6).$$

Az összeadást és szorzást koordinátánként modulárisan végezzük.

Absztrakciós szintek

(a)Objektumok szinje

(b) Forma szintje

(c) Adatstruktúra szintje

$$p(x) = x^2 + x - 2$$

együtthatókból álló tömb: $[-2, 1, 1]$,

láncolt lista: $[-2, 0] \rightarrow [1, 1] \rightarrow [1, 2]$.

Megjegyzés. Tekintsünk egy n egyenletből és n ismeretlenből álló egyenletrendszert, ahol minden együttható egész és elfér egy ω hosszúságú rekeszben. Gauss eliminációt alkalmazva a redukció eredményeként kapott együtthatók $2^{n-1}\omega$ tárhelyet igényelnek.

Köztes számítási tárrobbanás.

Tétel. Ha F test, $a, b \in F[x]$,

$$\deg(a) = m \geq n = \deg(b),$$

akkor a Klasszikus-Euklidesz és a Bővített-Euklidesz algoritmusok $O(m, n)$ F-beli aritmetikai műveletet igényelnek.

Megjegyzés.

$$O(g(n)) = \{f(n) : 0 \leq f(n) \leq cg(n), n \geq n_0\}$$

A rezultáns

Legyenek

$$f(x) = f_m(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m),$$

$$g(x) = g_n(x-\beta_1)(x-\beta_2)\cdots(x-\beta_n).$$

Definíció. A $res(f,g)$ szorzatot az f és g polinomok *rezultánsának* nevezzük, ahol

$$res(f,g) = f_m^n g_n^m(\alpha_1-\beta_1)(\alpha_1-\beta_2)\cdots(\alpha_1-\beta_n)$$

$$\cdot(\alpha_2-\beta_1)(\alpha_2-\beta_2)\cdots(\alpha_2-\beta_n)$$

$$\cdots(\alpha_m-\beta_1)(\alpha_m-\beta_2)\cdots(\alpha_m-\beta_n).$$