Reziduumi i aritmetika sa reziduumima

Imamo stvari čiji broj ne znamo
ako ih grupišemo u trojke, ostatak je 2,
ako ih grupišemo u petorke, ostatak je 3,
ako ih grupišemo u sedmorke, ostatak je 2.
Koliko stvari imamo?

Sun Tzu, 4. vek n.e

Tehnika za rešavanje ovog problema danas je poznata pod nazivom *Kineska teorema o ostacima*

U aritmetici rezuduuma (modularnoj aritmetici) ostatak (eng. *residue*) nekih brojeva x i y je broj r koji se dobija kada se od x oduzme najveći mogući broj w, tako da je $w = b * y$, tj. $r = x - b * y$

Reziduumski brojčani sistem (RBS)

Pozicioni broji̇ sistem kod koga svaka pozicija ima različitu težinu

Za broj $X = (x_n|x_{n-1}|...|x_1|x_0)$ zapisan u reziduumskom brojčanom sistemu sa modulima $(t_n|t_{n-1}|...|t_1|t_0)$ važi

- moduli su uzajmno prosti brojevi t_n, t_{n-1}, t_1, t_0 pri čemu važi $t_n > t_{n-1} > ... > t_1 > t_0$
- Cifre u zapisu broja u reziduumskom sistemu se odredjuju na sledeći način:

  $x_i = X \bmod t_i = <X>_{t_i}$, $x_i = [0, t_i - 1]$
- Broj razlčitih vrednosti koji može da se predstavi je jednak proizvodu $t_n \times t_{n-1} \times ... \times t_1 \times t_0$

Primer: U RBS (8 | 7 | 5 | 3) (tzv. pretpostavljeni (eng. *default*) RBS) može da se predstavi 840 različitih brojeva. Interval (tzv. dinamički interval) može da bude

- za neoznačene brojevi [0,839],
- za označene brojevi [-420, 419]
- bilo koji interval od 840 uzastopnih celih brojeva koji sadrži 0

Odredjivanje težine pozicija

Da bi izračunali težinu odgovarajuće pozicije u RBS sa modulima $(t_n|t_{n-1}|...|t_1|t_0)$ poslužimo se sličnim principom kao i kod pozicionih brojčanih sistema koda kojih je težina pozicije jednaka osnovi stepenovanoj na poziciju na kojoj se nalazi cifra.

Tako je težina pozicije n na kojoj se nalazi modul t_n jednaka vrednosti broja (1 | 0 | ... | 0 | 0) zapisanog u tom RBS-u. Sa druge strane, ovaj zapis označava da je broj koji se zapisuje deljiv sa svim ostlim modulima t_i $(0 \geq i \leq n-1)$, dok se pri deljenju sa t_n dobija ostatak 1. Na osnovu Kineske teoreme o ostacima (pojednostavljeno) težina te pozicije je jednaka umnošku proizvodu modula na ostalim pozicijama $t_{i-1} \times t_{i-2} \times ... \times t_1 \times t_0$. Analogno se izračunavaju i težine na ostalim pozicijama.

Veličina umnoška u sa kojim se množi dobijeni proizvod se računa na osnovu iste teoreme tako da važi
$u \times proizvod$ mod $modul = 1$. Na osnovu toga, težine pozicija u pretpostavljenom RBS-u su:

$(1 \mid 0 \mid 0 \mid 0)_{RBS(8|7|5|3)}$=7*5*3=105
$(0 \mid 1 \mid 0 \mid 0)_{RBS(8|7|5|3)}$=8*5*3=120
$(0 \mid 0 \mid 1 \mid 0)_{RBS(8|7|5|3)}$=8*7*3=336 (jer 336 mod 5 = 1, a 168 mod 5$\neq$1)
$(0 \mid 0 \mid 0 \mid 1)_{RBS(8|7|5|3)}$=8*7*5=280

Predstavljanje celih brojeva u RBS

Predstavljanje pozitivnih brojeva u RBS

Primer: predstavljanje broja 62 u pretpostavljenom RBS:

$r_1 = 62 \bmod 8 = 6$
$r_2 = 62 \bmod 7 = 6$
$r_3 = 62 \bmod 5 = 2$
$r_3 = 62 \bmod 3 = 2$
Dakle $(62)_{10} = (\ 6 \mid 6 \mid 2 \mid 2)_{RBS(8|7|5|3)}$

Predstavljanje broja 62 u RBS (9|8|7)

$r_1 = 62 \bmod 9 = 8$
$r_2 = 62 \bmod 8 = 6$
$r_3 = 62 \bmod 7 = 6$

Dakle: $(62) = (\ 8 \mid 6 \mid 6\ )_{RBS(9|8|7)}$

Predstavljanje broja 902 u pretpostavljenom RBS:

$r_1 = 902 \bmod 8 = 6$
$r_2 = 902 \bmod 7 = 6$
$r_3 = 902 \bmod 5 = 2$
$r_4 = 902 \bmod 3 = 2$
Dakle $(902)_{10} = (\ 6 \mid 6 \mid 2 \mid 2)_{RBS(8|7|5|3)}$

Predstavljanje negativnih brojeva u RBS

Kada želimo da zapišemo negativan broj $-m$ u RBS-u primenjujemo sledeće pravilo:

Zapišemo pozitivan broj m u RBS i svaki ostatak u dobijenom zapisu se dopuni do težine na odgovarajućoj poziciji. U slučaju da je ostatak jednak nuli, ne vrši se dopunjavanje. Formalno, u RBS (t_n |t_{n-1} | ... |t_1 |t_0) se pozitivan broj m zapisuje kao m = (r1 | r2 | ... | rn)

Kada želimo da pretstavimo negativan broj $-m$ to ćemo uraditi na sledeći način:

$-m = (t_n\text{-}r_n|t_{n-1} - r_{n-1}|...|t_1 - r_1|t_0 - r_0)$

Primer zapisa negativnog broja -62 u RBS(8 | 7 | 5 | 3)

$(62)_{10}$ = (6 | 6 | 2 | 2)$_{RBS(8|7|5|3)}$

$(-62)_{10}$ = (8 - 6 | 7 - 6 | 5 - 2 | 3 - 2)$_{RBS(8|7|5|3)}$ = (2 | 1 | 3 | 1)$_{RBS(8|7|5|3)}$

Konverzija iz RBS u dekadni sistem

Konverzija iz RBS u dekadni sistem se vrši tako što se vrednost svake cifre u zapisu broja množi sa odgovarajućom težinom, dobijene vrednosti saberu i odredi ostatak po modulu proizvoda svih modula RBS-a.

Za RBS (8|7|5|3) težine koje su pridružene odgovarajućim pozicijama su 105, 120, 336 i 280. Tako

$(1|2|4|0) = 105\times1 + 120\times2 + 336\times4 + 280\times0 \bmod 840 = 9$

$(5|5|4|0) = 105\times5 + 120\times5 + 336\times4 + 280\times0 \bmod 840 = 789$

Aritmetika u RBS-u

Negacija, sabiranje, oduzimanje i množenje brojeva zapisanih u RBS-u se izvode nezavisno nad svakom od pojedinačnih cifara. Ako su

$A = (a_n|a_{n-1}|...|a_1|a_0)$ i $B = (b_n|b_{n-1}|...|b_1|b_0)$

brojevi zapisani u reziduumskom brojčanom sistemu sa modulima $(t_n|t_{n-1}|...|t_1|t_0)$ tada je vrednost

$C = A\ \Delta\ B$ gde $\Delta \in \{+, -, \times\}$ broj zapisan u reziduumskom brojčanom sistemu na sledeći način:

$C = (c_n|c_{n-1}|...|c_1|c_0)$ gde $c_i\ =\ a_i\ \Delta\ b_i\ \ mod\ t_i$.

Deljenje je dosta složeno i teško za implementaciju i na njemu se nećemo zadržavati.

Primeri aritmetičkih operacija

Neka je RBS=(8|7|5|3), i neka su brojevi A=26 =(2|5|1|2) i B=12 =(4|5|2|0).

Sabiranje

C = A+B
= ((2+4) mod 8| (5+5) mod 7| (1+2) mod 5| (2+0) mod 3)
= (6|3|3|2)

Konverzija u dekadni sistem daje

C = (6*105 + 3*120 + 3*336 + 2*280) mod 840
= (630 + 360 + 1008 + 560) mod 840
= 2558 mod 840
= 38

Oduzimanje

Oduzimanje može da se izvede kao sabiranje komplementa broja, pri čemu se komplementiranje radi u RBS-u. Primenom pravila za komplementiranje -12 = (4|2|3|0). Na tako dobijeni broj može da se primeni pravilo za sabiranje:

C = A-B
= ((2+4) mod 8 | (5+2) mod 7 | (1+3) mod 5 | (2+0) mod 3)
= (6 | 0| 4| 2).

Konverzija u dekadni sistem daje

C = (6*105 + 0*120 + 4*336 + 2*280) mod 840
= (630 + 0 + 1344 + 560) mod 840
= 2534 mod 840
= 14

Alternativni način je da se direktno primenjuje operacija oduzimanja:

C = A-B
= ((2-4) mod 8 | (5-5) mod 7 | (1-2) mod 5 | (2-0) mod 3)
= (6 | 0| 4| 2)

(uz pažljivo odredjivanje ostatka!). Konverzija u dekadni sistem daje

C = (6*105 + 0*120 + 4*336 + 2*280) mod 840
= (630 + 0 + 1344 + 560) mod 840
= 2534 mod 840
= 14

Množenje

C = A*B
= ((2*4) mod 8 | (5*5) mod 7 | (1*2) mod 5 | (2*0) mod 3)
= (0 | 4| 2| 0)

Konverzija u dekadni sistem daje

C = (0*105 + 4*120 + 2*336 + 0*280) mod 840
= (0 + 480 + 672 + 0) mod 840
= 1152 mod 840
= 312

Prednosti i nedostaci reziduumskog brojčanog sistema

Prednosti

- Nema problema sa prenosom sa mesta najveće težine
- Cifre su male čak i za velike brojeve. Operacije mogu da budu vrlo brze ako se realizuju preko predefinisanih tabela
- Aritmetika (sabiranje, oduzimanje, moženje) je jednostavna i brza

Nedostaci

Sledeće operacije su složene i teške za implementaciju

- Testiranje znaka broja
- Poredjenje veli cina brojeva
- Otkrivanje prekoračenja
- Deljenje

Primena RBS

- U obradi digitalnih signala i slika
- Obrade sa digitalnim filterima