Zapis brojeva pomoću ostataka

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 Cu, 4. vek n.e

Prevedno na jezik matematike jezik, pitanje glasi: koji broj daje ostatak 2, 3 i 2 ako se redom deli sa 3, 5 i 7?

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

Brojčani sistem sa ostacima

- Brojčani sistem sa ostacima (reziduumski brojčani sistem, RBS) - pozicioni brojčani sistem sa više osnova kod koga svaka pozicija u zapisu broja ima različitu osnovu.
- Zasnovan je na relaciji kongruentnosti. Brojevi a i b su kongruentni po modulu m ako m deli bez ostatka razliku $a-b$.
- Broj m se naziva *moduo* ili *osnova*.
- Ostatak pri deljenju brojeva a i m je broj r koji se dobija kada se od a oduzme najveći mogući broj c, tako da je $c = d*m$, tj. $r = a - d*m$. Oznaka: $r = |a|_m$.
- Za dati skup $\{m_n, m_{n-1}, ..., m_1\}$ pozitivnih celih brojeva (modula) koji su veći od 1, $RBS(m_n|m_{n-1}|...|m_1)$ označava brojčani sistem sa ostacima $m_n, m_{n-1}, ..., m_1$.
- Broj $(A)_{10}$ zapisuje se u RBS pomoću n cifara:
  $(A)_N = (a_n|a_{n-1}|...|a_1)_{RBS(m_n|m_{n-1}|...|m_1)}$
  gde važi $\mathrm{a}_i = \mathrm{A} \bmod \mathrm{m}_i = |\mathrm{A}|_{m_i}$, $\mathrm{a}_i \in [0, m_i - 1]$, $i \in [1, n]$

Primer: zapis broja 62 u RBS (8 | 7 | 5 | 3) je

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

Zapis broja 62 u RBS (9|8|7) je

r_1=62 mod 9=8
r_2=62 mod 8=6
r_3=62 mod 7=6

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

Zapis broja 902 u pretpostavljenom RBS je

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

- Duplikati?
- Interval zapisa?
- Da bi se izbegla višeznačnost zapisa brojeva i pojava duplikata, moduli moraju da budu uzajmno prosti brojevi $m_n, m_{n-1}, ..., m_1$ pri čemu važi $m_n > m_{n-1} > ... > m_1$.
- $RBS(m_n|m_{n-1}|...|m_1) \longrightarrow$ broj razlčitih vrednosti koje mogu da se predstave je jednak $M = \prod_{i=1}^{n} m_i$.
- Primer: u RBS (8 | 7 | 5 | 3) može da se predstavi $M = 8 \times 7 \times 5 \times 3 = 840$ različitih brojeva. Kako važi $(-X)m_i = (M - X_{m_i})$ interval može da bude
  - za neoznačene brojevi [0,839],
  - za označene brojevi [-420, 419]
  - bilo koji interval oblika [-N,P] gde važi M=N+P+1

Modularna aritmetika

Aditivni inverz

1. Za ostatak x, aditivni inverz $\overline{\mathrm{x}}$ je definisan pomoću jednakosti $x+\overline{\mathrm{x}}=0$
2. Izračunava se kao $\overline{\mathrm{x}}=|m-x|_m$

Primeri:

- $(62)_{10}=(6|6|2|2)_{RBS(8|7|5|3)}$. Aditivni inverz može da se izračuna kao

  $$\begin{aligned} |8-6|_8 &= 2 \\ |7-6|_7 &= 1 \\ |5-2|_5 &= 3 \\ |3-2|_3 &= 1 \end{aligned}$$

  Odavde je $\overline{(6|6|2|2)}_{RBS(8|7|5|3)}=(2|1|3|1)_{RBS(8|7|5|3)}$

- $(62)_{10}=(8|6|6)_{RBS(9|8|7)}$. Aditivni inverz može da se izračuna kao

  $$\begin{aligned} |9-8|_9 &= 1 \\ |8-6|_8 &= 2 \\ |7-6|_7 &= 1 \end{aligned}$$

  Odavde je $\overline{(8|6|6)}_{RBS(9|8|7)}=(1|2|1)_{RBS(9|8|7)}$

Zapis negativnih brojeva

Formalno, u $RBS(m_n|m_{n-1}|...|m_1)$ negativni brojevi mogu da se predstave u zapisu pomoću komplementa gde je komplementaciona konstanta jednaka $M = \prod_{i=1}^{n} m_i$.

Zapis negativnog broja se takodje dobija nalaženjem aditivnog inverza apsolutne vrednosti broja.

Primer: zapis broja $(-62)_{10}$ u RBS(8|7|5|3) može da se dobije

- pomoću aditivnog inverza:

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

- Pomoću zapisa broja koji se dobija komplementiranjem sa komplementacionom konstantom 840. Kako je 840-62=778, a zapis broja 778 u RBS (8|7|5|3) je

  r_1=778 mod 8=2
  r_2=778 mod 7=1
  r_3=778 mod 5=3
  r_3=778 mod 3=1

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

Sabiranje i oduzimanje

Pravilo za sabiranje i oduzimanje u modularnoj aritmetici je:

$$| A \pm B |_m = | |A|_m \pm |B|_m|_m$$

Oduzimanje se može izvesti i kao sabiranje sa aditivnim inverzom umanjioca.

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

- Zbir $C = A + B$ je jednak

$$\begin{aligned} \mathrm{C} &= \mathrm{A+B} \\ &= ((2+4)\mathrm{mod}\ 8|(5+5)\mathrm{mod}\ 7|(1+2)\mathrm{mod}\ 5|(2+0)\mathrm{mod}\ 3)_{RBS(8|7|5|3)} \\ &= (6|3|3|2)_{RBS(8|7|5|3)} \end{aligned}$$

- Razlika $C = A - B$ preko direktne operacije oduzimanja:

$$\begin{aligned} \mathrm{C} &= \mathrm{A\text{-}B} \\ &= ((2\text{-}4)\mathrm{mod}\ 8|(5\text{-}5)\mathrm{mod}\ 7|(1\text{-}2)\mathrm{mod}\ 5|(2\text{-}0)\mathrm{mod}\ 3)_{RBS(8|7|5|3)} \\ &= (\overline{\text{-}2}\ |\ 0|\ \overline{\text{-}1}|2)_{RBS(8|7|5|3)} \\ &= (6|0|4|2)_{RBS(8|7|5|3)} \end{aligned}$$

- Razlika $C = A - B$ preko sabiranja sa aditivnim inverzom:

$$\begin{aligned} \text{-}12 &= 840\text{-}12 \\ &= 828=(4|2|3|0)_{RBS(8|7|5|3)} \end{aligned}$$

$$\begin{aligned} \mathrm{C} &= \mathrm{A\text{-}B} \\ &= ((2+4)\mathrm{mod}\ 8|(5+2)\mathrm{mod}\ 7|(1+3)\mathrm{mod}\ 5|(2+0)\mathrm{mod}\ 3)_{RBS(8|7|5|3)} \\ &= (6|0|4|2)_{RBS(8|7|5|3)}. \end{aligned}$$

Množenje

Pravilo za množenje u modularnoj aritmetici je:

$$| A \times B |_m = | |A|_m \times |B|_m|_m$$

Primer: Neka je RBS=(8|7|5|3), $A = 26 = (2|5|1|2)_{RBS(8|7|5|3)}$,
$B = 12 = (4|5|2|0)_{RBS(8|7|5|3)}$. Proizvod $C = A \times B$ je jednak

$$\begin{aligned} \mathrm{C} &= \mathrm{A} \times \mathrm{B} \\ &= ((2 \times 4)\mathrm{mod}\ 8|(5 \times 5)\mathrm{mod}\ 7|(1\times 2)\mathrm{mod}\ 5|(2\times 0)\mathrm{mod}\ 3)_{RBS(8|7|5|3)} \\ &= (0|4|2|0)_{RBS(8|7|5|3)} \end{aligned}$$

Množenje modulom

Za svaku celobrojnu vrednost k i moduo m važi:

1. $|k \times m|_m = 0$
2. $|A \pm k \times m|_m = |A|_m$

Skraćuje se postupak sabiranja i oduzimanja u slučajevima kada je jedan od sabiraka umnožak modula, tako što se ne vrši sabiranje ili oduzimanje na poziciji tog modula.

Primer: RBS(8|7|5|3), $A = 26$, $B = 14$. Sabiranjem na uobičajeni način dobija se:

$A = 26 = (2|5|1|2)_{RBS(8|7|5|3)}$, $B = 14 = (6|0|4|2)_{RBS(8|7|5|3)}$
$A + B = (2+6|5+0|1+4|2+2)_{RBS(8|7|5|3)} = (0|5|0|1)_{RBS(8|7|5|3)}$

Kako je $14 = 2 \times 7$, prema prethodnim pravilima ne treba izvršiti sabiranje na poziciji koja odgovara modulu 7:

$A + B = (2+6|5|1+4|2+2)_{RBS(8|7|5|3)} = (0|5|0|1)_{RBS(8|7|5|3)}$

Multiplikativni inverz

Za uzajamno proste ne-nula brojeve A i m, A^{-1} je multiplikativni inverz broja A u odnosu na moduo m ako važi

$$|A \times A^{-1}|_m = 1$$

Primeri:

1. Neka je $A = 5$. Multiplikativni inverz u odnosu na moduo 11 je vrednost A^{-1} za koju važi

   $$|5 \times A^{-1}|_{11} = 1$$

   Za rešavanje se može koristiti diofanska jednačina 5*x = 11*y +1. Jedno od rešenja jednačine je x=9, y=4. Odavde se dobija da 9 je multiplikativni inverz broja 5 u odnosu na moduo 11 (jer 5*9=45, 45 mod 11 = 1).

2. Neka je $A = 9$. Multiplikativni inverz u odnosu na moduo 13 je vrednost A^{-1} za koju važi

   $$|9 \times A^{-1}|_{13} = 1$$

   Za rešavanje se može koristiti diofantska jednačina 9*x = 13*y +1. Jedno od rešenja jednačine je x=3, y=2. Odavde se dobija da 3 je multiplikativni inverz broja 9 u odnosu na moduo 13 (jer 9*3=27, 27 mod 13 = 1).

Deljenje

1. Najsloženija od osnovnih aritmetičkih operacija u modularnoj aritmetici
2. Problemi i oko definisanja
3. Nula nema multiplikativni inverz
4. Uobi vcajena definicija deljenja: $c = a/b$. Odavde $\longrightarrow a = c \times b$
5. U RBS ekvivalentan zapis bi bio $c \times b \equiv a(mod\ m)$, odakle se množenjem sa multiplikativnim inverzom od b dobija

   $c \equiv a \times b^{-1}(mod\ m)$

   c predstavlja količnik samo u slučaju kada je ceo broj.

1. Neka $m = 7$ i neka treba izračunati količnik $c = 6/2$. Odavde se dobija:

$$\begin{aligned} 2*c &\equiv 6 \text{ (mod 7)} \\ c &\equiv 6 * 2^{-1} \text{ (mod 7)} \\ &\equiv 6 * 4 \text{ (mod 7)} \\ &\equiv 3 \text{ (mod 7)} \end{aligned}$$

2. Neka $m = 7$ i neka treba izračunati količnik $c = 6/4$. Odavde se dobija:

$$\begin{aligned} 4*c &\equiv 6 \text{ (mod 7)} \\ c &\equiv 6 * 4^{-1} \text{ (mod 7)} \\ &\equiv 6 * 2 \text{ (mod 7)} \\ &\equiv 5 \text{ (mod 7)} \end{aligned}$$

3. Neka $m = 7$ i neka treba izračunati količnik $c = 4/6$. Odavde se dobija:

$$\begin{aligned} 6*c &\equiv 4 \text{ (mod 7)} \\ c &\equiv 4 * 6^{-1} \text{ (mod 7)} \\ &\equiv 4 * 6 \text{ (mod 7)} \\ &\equiv 3 \text{ (mod 7)} \end{aligned}$$

U sva tri primera važi kongruencija $c \equiv ab^{-1}$ (mod m), ali je vrednost za c ispravan količnik samo u prvom slučaju.

Izbor modula

1. U principu, za module brojčanog sistema sa ostaima se mogu uzeti bilo koji celi brojevi
2. U računaru je važna efikasnost izvršavnjaa operacija
3. Ideja je da moduli budu što je moguće manji, jer veličina najvećeg modula m_n odredjuje brzinu izvodjenja aritmetičkih operacija
4. Zbog poredjenja modula po veličini sa najvećim, nije prednost upotreba jednog velikog i velikog broja malih modula
5. Zbog boljeg iskorišćenja memorije, poželjno je da svi moduli budu predstavljeni pomoću što je manje mogućeg broja bitova

Primer: predstavljanje neoznačenih dekadnih brojeva $\in$[0,1000000]. Za predstavljanje ovih brojeva u računaru je potrebno 20 bitova ($2^{20} - 1 =$ 1048575) Neke mogućnosti za izbor modula su:

1. Uzimanje (uzajmno) prostih brojeva sve dok njihov proizvod M ne bude veći od postavljene granice. Uzimanjem $m_1 = 2, m_2 = 3, m_3 = 5, m_4 = 7, m_5 = 11, m_6 = 13, m_7 = 17$ i $m_8 = 19$ dobija se da je M= 9699690.

   Dinamički opseg više od 9 puta veći od potrebne veličine $\longrightarrow$ iz skupa modula može da se ukloni moduo (ili moduli čiji je proizvod) manji (ali najbliže sa donje strane) od 9.

   RBS(19,17,13,11,5,3,2) i M=1385670. U računaru se brojevi predstavljaju pomoću ukupnog broja bitova potrebnog za zapis svakog od ostataka: 5 + 5 + 4 + 4 + 3 + 2 + 1 = 24.

   Posledica: zapis u ovom sistemu troši 20% više prostora nego zapis u obliku neoznačenih binarnih brojeva.

2. Poboljšanje: brzinu izvodjenja aritmetičkih operacija odredjuje 5-bitni modul $m_7 = 19 \longrightarrow$ mogu se kombinovati parovi modula 13 i 2 kao i 5 i 3 bez gubitka brzine. Novodobijeni sistem je RBS(26,19,17,15,11) i M=1385670 koji zahteva 5 + 5 + 5 + 4 + 4=23 bita

Isti ili bolji rezultati po pitanju zauzeća memorije se dobijaju ako se postupa na sličan način, ali se, pre prelaska na naredni prost broj, kao moduli uključe stepeni manjih prostih brojeva (uz istovremno njihovo isključivanje iz skupa modula).

Primer: za predstavljanje neoznačenih brojeva $\in$ [0,1000000] mogu se izabrati sledeći moduli:

- $m_1 = 2, m_2 = 3, M = 6$ Kako je naredni prosto broj $5 > 2^2$ to skup modula postaje
- $m_1 = 3, m_2 = 2^2, M = 12$. Pošto dinamički interval nije dovoljan, uzima se naredni prost broj 5. Nadalje se moduli uzimaju po istom principu.
- $m_1 = 3, m_2 = 2^2, m_3 = 5, M = 60$
- $m_1 = 3, m_2 = 2^2, m_3 = 5, m_4 = 7, M = 420$
- $m_1 = 3, m_2 = 5, m_3 = 7, m_4 = 2^3, M = 840$
- $m_1 = 5, m_2 = 7, m_3 = 2^3, m_4 = 3^2, M = 2520$
- $m_1 = 5, m_2 = 7, m_3 = 2^3, m_4 = 3^2, m_5 = 11, M = 27720$
- $m_1 = 5, m_2 = 7, m_3 = 2^3, m_4 = 3^2, m_5 = 11, m_6 = 13, M = 360360$
- $m_1 = 5, m_2 = 7, m_3 = 3^2, m_4 = 11, m_5 = 13, m_6 = 2^4, M = 720720$
- $m_1 = 5, m_2 = 7, m_3 = 3^2, m_4 = 11, m_5 = 13, m_6 = 2^4, m_7 = 17, M = 12252240$

Dinamički opseg je 12 puta veći $\longrightarrow$ može da se isključi modul $m_4 = 11$.
Dobija se RBS(17,16,13,9,7,5), i M=1113840. Broj bitova potreban za zapis kodiranih brojeva je 5+4+4+4+3+3=23.

Dalje poboljšanje:

1. Na računarima (koji su binarne mašine) brzina ne zavisi samo od broja bitova za zapis ostataka, već i od načina izbora modula.

2. Pokazuje se da moduli koji su jednaki stepenu broja 2 uprošćavaju izvodjenje aritmetičkih opercija

3. Moduli oblika $2^n - 1$ imaju nisku cenu operacija jer se sabiranje izvodi kao sabiranje n-bitne binarne vrednosti u nepotpunom komplementu

4. Ako su a i b uzajamno prosti takvi su i $2^a - 1$ i $2^b - 1 \longrightarrow$ elementi bilo koje liste relativno prostih brojeva $a_{k-1} > a_{k-2} > ... > a_1$ se biraju za k modula u RBS($2^{a_{k-1}}|2^{a_{k-1}} - 1|...|2^{a_1} - 1$)

5. Parni moduo bira najveći moguć da bi maksimizirao dinamički opseg sa datom veličinom (u broju bitova) ostatka.

Primer: za predstavljanje neoznačenih brojeva $\in$ [0,1000000] mogu se izabrati sledeći moduli:

RBS($2^3|2^3 - 1|2^2$-1)	Uzajamno prosti brojevi su3,2	M=168
RBS($2^4|2^4 - 1|2^3$-1)	Uzajamno prosti brojevi su4,3	M=1680
RBS($2^5|2^5 - 1|2^3$-1$|2^2$-1)	Uzajamno prosti brojevi su5,3,2	M=20832
RBS($2^5|2^5 - 1|2^4$-1$|2^3$-1)	Uzajamno prosti brojevi su5,4,3	M=104160
RBS($2^6|2^6 - 1|2^5$-1)	Uzajamno prosti brojevi su6,5	M=124992
RBS($2^7|2^7 - 1|2^3$-1$|2^2$-1)	Uzajamno prosti brojevi su7,3,2	M=341376
RBS($2^7|2^7 - 1|2^5$-1$|2^2$-1)	Uzajamno prosti brojevi su7,5,2	M=1511808
RBS($2^7|2^7 - 1|2^4$-1$|2^3$-1)	Uzajamno prosti brojevi su7,4,3	M=1706880

Dva poslednja sistema pokrivaju potreban opseg brojeva i zahtevaju 21 bit za predstavljanje proizvoljnog broja.

Prevodjenje brojeva

Prevodjenje brojeva iz dekadnog sistema u RBS

- Pravilo je prethodno definisano.
- $(A)_{10}$=$(A)_N = (a_n|a_{n-1}|...|a_1)_{RBS(m_n|m_{n-1}|...|m_1)}$ gde važi
  $\mathrm{a}_i = \mathrm{A} \bmod \mathrm{m}_i = |\mathrm{A}|_{m_i}, \quad \mathrm{a}_i \in [0, m_i - 1], \quad i \in [1, n]$

Prevodjenje brojeva iz binarnog sistema u RBS

Biće prikazan prevod neoznačenih binarnih brojeva, dok se brojevi zapisani u obliku znak i apsolutna vrednost prevode tako što se konvertuje apsolutna vrednost i zatim, po potrebi, komplementira dobijeni prevod.

Neka je $A = a_{n-1}...a_1a_0$ neoznačen binarni broj. Tada važi jednakost:

$$|(a_{n-1}...a_1a_0)|_m = ||2^{n-1}a_{n-1}|_m + ... + |2a_1|_m + |a_0|_m|_m \quad (1)$$

Neka su $m_i, i \in [0, k-1]$ moduli RBS. Ako se unapred izračuna i sačuva $|2^j|_{m_i}$ za svako i i j, tada ostatak $b_i = A \ mod \ m_i$ može da bude izračunat dodavanjem neke od ovih izračunatih konstanti.

Primer: izračunate vrednosti ostataka prvih deset stepena broja 2 koje supotrebne za konverziju 10-bitnog binarnog broja u intervalu [0,839] u RBS(8|7|5|3) su prikazane u narendoj tabeli.

j	2^j	$(2^j)_7$	$(2^j)_5$	$(2^j)_3$
0	1	1	1	1
1	2	2	2	2
2	4	4	4	1
3	8	1	3	2
4	16	2	1	1
5	32	4	2	2
6	64	1	4	1
7	128	2	3	2
8	256	4	1	1
9	512	1	2	2

U tabeli se nalaze samo ostaci za module 7, 5, i 3. Ostatak za moduo 8 se dobija direktno kao tri cifre najmanje težine u zapisu broja.

Primer: Prevod broja $A = (186)_{10} = (10111010)_2$ u RBS(8|7|5|3) se dobija na sledeći način:

- Ostatak A po modulu 8 je jednak 010 (tri cifre najmanje težine u binarnom zapisu broja, odnosno 2 dekadno).
- Kako je $A = 2^7 + 2^5 + 2^4 + 2^3 + 2^1$ kod izračunavanja ostaka po modulima 7,5 i 3 koristi se jednakost 1. Prema ovoj jednakosti se ostaci izračunavaju jednostavnim dodavanjem vrednosti koje se nalaze u odgovarajućim redovima za $j = 7, 5, 4, 3, 1$. Tako je

$$\begin{aligned} |A|_7 &= |2 + 4 + 2 + 1 + 2|_7 = 4 \\ |A|_5 &= |3 + 2 + 1 + 3 + 2|_5 = 1 \\ |A|_3 &= |2 + 2 + 1 + 2 + 2|_3 = 0 \end{aligned}$$

Odavde se dobija da je $A = (186)_{10} = (10111010)_2 = (2|4|1|0)_{RBS(8|7|5|3)}$

Odredjivanje težine pozicija

- Način računanja sličan kao kod pozicionih brojčanih sistema kod kojih je težina pozicije jednaka osnovi stepenovanoj na poziciju na kojoj se nalazi cifra
- Težina pozicije i na kojoj se nalazi modul m_i jednaka vrednosti $(0|\ldots|0|1|0|\ldots|0)$
- Ovaj zapis označava da je broj koji se zapisuje deljiv sa svim ostalim modulima $m_i, i \in [0, i-1] \bigcup [i+1, n-1]$, dok se pri deljenju sa m_i dobija ostatak 1
- Na osnovu Kineske teoreme o ostacima (pojednostavljeno) težina te pozicije je jednaka umnošku proizvoda modula na ostalim pozicijama $m_{n-1} \times \ldots \times m_{i+1} \times m_{i-1} \times m_{i-2} \times \ldots \times m_1 \times m_0$ pomnoženom sa mulitplikativnim inverzom u odnosu na m$_i$.

Primeri:

1. Težine pozicija u RBS-u (8|7|5|3) su

Pozicija	Proizvod modula	Multipl. inverz	Težina pozicije
$(1 \mid 0 \mid 0 \mid 0)_{RBS(8\|7\|5\|3)}$	7*5*3=105	1	105
$(0 \mid 1 \mid 0 \mid 0)_{RBS(8\|7\|5\|3)}$	8*5*3=120	1	120
$(0 \mid 0 \mid 1 \mid 0)_{RBS(8\|7\|5\|3)}$	8*7*3=168	2	336
$(0 \mid 0 \mid 0 \mid 1)_{RBS(8\|7\|5\|3)}$	8*7*5=280	1	280

2. Težine pozicija u RBS-u (9|7|5|2) su

Pozicija	Proizvod modula	Multipl. inverz	Težina pozicije
$(1 \mid 0 \mid 0 \mid 0)_{RBS(9\|7\|5\|2)}$	7*5*2=70	4	280
$(0 \mid 1 \mid 0 \mid 0)_{RBS(9\|7\|5\|2)}$	9*5*2=90	6	540
$(0 \mid 0 \mid 1 \mid 0)_{RBS(9\|7\|5\|2)}$	9*7*2=126	1	126
$(0 \mid 0 \mid 0 \mid 1)_{RBS(9\|7\|5\|2)}$	9*7*5=315	1	315

Prevodjenje brojeva iz RBS u dekadni sistem

Vrednost svake cifre u zapisu broja pomnoži sa odgovarajućom težinom, dobijene vrednosti saberu po modulu M (koji je jednak proizvodu svih modula RBS-a).

Primeri:

1. $(1|2|4|0)_{RBS(8|7|5|3)} = 105\times1 + 120\times2 + 336\times4 + 280\times0 \bmod 840 = 9$
2. $(5|5|4|0)_{RBS(8|7|5|3)} = 105\times5 + 120\times5 + 336\times4 + 280\times0 \bmod 840 = 789$
3. $(6|6|2|2)_{RBS(8|7|5|3)} = 105\times6 + 120\times6 + 336\times2 + 280\times2 \bmod 840 = 62$
4. $(6|6|3|1)_{RBS(9|7|5|2)} = 280\times6 + 540\times6 + 126\times3 + 315\times1 \bmod 630 = 573$
5. $(8|3|0|0)_{RBS(11|5|3|2)} = 210\times8 + 66\times2 + 220\times0 + 165\times0 \bmod 330 = 228$

Prevodjenje brojeva iz RBS u binarni sistem

Prevodjenje brojeva iz RBS u binarni sistem se vrši na analogan način kao u slučaju dekadnih brojeva. U računarskim sistemima se, zbog efikasnosti, težine pozicija za najčešće primenjivane brojčane sisteme sa ostacima računaju unapred i čuvaju u memoriji. Na desnoj strani prethodnih jednakosti se dobijaju binarne vrednosti koej se množe, sabiraju i dele (zbog računanja modula). Dobjeni rezultat je vrednost broja zapisana u binarnom sisitemu.

Poredjenje brojeva u RBS

- Direktno poredjenje nije moguće: npr. $62=(6|6|2|2)_{RBS(8|7|5|3)}$ i $67=(3|4|2|1)_{RBS(8|7|5|3)}$
- Koristi se prevodjenje iz RBS u brojčanom sistemu sa promenljivom osnovom: $62=(0|4|0|2)_{BSPO(8|7|5|3)}$ i $67=(0|4|2|1)_{BSPO(8|7|5|3)}$
- Takodje se koristi aproksimativno dekodiranje pomoću kineske teoreme o ostacima.

Prednosti i nedostaci brojčanog sistema sa ostacima

Nedostaci

- Složenost za implementaciju
- Relativno loša efikasnost (u poredjenju sa drugim brojčanim sistemima) testiranja znaka broja i poredjenja veličine brojeva, otkrivanja prekoračenja i deljenja.
- ...

Prednosti

- Ne postoji problem prenosa izmedju pozicija pri sabiranju i množenju
- 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
- Mogućnost izolacije pojedinačnih cifara koje mogu da imaju grešku

Primena

- U aplikacijama koje zahtevaju otpornost na greške
- U apliakcijama u kojima se uglavnom koriste množenje i sabiranje.
- Pri obradi digitalnih signala (posebno pri radu sa digitralnim filetrima)
- U aplikacijama koje treba da preduzmu odredjenu vrstu akcije u slučaju pojave greške u računarskim sistemima (i kao takve, same moraju da budu otporne na pojavu grešaka)
- U nekim aplikacijama u oblasti telekomunikacija
- ...