1 Brojevni sistemi sa ostacima

Brojevne sisteme sa ostacima karakteriše različita osnova za svaku poziciju. Skup pozitivnih celih brojeva

$$m_n, m_{n-1}, \ldots, m_1$$

pri čemu broj $m_i,\ i=1,\dots,n$ predstavlja osnovu pozicije i, nazivamo skupom modula ili osnova i obeležavamo sa

$$RBS(m_n|m_{n-1}|\ldots|m_1)$$

Da bi se izbegla višeznačnost zapisa brojeva moduli imaju svojstvo da su uzajamno prosti

$$NZD(m_{i+1}, m_i) = 1, i = 1, ..., n-1$$

i da opadaju u odnosu na poziciju najveće težine

$$m_n > m_{n-1} > \ldots > m_1$$

U ovom sistemu se može predstaviti ukupno $M = m_n \cdot m_{n-1} \cdot \ldots \cdot m_1$ različitih vrednosti.

Dinamički interval u kome se predstavljaju brojevi može da bude:

- za neoznačene brojeve: [0, M-1]
- za označene brojeve: [-M/2, M/2 1] ili bilo koji interval oblika [-N, P], gde važi M = N + P + 1

Brojevni sistem sa ostacima zasnovan je na relaciji kongruentnosti:

$$a \equiv b \pmod{m} \Leftrightarrow m \mid (a - b)$$

i Kineskoj teoremi o ostacima.

2 Zapis brojeva

2.1 Zapis pozitivnih brojeva

Dekadni broj X se u sistemu $RBS(m_n|m_{n-1}|\ldots|m_1)$ predstavlja skupom n brojeva $(r_n|r_{n-1}|\ldots|r_1)$ gde je $r_i = X \mod m_i = |X|_{m_i}$, $i=1,\ldots,n$.

Na osnovu relacije:

$$|A \pm k \cdot m|_m = |A|_m$$

koja važi za proizvoljnu dekadnu vrednost A i moduo m, može se zaključiti sledeće:

ukoliko za dekadni broj X važi relacija X > M, umesto broja X se može posmatrati njegov ostatak pri deljenju sa M (X mod M) s obzirom da imaju istu reprezentaciju.

Zadaci:

- 1. Zapisati broj 83 u sistemu RBS(5|3|2).
 - $r_3 = 83 \mod 5 = 3$
 - $r_2 = 83 \mod 3 = 2$
 - $r_1 = 83 \mod 2 = 1$
 - $83 = (3|2|1)_{RBS(5|3|2)}$

Broj 83 predstavlja se isto kao broj 23, jer je 83 mod 30 = 23.

2. Zapisati broj 46 u sistemu RBS(6|5).

Broj 46 predstavlja se isto kao broj 16, jer je 46 mod 30 = 16.

$$46 = 16 = (4|1)_{RBS(6|5)}$$

3. Zapisati broj 538 u sistemu RBS(9|7|4).

Broj 538 predstavlja se isto kao broj 34, jer je 538 mod 252 = 34. Lakše je računati sa 34. 538 = $34 = (7|6|2)_{RBS(9|7|4)}$

4. Zapisati broj 157 u sistemu RBS(7|4|3).

Broj 157 predstavlja se isto kao broj 73, jer je 157 mod 84 = 73.

$$157 = 73 = (3|1|1)_{RBS(7|4|3)}$$

2.2 Zapis negativnih brojeva

1. Zapisati broj -83 u sistemu RBS(5|3|2).

Broj -83 se može predstaviti nalaženjem aditivnog inverza apsolutne vrednosti broja. U opštem slučaju, ako je x ostatak i m moduo, za aditivni inverz \overline{x} važi: $x+\overline{x}=0$ mod m, tj. $\overline{x}=|m-x|_m$

$$83 = (3|2|1)_{RBS(5|3|2)} \\ (-83)_{10} = \overline{(83)_{10}} = \overline{(3|2|1)}_{RBS(5|3|2)} = (\overline{3}|\overline{2}|\overline{1})_{RBS(5|3|2)} = ((5-3) \bmod 5|(3-2) \bmod 3|(2-1) \bmod 1)_{RBS(5|3|2)} = (2|1|1)_{RBS(5|3|2)}$$

Zapis broja -83 može se dobiti i komplementiranjem sa komplementacionom konstantom $M=5 \cdot 3 \cdot 2=30$. Najpre se, umesto broja 83, posmatra broj 23, pošto je najmanji pozitivan broj sa istom reprezentacijom kao broj 83.

```
23=(3|2|1)_{RBS(5|3|2)} Kako je 30-23=7,tj. 23+7=0\ mod\ 30,zapis broja 7 uRBS(5|3|2) je ujedno i zapis broja -23. Kako je 7=(2|1|1)_{RBS(5|3|2)}, sledi: -23=(2|1|1)_{RBS(5|3|2)}=-83
```

Napomena:

Može se postaviti pitanje da li reprezentacija $(2|1|1)_{RBS(5|3|2)}$ predstavlja broj 7 ili broj -23. Odgovor zavisi od toga kako se postavi dinamički interval. Interval [0, M-1] može da se podeli na dva jednaka dela u kojima će biti zapisivani brojevi A i njihova negacija \overline{A} : [0, M/2-1] - pozitivni, [M/2, M-1] - negativni.

2. Zapisati broj -46 u sistemu RBS(6|5).

```
46 = (4|1)_{RBS(6|5)} -46 = ((6-4) \mod 6|(5-1) \mod 5)_{RBS(6|5)} -46 = (2|4)_{RBS(6|5)}
```

3. Zapisati broj -538 u sistemu RBS(9|7|4).

```
\begin{array}{l} 538 = (7|6|2)_{RBS(9|7|4)} \\ -538 = ((9-7) \ mod \ 9|(7-6) \ mod \ 7|(4-2) \ mod \ 4)_{RBS(9|7|4)} \\ -538 = (2|1|2)_{RBS(9|7|4)} \end{array}
```

4. Zapisati broj -157 u sistemu RBS(7|4|3).

```
157 = (3|1|1)_{RBS(7|4|3)} -157 = ((7-3) \mod 7|(4-1) \mod 4|(3-1) \mod 3)_{RBS(7|4|3)} -157 = (4|3|2)_{RBS(7|4|3)}
```

3 Aritmetičke operacije

3.1 Sabiranje

- 1. $(3|2|2)_{RBS(7|5|3)} + (4|1|1)_{RBS(7|5|3)} = ((3+4) \mod 7|(2+1) \mod 5|(2+1) \mod 3)_{RBS(7|5|3)} = (7 \mod 7|3 \mod 5|3 \mod 3)_{RBS(7|5|3)} = (0|3|0)_{RBS(7|5|3)}$
- $2. \ (9|5|2|0)_{RBS(11|7|5|2)} + (4|6|3|1)_{RBS(11|7|5|2)} = ((9+4)\ mod\ 11|(5+6)\ mod\ 7|(2+3)\ mod\ 5|(0+1)\ mod\ 2)_{RBS(11|7|5|2)} = (13\ mod\ 11|11\ mod\ 7|5\ mod\ 5|1\ mod\ 2)_{RBS(11|7|5|2)} = (2|4|0|1)_{RBS(11|7|5|2)}$

3.2 Oduzimanje

Oduzimanje se može izvesti direktno ili kao sabiranje sa aditivnim inverzom umanjioca.

1. $(3|2|2)_{RBS(7|5|3)} - (4|1|1)_{RBS(7|5|3)}$

```
Razlika preko direktne operacije oduzimanja: (3|2|2)_{RBS(7|5|3)} - (4|1|1)_{RBS(7|5|3)} = ((3-4) \mod 7|(2-1) \mod 5|(2-1) \mod 3)_{RBS(7|5|3)} = (\overline{1}|1|1)_{RBS(7|5|3)} = (6|1|1)_{RBS(7|5|3)}
```

Razlika preko sabiranja sa aditivnim inverzom:

$$-(4|1|1)_{RBS(7|5|3)} = (4|1|1)_{RBS(7|5|3)} = (3|4|2)_{RBS(7|5|3)}$$

$$(3|2|2)_{RBS(7|5|3)} + (3|4|2)_{RBS(7|5|3)} = ((3+3) \bmod 7 | (2+4) \bmod 5 | (2+2) \bmod 3)_{RBS(7|5|3)} = (6|1|1)_{RBS(7|5|3)}$$

```
2. \ (9|5|2|0)_{RBS(11|7|5|2)} - (4|6|3|1)_{RBS(11|7|5|2)} = ((9-4)\ mod\ 11|(5-6)\ mod\ 7|(2-3)\ mod\ 5|(0-1)\ mod\ 2)_{RBS(11|7|5|2)} = (5|\overline{1}|\overline{1}|\overline{1})_{RBS(11|7|5|2)} = (5|6|4|1)_{RBS(11|7|5|2)}
```

3.3 Množenje

- 1. $(3|2|2)_{RBS(7|5|3)} \cdot (4|1|1)_{RBS(7|5|3)} = ((3 \cdot 4) \mod 7 | (2 \cdot 1) \mod 5 | (2 \cdot 1) \mod 3)_{RBS(7|5|3)} = (5|2|2)_{RBS(7|5|3)}$
- 2. $(9|5|2|0)_{RBS(11|7|5|2)} \cdot (4|6|3|1)_{RBS(11|7|5|2)} = ((9 \cdot 4) \mod 11|(5 \cdot 6) \mod 7|(2 \cdot 3) \mod 5|0)_{RBS(11|7|5|2)} = (3|2|1|0)_{RBS(11|7|5|2)}$

3.4 Deljenje (samo ideja)

Prilikom deljenja, dobijeni rezultat predstavlja količnik samo ako je u pitanju ceo broj, što nije uvek slučaj. S obzirom da nije opisan precizan algoritam za deljenje, posmatra se samo ideja.

```
1. Izračunati 3:4\pmod{5} 3:4\equiv x\pmod{5} 3\equiv 4x\pmod{5} 2\equiv x=0:3\equiv 0\pmod{5} 2\equiv x=1:3\equiv 4\pmod{5} 2\equiv x=1:3\equiv 4\pmod{5} 2\equiv x=1:3\equiv 4\pmod{5} 2\equiv x=1:3\equiv 2\pmod{5} 2\equiv x=1:3\equiv 2\pmod{5} 2\equiv x=1:3\equiv 2\pmod{5} (u odnosu na relaciju kongruentnosti ovo jeste tačno, ali ne može se uzeti za traženi količnik)
```

Prilikom određivanja količnika može se koristiti i multiplikativni inverz:

Ako su A i m uzajamno prosti ne-nula brojevi, A^{-1} je multiplikativni inverz broja A u odnosu na moduo m ako važi: $|A \cdot A^{-1}|_m = 1$

Kongruencija: $3 \equiv 4x \pmod{5}$

može da se reši ako se obe strane pomnože multiplikativnim inverzom broja 4 u odnosu na moduo 5. Kako je $4^{-1} = 4 \mod 5$, sledi:

```
3 \cdot 4^{-1} \equiv x \pmod{5}3 \cdot 4 \equiv x \pmod{5}2 \equiv x \pmod{5} \Rightarrow 3 : 4 \equiv 2 \pmod{5}
```

2. Izračunati 5 : 2 (mod 7)

```
\begin{array}{l} 5:2\equiv x\;(mod\;7)\\ 5\equiv 2x\;(mod\;7)\\ \text{za}\;x=0\colon 5\equiv 0\;(mod\;7)\perp\\ \text{za}\;x=1\colon 5\equiv 2\;(mod\;7)\perp\\ \text{za}\;x=2\colon 5\equiv 4\;(mod\;7)\perp\\ \text{za}\;x=3\colon 5\equiv 6\;(mod\;7)\perp\\ \text{za}\;x=4\colon 5\equiv 8\;(mod\;7)\perp\\ \text{za}\;x=5\colon 5\equiv 10\;(mod\;7)\perp\\ \text{za}\;x=6\colon 5\equiv 12\;(mod\;7) \\ \Rightarrow\;5\colon 2\equiv 6\;(mod\;7) \end{array}
```

3. Izračunati 9 : 5 (mod 11)

```
\begin{array}{l} 9:5\equiv x\ (mod\ 11)\\ 9\equiv 5x\ (mod\ 11)\\ \text{za } x=0\colon 9\equiv 0\ (mod\ 11)\ \bot\\ \text{za } x=1\colon 9\equiv 5\ (mod\ 11)\ \bot\\ \text{za } x=2\colon 9\equiv 10\ (mod\ 11)\ \bot\\ \text{za } x=3\colon 9\equiv 15\ (mod\ 11)\ \bot\\ \text{za } x=4\colon 9\equiv 20\ (mod\ 11)\ \top\\ \Rightarrow 9:5\equiv 4\ (mod\ 11) \end{array}
```

4. Izračunati 7 : 5 (mod 9)

```
7: 5 \equiv x \pmod{9}

7: 5 \equiv x \pmod{9}

7 \equiv 5x \pmod{9}

2a x = 0: 7 \equiv 0 \pmod{9} \perp

2a x = 1: 7 \equiv 5 \pmod{9} \perp
```

```
za x = 2: 7 \equiv 10 \pmod{9} \perp

za x = 3: 7 \equiv 15 \pmod{9} \perp

za x = 4: 7 \equiv 20 \pmod{9} \perp

za x = 5: 7 \equiv 25 \pmod{9} \perp

\Rightarrow 7 : 5 \equiv 5 \pmod{9}
```

5. $(3|2|2)_{RBS(7|5|3)}: (4|1|1)_{RBS(7|5|3)} = ((3:4) \mod 7 | (2:1) \mod 5 | (2:1) \mod 3)_{RBS(7|5|3)} = (6|2|2)_{RBS(7|5|3)},$ jer je:

```
3: 4 \equiv x \pmod{7}3 \equiv 4x \pmod{7} \Rightarrow x = 6
```

6. $(9|5|2|0)_{RBS(11|7|5|2)}: (4|6|3|1)_{RBS(11|7|5|2)} = ((9:4) \mod 11|(5:6) \mod 7|(2:3) \mod 5|0)_{RBS(11|7|5|2)} = (5|2|4|0)_{RBS(11|7|5|2)},$ jer je:

```
9: 4 \equiv x \pmod{11}
9 \equiv 4x \pmod{11} \Rightarrow x = 5
5: 6 \equiv y \pmod{7}
5 \equiv 6y \pmod{7} \Rightarrow y = 2
2: 3 \equiv z \pmod{5}
2 \equiv 3z \pmod{5} \Rightarrow z = 4
```

Jednačine oblika $ax = c \pmod{b}$ se strogo matematički svode na jednačine oblika ax = c + by tj. ax - by = c koje su poznate kao linearne Diofantove jednačine. Važi teorema:

Potreban i dovoljan uslov da linearna Diofantova jednačina ax + by = c ima rešenja je NZD(a,b)|c.

Ako su brojevi a i b uzajamno prosti (NZD(a,b)=1) linearna Diofantova jednačina uvek ima rešenja.

4 Odredjivanje dekadne vrednosti RBS brojeva

Da bi odredili dekadnu vrednost broja $(r_n|r_{n-1}|\dots|r_1)$ zapisanog u sistemu $RBS(m_n|m_{n-1}|\dots|m_1)$ neophodno je odrediti težinu svake pozicije u zapisu broja. Pozicija i na kojoj se nalazi modul m_i ima težinu t_i čija je vrednost $(0|0|\dots|0|1|0|\dots|0)$. Iz zapisa $(0|0|\dots|0|1|0|\dots|0)$ se može zakljuciti da je

$$t_i \bmod m_j = 0$$
, za sve $j = 1, \dots, n$, $j \neq i$

$$t_i \bmod m_i = 1$$

Na osnovu Kineske teoreme o ostacima ¹ postoji jedinstven broj po modulu $m_n \cdot m_{n-1} \cdot \cdots \cdot m_1$ sa ovim svojstvima.

Zadaci:

1. Odrediti težine pozicija u sistemu RBS(7|5|3).

```
\begin{split} t_3 &= (1|0|0)_{RBS(7|5|3)} \\ t_3 &= 1 \pmod{7} \\ t_3 &= 0 \pmod{5} \\ t_3 &= 0 \pmod{3} \end{split} \Rightarrow broj je deljiv sa 3 i 5 pa je deljiv i sa 3 \cdot 5 = 15, što znači da je oblika 15k15k \equiv 1 \pmod{7} \Leftrightarrow k \equiv 1 \pmod{7} \text{ (jer je 15} \equiv 1 \pmod{7}) \Rightarrow k = 1
```

¹Kineska teorema o ostacima: Neka su m_1, m_2, \ldots, m_n po parovima uzajamno prosti prirodni brojevi i a_1, a_2, \ldots, a_n bilo koji celi brojevi. Tada postoji jedinstven po modulu $m_n \cdot m_{n-1} \cdots m_1$ broj x takav da je $x \equiv a_i \pmod{m_i}$.

```
težina t_3 je 15 \cdot k = 15 \cdot 1 = 15
    t_2 = (0|1|0)_{RBS(7|5|3)}
    t_2 = 0 \; (mod \; 7)
    t_2 = 1 \; (mod \; 5)
    t_2 = 0 \ (mod \ 3)
    \Rightarrow broj je deljiv sa 7 i 3, pa je deljiv i sa 7 \cdot 3 = 21, što znači da je oblika 21k
    21k \equiv 1 \pmod{5} \Leftrightarrow k \equiv 1 \pmod{5} (jer je 21 \equiv 1 \pmod{5}) \Rightarrow k = 1
    težina t_2 je 21 \cdot k = 21 \cdot 1 = 21
    t_1 = (0|0|1)_{RBS(7|5|3)}
    t_1 = 0 \ (mod \ 7)
    t_1 = 0 \ (mod \ 5)
    t_1 = 1 \; (mod \; 3)
    \Rightarrow broj je deljiv sa 7 i 5, pa je deljiv i sa 7 \cdot 5 = 35, što znači da je oblika 35k
    35k \equiv 1 \pmod{3} \Leftrightarrow 2k \equiv 1 \pmod{3} \text{ (jer je } 35 \equiv 2 \pmod{3}) \Rightarrow k = 2
    težina t_1 je 35 \cdot k = 35 \cdot 2 = 70
2. Odrediti dekadnu vrednost broja (3|2|2)_{RBS(7|5|3)}.
    Iz prethodnog primera, težine pozicija sistema su: t_3=15,\,t_2=21,\,t_1=70
    (3|2|2)_{RBS(7|5|3)} = (3 \cdot 15 + 2 \cdot 21 + 2 \cdot 70) \mod 7 \cdot 5 \cdot 3 = 227 \mod 105 = 17
3. Odrediti težine pozicija u sistemu RBS(11|9|7|4).
    t_4 = (1|0|0|0)_{RBS(11|9|7|4)}
    t_4 = 1 \; (mod \; 11)
    t_4 = 0 \ (mod \ 9)
    t_4 = 0 \; (mod \; 7)
    t_4 = 0 \ (mod \ 4)
    \Rightarrowbroj je deljiv sa 9, 7 i 4, pa je deljiv i sa 9 · 7 · 4 = 252, što znači da je oblika 252k
    252k \equiv 1 \pmod{11} \Leftrightarrow 10k \equiv 1 \pmod{11} (jer je 252 \equiv 10 \pmod{11}) \Rightarrow k = 10
    težina t_4 je 252 \cdot k = 252 \cdot 10 = 2520
    t_3 = (0|1|0|0)_{RBS(11|9|7|4)}
    t_3 = 0 \ (mod \ 11)
    t_3 = 1 \; (mod \; 9)
    t_3 = 0 \ (mod \ 7)
    t_3 = 0 \ (mod \ 4)
    \Rightarrow broj je deljiv sa 11, 7 i 4, pa je deljiv i sa 11 \cdot 7 \cdot 4 = 308, što znači da je oblika 308k
    308k \equiv 1 \pmod{9} \Leftrightarrow 2k \equiv 1 \pmod{9} (jer je308 \equiv 2 \pmod{9}) \Rightarrow k = 5
    težina t_3 je 308 \cdot k = 308 \cdot 5 = 1540
```

```
t_2 = (0|0|1|0)_{RBS(11|9|7|4)}
t_2 = 0 \ (mod \ 11)
t_2 = 0 \ (mod \ 9)
t_2 = 1 \; (mod \; 7)
t_2 = 0 \ (mod \ 4)
\Rightarrowbroj je deljiv sa 11, 9 i 4, pa je deljiv i sa 11 · 9 · 4 = 396, što znači da je oblika 396k
396k \equiv 1 \pmod{7} \Leftrightarrow 4k \equiv 1 \pmod{7} (jer je 396 \equiv 4 \pmod{7}) \Rightarrow k = 2
težina t_2 je 396 \cdot k = 396 \cdot 2 = 792
t_1 = (0|0|0|1)_{RBS(11|9|7|4)}
t_1 = 0 \ (mod \ 11)
t_1 = 0 \ (mod \ 9)
t_1 = 0 \; (mod \; 7)
t_1 = 1 \; (mod \; 4)
\Rightarrow broj je deljiv sa 11, 9 i 7, pa je deljiv i sa 11 \cdot 9 \cdot 7 = 693, što znači da je oblika 693k
693k \equiv 1 \pmod{4} \Leftrightarrow k \equiv 1 \pmod{4} \text{ (jer je } 693 \equiv 1 \pmod{4}) \Rightarrow k = 1
težina t_1 je 693 \cdot k = 693 \cdot 1 = 693
```

4. Odrediti dekadnu vrednost broja $(5|1|4|1)_{RBS(11|9|7|4)}$.

Iz prethodnog primera, težine pozicija sistema su: $t_4=2520,\,t_3=1540,\,t_2=792,\,t_1=693$

$$(5|1|4|1)_{RBS(11|9|7|4)} = (5 \cdot 2520 + 1 \cdot 1540 + 4 \cdot 792 + 1 \cdot 693) \ mod \ 11 \cdot 9 \cdot 7 \cdot 4 = 18001 \ mod \ 2772 = 1369 \cdot 111 \cdot 1$$

5. Izračunati 17 · (-6) u brojevnom sistemu sa ostacima 11, 5, 3 i 2.

```
\begin{split} &17 = (6|2|2|1)_{RBS(11|5|3|2)} \\ &6 = (6|1|0|0)_{RBS(11|5|3|2)} \Rightarrow -6 = ((11-6) \ mod \ 11|(5-1) \ mod \ 5|0|0)_{RBS(11|5|3|2)} = (5|4|0|0)_{RBS(11|5|3|2)} \\ &17 \cdot (-6) = (6|2|2|1)_{RBS(11|5|3|2)} \cdot (5|4|0|0)_{RBS(11|5|3|2)} = \\ &((6 \cdot 5) \ mod \ 11|(2 \cdot 4) \ mod \ 5|0|0)_{RBS(11|5|3|2)} = (8|3|0|0)_{RBS(11|5|3|2)} \\ &\text{težine pozicija:} \end{split}
```

t_4	(1 0 0 0)	$t_4 = 5 \cdot 3 \cdot 2 \cdot k = 30k, \ 30k \equiv 1 \ (mod \ 11), \ 8k \equiv 1 \ (mod \ 11), \ k = 7, \ t_4 = 210$
t_3	(0 1 0 0)	$t_3 = 11 \cdot 3 \cdot 2 \cdot k = 66k, 66k \equiv 1 \pmod{5}, k \equiv 1 \pmod{5}, k = 1, t_3 = 66$
t_2	(0 0 1 0)	$t_2 = 11 \cdot 5 \cdot 2 \cdot k = 110k, \ 110k \equiv 1 \ (mod \ 3), \ 2k \equiv 1 \ (mod \ 3), \ k = 2, \ t_2 = 220$
t_1	(0 0 0 1)	$t_1 = 11 \cdot 5 \cdot 3 \cdot k = 165k, \ 165k \equiv 1 \ (mod \ 2), \ k \equiv 1 \ (mod \ 2), \ k = 1, \ t_1 = 165$

dekadna vrednost rezultata:

 $(8|3|0|0)_{RBS(11|5|3|2)} = (8 \cdot 210 + 3 \cdot 66 + 0 \cdot 220 + 0 \cdot 165) \ mod \ 11 \cdot 5 \cdot 3 \cdot 2 = 1878 \ mod \ 330 = 228$ Polazni brojevi su bili različitog znaka, pa rezultat treba da bude negativan.

Konačno se dobija: 228 - 330 = -102.