

Uvod u organizaciju i arhitekturu računara 1

Stefan Mišković

2020/2021.

6 Zapis brojeva pomoću ostatka

Podsetimo se najpre oznaka vezanih za modularnu aritmetiku. Ako je $r = a \bmod m$, kažemo da je r ostatak pri celobrojnom deljenju broja a brojem m . Na primer, za $11 \bmod 3 = 2$ je $a = 11$, $m = 3$ i $r = 2$. Ako je $a \equiv b \pmod{m}$, tada brojevi a i b daju isti ostatak pri deljenju brojem m . Na primer, važi da je $11 \equiv 2 \pmod{3}$ ili $11 \equiv 20 \pmod{3}$, dok je $11 \not\equiv 4 \pmod{3}$.

Neka je dat skup celih brojeva m_1, m_2, \dots, m_n koji su veći od 1, za koje je $m_1 < m_2 < \dots < m_n$. Zapis $\text{RBS}(m_n|m_{n-1}|\dots|m_2|m_1)$ označava brojčani sistem sa ostacima $m_n, m_{n-1}, \dots, m_2, m_1$. Ceo dekadni broj a se tako u navedenom sistemu zapisuje pomoću n cifara sa

$$(a_n|a_{n-1}|\dots|a_2|a_1)_{\text{RBS}(m_n|m_{n-1}|\dots|m_2|m_1)},$$

pri čemu je $a_i = a \bmod m_i$ za $1 \leq i \leq n$. Jasno je da mora važiti da je $0 \leq a_i < m_i$.

Brojevi m_i se mogu izabrati proizvoljno, a zapis može biti proizvoljne dužine. Na primer, za RBS dužine 4, pri čemu su moduli redom jednaki 8, 7, 5 i 3, dekadni broj 62 se zapisuje kao

$$(6|6|2|2)_{\text{RBS}(8|7|5|3)},$$

budući da je redom $62 \bmod 8 = 6$, $62 \bmod 7 = 6$, $62 \bmod 5 = 2$ i $62 \bmod 3 = 2$. Isti dekadni broj se može zapisati i u, na primer, zapisu $\text{RBS}(9|8|7)$. Kako je $62 \bmod 9 = 8$, $62 \bmod 8 = 6$ i $62 \bmod 7 = 6$, to je

$$(62)_{10} = (8|6|6)_{\text{RBS}(9|8|7)}.$$

Da bi se izbegla višeznačnost zapisa, odnosno pojava da dva različita dekadna broja imaju isti RBS zapis, moduli brojeva moraju da budu uzajamno prosti. Drugim rečima, treba da važi $\text{NZD}(m_i, m_j) = 1$ za sve $i \neq j$. Neka je

$$m = \prod_{i=1}^n m_i = m_1 \cdot m_2 \cdot \dots \cdot m_n.$$

Ako su parovi modula uzajamno prosti, na ovaj način se može predstaviti bilo koji interval od m uzastopnih brojeva. Na primer, ukoliko treba predstaviti neoznačene brojeve, može se uzeti interval $[0, m-1]$, a za označene interval $[-m/2, m/2-1]$. Ukoliko izlazimo van nekog intervala od m uzastopnih brojeva, zapis takođe ne može biti jednoznačan. Tako će, na primer, svi brojevi iz intervala $[0, m-1]$, $[m, 2m-1]$ i $[2m, 3m-1]$ imati isti zapis.

6.1 Modularna aritmetika

Zapis negativnih brojeva. Za zapis negativnog dekadnog broja, prvo se vrši prevođenje odgovarajućeg pozitivnog broja, nakon čega se svakoj od dobijenih cifara u RBS zapisu promeni znak. Nakon toga se rezultat dobija tako što se svaka cifra iz RBS zapisa zameni onom koja joj je jednaka po modulu m_i , a koja se nalazi u intervalu $[0, m_i - 1]$.

Na primer, neka je potrebno zapisati dekadni broj -538 u sistemu $\text{RBS}(9|7|4)$. Najpre ćemo odgovarajući pozitivan broj 538 zapisati u tom sistemu. Važi da je $538 \bmod 9 = 7$, $538 \bmod 7 = 6$ i $538 \bmod 4 = 2$, pa je zapis pozitivnog broja $(538)_{10} = (7|6|2)_{\text{RBS}(9|7|4)}$. Za zapis negativnog broja, najpre je potrebno promeniti znak svakoj od cifara 7 , 6 i 2 . Dobija se da je $(-538)_{10} = (-7|-6|-2)_{\text{RBS}(9|7|4)}$. Nenegativan ceo broj manji od 9 koji pri deljenju sa 9 daje isti ostatak kao -7 je 2 . Slično je i $-6 \equiv 1 \pmod{7}$ i $-2 \equiv 2 \pmod{4}$, pa je konačno $(-538)_{10} = (2|1|2)_{\text{RBS}(9|7|4)}$.

Sabiranje. Za bilo koju od operacija sabiranja, oduzimanja, množenja i deljenja, potrebno je da dva broja budu u RBS zapisu sa istim modulima. Ako su dati brojevi $(a_n|a_{n-1}|\dots|a_2|a_1)$ i $(b_n|b_{n-1}|\dots|b_2|b_1)$ u zapisu $\text{RBS}(m_n|m_{n-1}|\dots|m_2|m_1)$, vrednost njihovog zbira je broj $(c_n|c_{n-1}|\dots|c_2|c_1)$, gde je $c_i = (a_i + b_i) \bmod m_i$, $1 \leq i \leq n$. Na primer, važi da je $(3|2|2)_{\text{RBS}(7|5|3)} + (4|1|1)_{\text{RBS}(7|5|3)} = (3+4|2+1|2+1)_{\text{RBS}(7|5|3)} = (7|3|3)_{\text{RBS}(7|5|3)} = (0|3|0)_{\text{RBS}(7|5|3)}$.

Oduzimanje. Ako su dati brojevi $(a_n|a_{n-1}|\dots|a_2|a_1)$ i $(b_n|b_{n-1}|\dots|b_2|b_1)$ u brojanom sistemu $\text{RBS}(m_n|m_{n-1}|\dots|m_2|m_1)$, vrednost njihove razlike je $(c_n|c_{n-1}|\dots|c_2|c_1)$, gde je $c_i = (a_i - b_i) \bmod m_i$, $1 \leq i \leq n$. Ako se pri oduzimanju $a_i - b_i$ dobije negativna cifra, ona se dopunjuje do pozitivne, slično kao u zapisu negativnog broja. Na primer, važi da je $(3|2|2)_{\text{RBS}(7|5|3)} - (4|1|1)_{\text{RBS}(7|5|3)} = (3-4|2-1|2-1)_{\text{RBS}(7|5|3)} = (-1|1|1)_{\text{RBS}(7|5|3)} = (6|1|1)_{\text{RBS}(7|5|3)}$.

Množenje. Ako su brojevi $(a_n|a_{n-1}|\dots|a_2|a_1)$ i $(b_n|b_{n-1}|\dots|b_2|b_1)$ zapisani u brojanom sistemu $\text{RBS}(m_n|m_{n-1}|\dots|m_2|m_1)$, njihov proizvod je broj $(c_n|c_{n-1}|\dots|c_2|c_1)$, pri čemu je $c_i = (a_i \cdot b_i) \bmod m_i$, $1 \leq i \leq n$. Na primer, važi da je $(3|2|2)_{\text{RBS}(7|5|3)} \cdot (4|1|1)_{\text{RBS}(7|5|3)} = (3 \cdot 4|2 \cdot 1|2 \cdot 1)_{\text{RBS}(7|5|3)} = (12|2|2)_{\text{RBS}(7|5|3)} = (5|2|2)_{\text{RBS}(7|5|3)}$.

Deljenje. Sa operacijom deljenja u RBS zapisu treba biti obazriv. Ona se ovde izvršava znatno sporije od sabiranja, oduzimanja i množenja, a često ne mora biti ni definisana. Da bi bila definisana, potrebno je da odgovarajući par brojeva bude deljiv u smislu koji će u nastavku biti opisan. Ako su dati brojevi $(a_n|a_{n-1}|\dots|a_2|a_1)$ i $(b_n|b_{n-1}|\dots|b_2|b_1)$ u zapisu $\text{RBS}(m_n|m_{n-1}|\dots|m_2|m_1)$, vrednost njihovog količnika je $(c_n|c_{n-1}|\dots|c_2|c_1)$, gde je $c_i = (a_i/b_i) \bmod m_i$, $1 \leq i \leq n$. Zapis $c_i = (a_i/b_i) \bmod m_i$ znači zapravo da je c_i , ukoliko postoji, rešenje jednačine $a_i \equiv b_i c_i \pmod{m_i}$. Ukoliko za sve $1 \leq i \leq n$ takvo c_i postoji, može se izvršiti deljenje. Najjednostavniji način za nalaženje takve vrednosti c_i je da se redom pokušava sa nenegativnim celim brojevima, počev od 0 pa naviše.

Na primer, neka je potrebno izvršiti deljenje $(9|5|2|0)_{\text{RBS}(11|7|5|2)}$ i $(4|6|3|1)_{\text{RBS}(11|7|5|2)}$. Za vrednost prve cifre sleva rezultata, treba pronaći cifru x takvu da je $9 \equiv 4x \pmod{11}$. Neposrednom proverom se proverava da $x = 0$, $x = 1$, $x = 2$, $x = 3$ i $x = 4$ nisu rešenja jednačine, a da $x = 5$ jeste, budući da je $9 \equiv 20 \pmod{11}$. Na sličan način se rešavanjem jednačina $5 \equiv 6x \pmod{7}$, $2 \equiv 3x \pmod{5}$ i $0 \equiv 1x \pmod{2}$ dobijaju redom rešenja 2 , 4 i 0 , pa je količnik jednak $(5|2|4|0)_{\text{RBS}(11|7|5|2)}$.

Aditivni i multiplikativni inverz. Usko sa operacijama sabiranja i oduzimanja se vezuje pojam aditivnog inverza, a usko sa operacijama množenja i deljenja pojam multiplikativnog inverza. U skupu realnih brojeva, aditivni inverz je broj koji ima suprotan znak. U ovom kontekstu, aditivni inverz broja a po modulu m je broj \bar{a} , takav da je $a \equiv -\bar{a} \pmod{m}$ i $0 \leq \bar{a} < m$. Na primer, aditivni inverz broja 6 po modulu 8 je 2, jer je $6 \equiv -2 \pmod{8}$ i $0 \leq 2 < 8$. Multiplikativni inverz nekog broja u skupu realnih brojeva je njegova recipročna vrednost. Kod RBS zapisa, multiplikativni inverz broja a po modulu m je broj a^{-1} takav da je $aa^{-1} \equiv 1 \pmod{m}$. Broj a^{-1} se bira slično kao količnik kod deljenja – isprobavaju se svi celi brojevi počev od 0 pa naviše. Da bi multiplikativni inverz bio definisan, potrebno je da brojevi a i m budu uzajamno prosti.

6.2 Prevođenje brojeva

Prevođenje brojeva iz dekadnog sistema u RBS zapis je već opisano. U nastavku će biti opisano direktno prevođenje iz binarnog sistema u RBS zapis, kao i prevođenje iz RBS zapisa u dekadni sistem.

Prevođenje iz binarnog sistema u RBS. Ako je dat binarni broj

$$(a)_2 = (a_{n-1} \dots a_1 a_0)_2,$$

njegova dekadna vrednost iznosi

$$(a)_{10} = 2^{n-1}a_{n-1} + \dots + 2^1a_1 + 2^0a_0.$$

Primetimo da, ukoliko želimo da izračunamo vrednost $(a)_{10} \bmod m$, dovoljno je za svaki sabirak izračunati $2^i a_i \bmod m$, a zatim odrediti zbir takvih sabiraka po modulu m . Formulom bi se ovo moglo zapisati u obliku

$$(a)_{10} \bmod m = \left(\sum_{i=0}^{n-1} (2^i a_i \bmod m) \right) \bmod m.$$

Odavde sledi da je u binarnom zapisu $(a_{n-1} \dots a_1 a_0)_2$ dovoljno posmatrati stepene 2^i uz koje je $a_i = 1$. Sabiranjem njihovih ostataka po modulu m se dobija i vrednost ostatka deljenja broja a po modulu m .

Na primer, neka je potrebno prevesti broj $a = (10111010)_2$ u zapis RBS(8|7|5|3). Najpre primetimo da se $a \bmod 8$ može jednostavno izračunati, budući da je dovoljno posmatrati njegove poslednje tri cifre u binarnom sistemu. Kako je $(010)_2 = (2)_{10}$, to je $a \bmod 8 = 2$. Ovo je zapravo ekvivalentno činjenici da se u dekadnom sistemu ostatak pri deljenju sa 1000 određuje tako što se posmatraju poslednje tri cifre, budući da je dekadni broj 8 u binarnom sistemu jednak 1000. Za određivanje ostataka pri deljenju sa 7, 5 i 3, potrebno je najpre primetiti da je $a = 2^7 + 2^5 + 2^4 + 2^3 + 2^1$. U nastavku ćemo kreirati tabelu vrednosti stepena 2^i , $0 \leq i \leq 7$ pri deljenju sa 7, 5 i 3:

i	2^i	$2^i \bmod 7$	$2^i \bmod 5$	$2^i \bmod 3$
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

Iz tabele sada jednostavno sledi:

- $a \bmod 7 = (2 + 4 + 2 + 1 + 2) \bmod 7 = 4$,
- $a \bmod 5 = (3 + 2 + 1 + 3 + 2) \bmod 5 = 1$,
- $a \bmod 3 = (2 + 2 + 1 + 2 + 2) \bmod 3 = 0$,

pa je traženi zapis $(2|4|1|0)_{\text{RBS}(8|7|5|3)}$.

Prevođenje iz RBS u dekadni sistem. Za određivanje dekadne vrednosti zapisa

$$(a_n|a_{n-1}|\dots|a_2|a_1)_{\text{RBS}(m_n|m_{n-1}|\dots|m_2|m_1)}$$

potrebno je odrediti vrednosti težina $t_n, t_{n-1}, \dots, t_2, t_1$. Težina t_i je dekadni broj čiji je zapis

$$(0|\dots|0|1|0|\dots|0)_{\text{RBS}(m_n|m_{n-1}|\dots|m_2|m_1)}.$$

Zapis je takav da se na i -toj poziciji nalazi vrednost 1, a na svim ostalim vrednost 0. Odavde sledi da je $t_i \bmod m_i = 1$ i $t_j \bmod m_j = 0$ za $j \neq i$. Nakon što se pronađu vrednosti težina, dekadna vrednost broja iznosi

$$\left(\sum_{i=1}^n a_i t_i \right) \bmod m, \text{ gde je } m = \prod_{i=1}^n m_i.$$

Neka je, na primer, potrebno odrediti dekadnu vrednost broja $(3|2|2)_{\text{RBS}(7|5|3)}$. Za težinu t_3 važi $t_3 = (1|0|0)_{\text{RBS}(7|5|3)}$, odakle sledi da je $t_3 \equiv 1 \pmod{7}$, $t_3 \equiv 0 \pmod{5}$ i $t_3 \equiv 0 \pmod{3}$. Kako je t_3 deljivo sa 3 i sa 5, a 3 i 5 su uzajamno prosti brojevi, zaključujemo da je t_3 oblika $15k$. Zamenom u prvu jednačinu sledi $15k \equiv 1 \pmod{7}$, pa je $k = 1$ (redom se probaju vrednosti za k počev od 0 pa naviše) i $t_3 = 15 \cdot 1 = 15$. Na sličan način se dobija da je $t_2 = 21$ i $t_1 = 70$. Konačno je

$$(3|2|2)_{\text{RBS}(7|5|3)} = (3 \cdot 15 + 2 \cdot 21 + 2 \cdot 70) \bmod (7 \cdot 5 \cdot 3) = 227 \bmod 105 = 17.$$

Primetimo i da je rešenje bilo koji broj koji je oblika $17 + 105k$, $k \in \mathbb{Z}$.

6.3 Izbor modula

Pretpostavimo da je potrebno predstaviti cele dekadne brojeve iz intervala $[0, 1000000]$. Budući da je vrednost 2^{20} nešto veća od 1000000, sledi da binarni zapis dekadnog broja 1000000 ima 20 cifara, što znači da je toliko bitova potrebno za predstavljanje brojeva iz navedenog intervala na klasičan način.

U nastavku će biti dato nekoliko pristupa za što efikasnije predstavljanje brojeva iz navedenog intervala u računar u pomoću RBS zapisa. Da bi se navedeni brojevi mogli predstaviti, potrebno je da proizvod modula bude veći od 1000000, a zbog jednoznačnosti, da su moduli uzajamno prosti brojevi. Pokušajmo sa nekoliko pristupa izbora modula koji zadovoljavaju ovaj uslov.

- Pokušajmo sa izborom prvih nekoliko prostih brojeva dok njihov proizvod ne pređe 1000000. Ispostavlja se da je $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = 9699690$ prvi takav izbor koji se nameće. Međutim, primetimo da se na ovaj način može predstaviti više od 9 puta više brojeva nego što ih ima u intervalu. Zbog toga je najpogodnije iz izbora modula izostaviti broj 7, a ostaviti sve ostale proste brojeve. Dobija se zapis RBS(19, 17, 13, 11, 5, 3, 2), čiji je proizvod modula 1385670. Imajući u vidu koliko svaki od modula zauzima bitova, ukupan broj bitova potrebnih za zapis na ovakav način iznosi $5 + 5 + 4 + 4 + 3 + 2 + 1 = 24$.
- Pokušajmo sada sa izborom prvih nekoliko brojeva koji su prosti ili stepeni prostih brojeva. Za prvi takav pogodan izbor važi $5 \cdot 7 \cdot 3^2 \cdot 11 \cdot 13 \cdot 2^4 \cdot 17 = 12252240$. Kako je proizvod takvih brojeva nešto više od 12 puta veći od navedenog intervala, najpogodnije je iz izbora modula izbaciti broj 11. Na taj način se dobija zapis RBS(17, 16, 13, 9, 7, 5) čiji je proizvod modula 1113840. Ovaj zapis zauzima 23 bita.
- U računar je pogodno birati module oblika 2^i ili $2^i - 1$, kako zbog bolje iskorišćenosti memorije, tako i zbog efikasnijeg izvršavanja operacija. Podsetimo se i da su ove vrednosti i komplementacione konstante kod potpunog, odnosno nepotpunog komplementa. Potrebno je voditi računa da moduli treba da budu uzajamno prosti brojevi. Može se primetiti da će 2^i ili $2^i - 1$ (za isti stepen i) uvek biti uzajamno prosti. Dodatno, važi da ako su brojevi i i j uzajamno prosti, takvi su i brojevi $2^i - 1$ i $2^j - 1$. Na ovaj način se mogu pogodno izabrati uzajamno prosti brojevi $a_{n-1} > \dots > a_1 > a_0$ i konstruisati zapis RBS($2^{a_{n-1}}|2^{a_{n-1}}-1| \dots |2^{a_1}-1|2^{a_0}-1$). Tako se, na primer, za uzajamno proste brojeve 7, 5 i 2 dobija zapis RBS($2^7|2^7-1|2^5-1|2^2-1$), čiji je proizvod modula 1511808. Ovaj zapis zauzima 21 bit.

6.4 Prednosti, mane i primene

Osnovne prednosti ovog zapisa se ogledaju u efikasnom izvršavanju operacija sabiranja, oduzimanja i množenja. Čak i za velike brojeve, cifre su veoma male, a prenos kod sabiranja i množenja ne postoji. Osnovna mana je što su operacije poput deljenja izuzetno spore i složene za implementaciju. Nedostatak je i to što je u odnosu na standardni način zapisa zauzeće memorije veće. Zbog toga je i primena ovog zapisa najčešće tamo gde se vrši samo sabiranje, oduzimanje i množenje, a gde nema deljenja. Neke od takvih primena su u obradi digitalnih signala i u oblasti telekomunikacija.