POZNAN UNIVERSITY OF TECHNOLOGY ACADEMIC JOURNALS
No 76 Electrical Engineering 2013

Mirosław PLEBANEK*

# OKREŚLANIE PARZYSTOŚCI LICZB W RESZTOWYM SYSTEMIE LICZBOWYM Z WYKORZYSTANIEM KONWERSJI DO SYSTEMU Z MIESZANYMI PODSTAWAMI

W artykule przedstawiono metodę konwersji liczb z systemu resztowego do systemu z mieszanymi podstawami. Następnie zaprezentowano dwie metody konwersji liczb z systemu z mieszanymi podstawami do systemu dziesiętnego, oraz metodę określania parzystości i porównywania liczb zapisanych w systemie z mieszanymi podstawami.

## 1. WSTĘP

Resztowy system liczbowy (ang. the Residue Number System, RNS) został stworzony w celu przyspieszenia obliczeń arytmetycznych w układach elektroniki. Jego zaletą jest możliwość wykonywania dodawania, mnożenia i dzielenia z pominięciem przeniesień. Z kolei operacje takie jak dzielenie lub porównywanie liczb są znacznie trudniejsze do realizacji niż w systemach wagowych. Przykładowo porównanie dwóch liczb w systemie wagowym polega na sprawdzeniu wartości cyfr dla najbardziej znaczących wag, w RNS nie da się w prosty sposób porównać liczb na podstawie ich reprezentacji.

Najłatwiejszym sposobem porównania dwóch liczb w RNS jest ich konwersja do systemu wagowego np.: przy pomocy chińskiego twierdzenia o resztach (ang. Chinese Reminder Theorem, CRT) i porównanie wyznaczonych liczb.

Ze względu na czasochłonność konwersji rozpoczęto badania nad innymi metodami porównywania liczb w RNS.

Jedną z metod jest metoda wykorzystująca funkcję rdzenia [2]. Z kolei w artykule [3] opisana jest metoda porównywania liczb oparta o wykorzystanie tablic parzystości. O ile metoda jest szybka i prosta tablice parzystości mogą osiągać znaczne rozmiary co może prowadzić do znacznych opóźnień oraz wzrostu nakładów sprzętowych.

W artykule przedstawiono metodę określania parzystości i porównywania dwóch liczb wykorzystującą konwersję liczb z RNS do MRS.

* Politechnika Gdańska.

## 2. RESZTOWY SYSTEM LICZBOWY - RNS

Niech B = {$m_1$, $m_2$, ..., $m_n$} będzie zbiorem parami względnie pierwszych modułów, zwanym bazą, oraz niech $M = \prod_{i=1}^{n} m_i$. W systemie resztowym, określonym przez bazę B, każda liczba X z zakresu [0, M) jest jednoznacznie reprezentowana przez wektor ($x_1$, $x_2$, ..., $x_n$), gdzie $x_i = |X|_{m_i}$ dla każdego $1 < i \le n$ jest najmniejszą nieujemną resztą z dzielenia liczby X przez moduł $m_i$.

## 3. SYSTEM RESZTOWY Z MIESZANYMI PODSTAWAMI - MRS

MRS jest systemem wagowym, który został przedstawiony w [1]. Liczba X z zakresu określonego przez bazę RNS, ma reprezentację w MRS w postaci:

$$X = a_n \prod_{i=1}^{n-1} m_i + \ldots + a_3 m_1 m_2 + a_2 m_1 + a_1 = a_n P_n + \ldots + a_3 P_3 + a_2 P_2 + a_1 P_1 \quad (1)$$

gdzie: $a_1$, ..., $a_n$ - są cyframi MRS, przy czym $0 \le a_i < m_i$, $P_1$, ..., $P_n$ - są kolejnymi wagami MRS, zdefiniowanymi jako $P_1 = 1$ oraz

$$P_n = \prod_{i=1}^{n-1} m_i .$$

Reprezentacja liczby w MRS określona jest jako ($a_n$, $a_{n-1}$, ..., $a_1$) gdzie $a_n$ jest cyfrą MRS stojącą przy najbardziej znaczącej wadze. Każda liczba z zakresu określonego przez RNS ma dokładnie jedną reprezentację w MRS. System dziesiętny jest szczególnym przypadkiem MRS, w którym wszystkie $m_i = 10$.

Zaletami MRS są:

– możliwość porównywania liczb przy pomocy prostych technik (porównywanie wartości odpowiadających sobie liczb MRS),

– konwersja z RNS do MRS jest operacją szybszą i prostszą w implementacji niż CRT (brak konieczności obliczania |X|mod M ).

## 4. KONWERSJA Z RNS DO MRS

Wektor ($x_1$, $x_2$, ..., $x_n$) jest reprezentacją liczby X w RNS o bazie B = {$m_1$, $m_2$, ..., $m_n$}. Konwersję liczby X, do MRS przeprowadza się w następujący sposób zaczynając od wyznaczenia $a_1$. $a_1 = |X|_{m_i} = x_1$ jest resztą dla $m_1$.

$a_2 = \left| \frac{x_2 - a_1}{m_1} \right|_{m_1}$ (licznik mnożony przez inwersję multiplikatywną mianownika).

Ponieważ $a_1 = |X|_{m_i}$, stąd $|X - a_1|_{m_1} = 0$. Co za tym idzie, możliwe jest wyznaczenie wyniku $\left| |X - a_1|_{m_1} \cdot |m_i|_{m_i}^{-1} \right|_{m_i}$ bezpośrednio w RNS.

Obliczenia są kontynuowane dla kolejnych $a_i = \left\| \frac{X}{m_1 m_2 \ldots m_{i-1}} \right\|_{m_i}$ aż do wyznaczenia wszystkich cyfr MRS.

Poniższy przykład ilustruje opisane powyżej zależności.

Tabela 4.1. Konwersja liczby z systemu RNS do MRS

| $\mathbf{B} = \{m_1, m_2, m_3, m_4, m_5\}$ | 17 | 19 | 23 | 29 | 31 |
|---|---|---|---|---|---|
| $X = (x_1, x_2, x_3, x_4, x_5)$ | $\mathbf{a_1 = 1}$ | 11 | 13 | 23 | 12 |
| $a_1$ | 1 | 1 | 1 | 1 | 1 |
| $\lvert x_i - a_1 \rvert_{m_i}$ | 0 | 10 | 12 | 22 | 11 |
| $\lvert 17 \rvert_{m_i}^{-1}$ | | 9 | 19 | 12 | 11 |
| $\left\lvert \lvert x_i - a_1 \rvert_{m_i} \cdot \lvert 17 \rvert_{m_i}^{-1} \right\rvert_{m_i}$ | | $\mathbf{a_2 = 14}$ | 21 | 3 | 28 |
| $a_2$ | | 14 | 14 | 14 | 14 |
| $\lvert x_i - a_2 \rvert_{m_i}$ | | 0 | 7 | 18 | 14 |
| $\lvert 19 \rvert_{m_i}^{-1}$ | | | 17 | 26 | 18 |
| $\left\lvert \lvert x_i - a_2 \rvert_{m_i} \cdot \lvert 19 \rvert_{m_i}^{-1} \right\rvert_{m_i}$ | | | $\mathbf{a_3 = 4}$ | 4 | 4 |
| $a_3$ | | | 4 | 4 | 4 |
| $\lvert x_i - a_3 \rvert_{m_i}$ | | | 0 | 0 | 0 |
| $\lvert 23 \rvert_{m_i}^{-1}$ | | | | 24 | 27 |
| $\left\lvert \lvert x_i - a_3 \rvert_{m_i} \cdot \lvert 23 \rvert_{m_i}^{-1} \right\rvert_{m_i}$ | | | | $\mathbf{a_4 = 0}$ | 0 |
| $a_4$ | | | | 0 | 0 |
| $\lvert x_i - a_4 \rvert_{m_i}$ | | | | 0 | 0 |
| $\lvert 29 \rvert_{m_i}^{-1}$ | | | | | 15 |
| $\left\lvert \lvert x_i - a_4 \rvert_{m_i} \cdot \lvert 29 \rvert_{m_i}^{-1} \right\rvert_{m_i}$ | | | | | $\mathbf{a_5 = 0}$ |

Konwersja liczby z systemu MRS do dziesiętnego

| $P = \{P_5, P_4, P_3, P_2, P_1\}$ | 215441 | 7429 | 323 | 17 | 1 |
|---|---|---|---|---|---|
| $X_{MRS} = (a_5, a_4, a_3, a_2, a_1)$ | 0 | 0 | 4 | 14 | 1 |
| $a_i \cdot P_i$ | 0 | 0 | 1292 | 238 | 1 |
| $X = \sum_{i=1}^{5} a_i \cdot P_i$ | | | | | **1531** |

Do przeprowadzenia konwersji konieczne jest wykonanie n − 1 operacji dodawania i tyle samo operacji mnożenia, gdzie n to ilość cyfr MRS w reprezentacji liczby X. Zaletą zaprezentowanej metody są niski stopień skomplikowania, krótki czas obliczeń i brak konieczności wykonywania czasochłonnych operacji modulo.

### 4.1. Alternatywna metoda konwersji z MRS do systemu dziesiętnego

Znając moduły RNS, które zostały użyte do określenia wag MRS podczas MRC, konwersję liczby z MRS do systemu dziesiętnego można przeprowadzić w oparciu o wyrażenie

$$(((((((a_5) \cdot m_4) + a_4) \cdot m_3) + a_3) \cdot m_2) + a_2) \cdot m_1) + a_1 = X.$$

**Przykład**

Znana jest reprezentacja liczby X w MRS $X_{MRS} \leftrightarrow (0, 0, 4, 14, 1)$. Wiadomo, że RNS, z którego wykonano MRC posiada bazę $B = m_1, m_2, m_3, m_4, m_5\} = \{17, 19, 23, 29, 31\}$ Wyznacz wartość X w systemie dziesiętnym.

Tabela 4.2. Wyznaczanie wartości dziesiętnej liczby na podstawie jej reprezentacji w MRS

| $B = \{m_1, m_2, m_3, m_4, m_5\}$ | 17 | 19 | 23 | 29 | 31 |
|---|---|---|---|---|---|
| $X_{MRS} = (a_5, a_4, a_3, a_2, a_1)$ | 0 | 0 | 4 | 14 | 1 |
| $a_5 \cdot m4$ | 0 | | | | |
| $(a_5 \cdot m4) + a_4$ | | 0 | | | |
| $((a_5 \cdot m4) + a_4) \cdot m_3$ | | 0 | | | |
| $(((a_5 \cdot m4) + a_4) \cdot m_3) + a_3$ | | | 4 | | |
| $((((a_5 \cdot m4) + a_4) \cdot m_3) + a_3) \cdot m_2$ | | | 76 | | |
| $(((((a_5 \cdot m4) + a_4) \cdot m_3) + a_3) \cdot m_2) + a_2$ | | | | 90 | |
| $((((((a_5 \cdot m4) + a_4) \cdot m_3) + a_3) \cdot m_2) + a_2) \cdot m_1$ | | | | 1530 | |
| $(((((((a_5 \cdot m4) + a_4) \cdot m_3) + a_3) \cdot m_2) + a_2) \cdot m_1) + a_1$ | | | | | **1531** |

Ilość operacji koniecznych do wykonania jest taka sama jak w metodzie zaprezentowanej w [1]. Zaletami zaprezentowanej metody są niskie nakłady sprzętowe oraz brak konieczności przechowywania w ROM wag MRS, wystarczy znajomość modułów bazy RNS użytych podczas MRC.

Wadą jest brak możliwości wykonania wszystkich operacji mnożenia niezależnie od siebie, a następnie dodania otrzymanych iloczynów jak ma to miejsce w [1].

## 5. OKREŚLANIE PARZYSTOŚCI W SYSTEMIE LICZBOWYM Z MIESZANYMI PODSTAWAMI

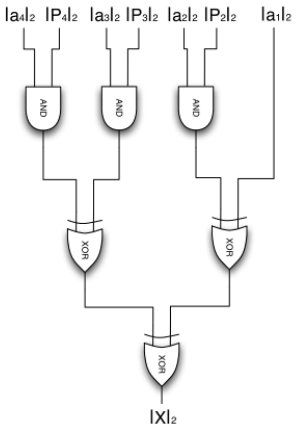
Wiedząc, że na podstawie (1) wartość liczby X w MRS określona jest jako

$$X = \sum_{i=1}^{n} a_i \cdot P_i$$

zatem jej parzystość można określić na podstawie wyrażenia

$$|X|_2 = \left| \sum_{i=1}^{n} |a_i \cdot P_i|_2 \right|_2$$

Przyjmując, że $|X|_2 = 0$ oznacza liczbę parzystą oraz $|X|_2 = 1$ nieparzystą. Wyrażenie to można zrealizować przy pomocy układu kombinacyjnego przedstawionego na rysunku 5.1.




Rys. 5.1. Układ do wyznaczania parzystości liczb zapisanych w MRS

Przedstawiona metoda pozwala na szybkie obliczenie parzystości liczby, jeżeli znana jest jej reprezentacja w MRS. Zaletą metody jest brak konieczności wykonywania operacji modulo M, jak ma to miejsce w CRT, lub w funkcji rdzenia [4].

# 6. PORÓWNYWANIE LICZB W RNS Z WYKORZYSTANIEM KONWERSJI DO MRS

Zaprezentowane w artykule metody konwersji liczb z RNS do MRS i określania ich parzystości mogą zostać wykorzystane do porównywania liczb określonych przy pomocy ich reprezentacji w RNS.

W artykule [5] przedstawiono dwie metody porównywania liczb w RNS wykorzystujące funkcję rdzenia do określania parzystości liczb na podstawie ich reprezentacji w RNS. Jedna z zaprezentowanych metod pozwala na porównywania liczb, gdy baza RNS składa się z modułów nieparzystych.

## 6.1. Metoda porównywania liczb w RNS z bazą złożoną z modułów nieparzystych

Zaprezentowany algorytm oparto o dwa twierdzenia [1] o parzystości, w przypadku, gdy moduły RNS są parami względnie pierwsze.

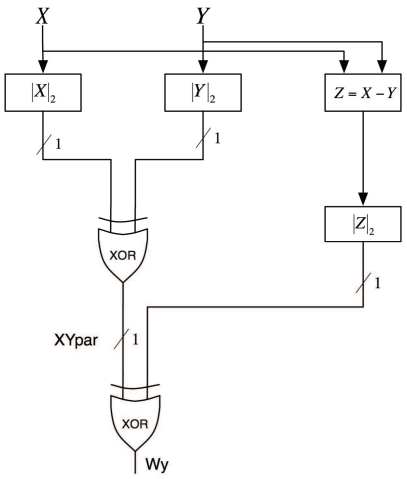
*Twierdzenie 1*: Niech $X$ i $Y$ są tej samej parzystości i $Z = X - Y$.
$X \geq Y <=> Z$ jest liczbą parzystą, $X < Y <=> Z$ jest nieparzystą liczbą.

*Twierdzenie 2*: Niech $X$ i $Y$ są różnej parzystości i $Z = X - Y$.
$X \geq Y <=> Z$ jest liczbą nieparzystą, $X < Y <=> Z$ jest parzystą liczbą.

Wynik algorytmu jest poprawny tylko, gdy liczby X i Y są tego samego znaku, stąd konieczność sprawdzenia ich znaku przed rozpoczęciem obliczeń.

1. Obliczyć Z = X −Y.
2. Wyznaczyć $|X|_2, |Y|_2, |Z|_2$.
3. Sprawdzić, czy $|X|_2 = |Y|_2$. Jeżeli obie liczby są tej samej parzystości, wynik porównania przyjmuje wartość 1, w przeciwnym wypadku wynik porównania przyjmuje wartość 0.
4. Porównać $|Z|_2$ z wynikiem porównania $|X|_2$ i $|Y|_2$ wyznaczonym w punkcie 3. Jeżeli obie wartości są sobie równe, wynik porównania ma wartość 0, co oznacza, że $X \geq Y$, w przeciwnym przypadku wynik porównania przyjmuje wartość 1, co oznacza, że X < Y .

Algorytm zaprezentowany w [5] można przedstawić w postaci schematu blokowego:




Rys. 6.1. Schemat układu porównywania liczb w RNS o bazie z modułami nieparzystymi

W [5] zaproponowano aby wartość parzystości była wyznaczana przy pomocy funkcji rdzenia, aczkolwiek dużo efektywniejszą metodą jest wykorzystanie konwersji liczb do MRS i wyznaczenie ich parzystości przy pomocy zaprezentowanej wcześniej metody.

Tego typu rozwiązanie jest znacznie bardziej proste w realizacji ze względu na brak konieczności wykonywania operacji modulo M, która występuje podczas wyznaczania wartości funkcji rdzenia oraz, co za tym idzie, znacznie mniejszy poziom skomplikowania układu realizującego algorytm porównywania liczb.

## 6.2. Metoda porównywania liczb na podstawie reprezentacji RNS

Porównanie dwóch liczb o reprezentacji w MRS można przeprowadzić porównując miedzy sobą cyfry MRS obu liczb określone dla tej samej wagi zaczynając od cyfry stojącej przy największej wadze. Operacja porównania wymaga użycia n+1 komparatorów, gdzie n jest ilością cyfr MRS w reprezentacji. Przyjmując $(x_1, x_2, ..., x_n)$ oraz $(y_1, y_2, ..., y_n)$ jako reprezentacje odpowiednio X i Y w RNS oraz P1, P2, ..., Pn jako kolejne wagi MRS. Gdzie Pn > ... > P2 > P1. Algorytm porównywania liczb w systemach resztowych z użyciem konwersji do MRS ma postać:

1. Przeprowadzić konwersję RNS → MRS dla obu liczb X i Y.
2. Sprawdzić czy $x_n > y_n$. Jeżeli tak, to X > Y . W przeciwnym przypadku przejść do kolejnego punktu 3,.
3. Sprawdzić czy $x_{n-1} > y_{n-1}$. Jeżeli tak, to X > Y . W przeciwnym przypadku przejść do kolejnego punktu.

4. Operacja 3. jest powtarzana dla kolejnych wag aż do ostatniej wagi $P_1$ o najmniejszej wartości.
5. Sprawdzić czy $x_1 > y_1$. Jeżeli tak, to $X > Y$ . W przeciwnym wypadku $X \leq Y$.

Zaletami metody są, niski poziom skomplikowania, brak konieczności wykonywania operacji modulo oraz sprawdzania parzystości liczb. Z kolei wadą jest konieczność wykonywania konwersji do MRS.

## 7. PODSUMOWANIE.

W artykule zaprezentowano metodę konwersji z RNS do MRS oraz dwie metody wyznaczania wartości liczb w systemie dziesiętnym na podstawie ich reprezentacji w MRS. Przedstawiono metodę określania parzystości liczb na podstawie ich reprezentacji w MRS oraz przedstawiono dwie metody porównywania liczb.

## LITERATURA

[1] N. S. Szabo, R. I. Tanaka. „Residue Arithmetic and its Applications to Computer Technology". NY McGraw-Hill, 1967.

[2] D. Miller, R. Altschul, J. King, J. Polky. „Analysis of the Residue Class Core Function of Akushskii, Brucev and Pak". Residue Number System Arithmetic: Modern Applications in Digital Signal Processing, IEEE Press, pp. 390-401, 1986.

[3] J. Chiang, M. Lu. „*A General Division Algorithm for Residue Number Systems*". Proceedings of the 10th IEEE Symposium Computer Arithmetic on 26-28 June 1991, s. 76 – 83.

[4] D. Miller, J. Polky, J. King. „*A Survey of Recent Soviet Developments in Residue Number Systems*". 26th Midwest Sympodium on Circuits and Systems, 1983, s. 385 – 389 , Periodicals.

[5] M. Plebanek, Z. Ulman, M. Ożarowski. „*Porównywanie liczb w resztowym systemie liczbowym z wykorzystaniem parzystości*", Metody Informatyki Stosowanej, PAN 02.2008, s. 89-98.

### PARITY DETECTION IN RESIDUE NUMBER SYSTEM, WITH USE OF MIXED RADIX SYSTEM CONVERSION

Conversion method between RNS and MRS numeric systems was presented in article. Also two methods of conversion from MRS to decimal system and algorithms of parity detection in MRS are shown. At last two methods of comparison of numbers in MRS are presented.