Journal of Theoretical and Applied Information Technology
30th April 2016. Vol.86. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ON SOME PROBLEMS AND APPROACH TO SOLUTION THEREOF UPON COMPUTING IN RESIDUE NUMBER SYSTEM

ALEXEY ALEXEEVICH LYUBOMUDROV, ALEXEY ALEKSANDROVICH BASHKOV
National Research Nuclear University «MEPhI»
Kashirskoe shosse, 31, Moscow, 115409 Russia

ABSTRACT

Major problems occurring upon designing of computing tools in residue number systems (RNS) include number conversion from positional number systems into RNS and reverse. A possible approach to solution of these problems is selection of RNS base values. This work proposes series of RNS base values in the respective forms of 2^k, $2^k - \lambda$, $2^k + \lambda$. With these base values upon number conversion mathematical operations in positional number systems are excluded, and favorable conditions are established for spreadsheet computing. This reduces time consumptions, simplifies designing of computing tools and creates positive backgrounds for further researches, hence, creation of computing tools of higher rate operating in RNS.
Keywords: *Residue Number Systems, Positional Number Systems, Number Conversion, Base Series, Selection Of Base Values, Spreadsheet Computations.*

1. INTRODUCTION

One of the approaches to increase operation rate of computing tools is application of residue number system (RNS). Hence, the aspects of designing of computing tools in RNS are considered with sufficient interest [3], [7], [1], [5], [10], [14], [16], [4].

The increase in operation rate with application of RNS is achieved due to parallelizing of arithmetic operations. Thus, if RNS applies the bases $p_1, p_2, \dots, p_s$, where p_i $(i = 1, 2, \dots, s)$ are coprime numbers, then arithmetic operations to all bases p_i are executed in parallel without transfers between the bases.

Moreover, computations in RNS facilitate additional increase in operation rate. Thus, if the numbers A and B, represented in RNS, have the form of : $A = \{\alpha_1, \alpha_2, \dots, \alpha_s\}$ and $B = \{\beta_1, \beta_2, \dots, \beta_s\}$, where $\alpha_i = rest\ A\ mod\ p_i$ and $\beta_i = rest\ B\ mod\ p_i$ $(i = 1, 2, \dots, s)$ are the remainders, that is, the residues of dividing A and B by p_i, then the arithmetic operations on the numbers A and B are executed as follows:

$$A + B = (\alpha_1 + \beta_1)\ mod\ p_1, (\alpha_2 + \beta_2)\ mod\ p_2, \dots, (\alpha_s + \beta_s)\ mod\ p_s;$$

$$A - B = (\alpha_1 - \beta_1)\ mod\ p_1, (\alpha_2 - \beta_2)\ mod\ p_2, \dots, (\alpha_s - \beta_s)\ mod\ p_s;$$

$$A \times B = (\alpha_1 \times \beta_1)\ mod\ p_1, (\alpha_2 \times \beta_2)\ mod\ p_2, \dots, (\alpha_s \times \beta_s)\ mod\ p_s.$$

The mentioned operations due to low capacity of residues α_i and β_i can be readily executed in the form of spreadsheets using data storage of IC memory chip. Thus, if $p_i = 16$, then the p_i-base residues α_i and β_i will have four binary digits upon binary coding. Herewith, in order to execute addition, subtraction and multiplication to the base $p_i = 16$ three IC memory chips are required with 256 four-digit binary words, one IC for execution of each operation. Addresses for accesses to computation results stored in IC memory chip will be the arguments in the form of eight-digit binary address $\alpha_i\beta_i$. If $p_i = 32$, then for execution of arithmetic operations of addition, subtraction and multiplication to this base three IC memory chips are required with the capacity of 1024 five-digit binary words, where ten-digit binary addresses of the results are the residues $\alpha_i\beta_i$. Due to increased operation rate the spreadsheet computations are

Journal of Theoretical and Applied Information Technology
30th April 2016. Vol.86. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

currently of sufficiently high interest [15], [11], [2], [13], [12], [6]

Spreadsheet implementation of arithmetic operations, in addition to increased operation rate, enables unification of equipment of developed computing tools, based on IC memory chips.

However, certain difficulties occur upon arrangement of computations in RNS. One of the major difficulties is relative complication of conversion of data represented in positional number systems into RNS and reverse [8], [9]. Thus, for instance, if a number A is represented in positional number system, then for conversion of this number into RNS to the bases $p_1, p_2, \dots, p_s$, that is, for representation of the number A in the form $A = \{\alpha_1, \alpha_2, \dots, \alpha_s\}$, where $\alpha_i = rest\ A\ mod\ p_i$ $(i = 1, 2, \dots, s)$, it is required to execute s operations of division in order to calculate the required residues α_i. Upon reverse conversion of numbers from RNS into positional system it is required to solve the problem of determination of the number A, provided that the residues $\alpha_i = A - [A/p_i]$ after division of the number A by p_i are known. This problem cannot be solved by one short or extensive operation.

This work is aimed at consideration of approach to selection of base values of RNS, which would enable elimination of the aforementioned difficulties.

2. SOLUTION OF THE PROBLEM AND ITS SUBSTANTIATION

According to the proposed approach one the bases of RNS is set to $p_1 = 2^k$, where $k = 1, 2, 3, \dots$, and the auxiliary bases with consideration for the required accuracy of computations are selected from two numerical series. One of the series at predetermined $\boldsymbol{k}$ is as follows: $2^k - \lambda$, where $\lambda = 1, 2, 3, \dots$ and $2^k - \lambda > 2^{k-1}$. The second series at predetermined $\boldsymbol{k}$ is as follows: $2^k + \lambda$, where $\lambda = 1, 2, 3, \dots$ and $2^k + \lambda < 2^{k+1}$. Thus, for instance, if $k = 4$, that is, $p_1 = 2^4 = 16$, then, possible base values of the first series are 15, 13, 11, 9, and possible base values of the second series are, respectively, 17, 19, 21, 23, 25, 27, 29, 31.

At such base values conversion of number from positional binary number system into RNS and reverse is simplified. Let us demonstrate this fact.

Let us assume that we have some initial number $A = a_1 a_2 \dots a_n$, represented in positional binary number system, where a_i are the binary digits of the number A (i = 1, 2, …, n).

Let us write this number in positional number system with the base $p = 2^k$ in three equivalent forms as follows:

$$A = b_1 p^{m-1} + b_2 p^{m-2} + \dots + b_{m-1} p^1 + b_m p^0, \quad (1)$$

$$A = b_1[(p - \lambda) + \lambda]^{m-1} + b_2[(p - \lambda) + \lambda]^{m-2} + \dots + \dots + b_{m-1}[(p - \lambda) + \lambda]^1 + b_m p^0, \quad (2)$$

$$A = b_1[(p + \lambda) - \lambda]^{m-1} + b_2[(p + \lambda) - \lambda]^{m-2} + \dots + \dots + b_{m-1}[(p + \lambda) - \lambda]^1 + b_m p^0, \quad (3)$$

where b_j are digits of the number A (j = 1, 2, …, m), each of them due to equality $p = 2^k$ is represented by a group of $\boldsymbol{k}$ binary digits of the number A in its initial binary notation.

It follows from Eq. (1) that $rest\ A\ (mod\ 2^k) = b_m$. This is a consequence that all constituents in Eq. (1), except for $b_m p^0$, are divided exactly by $p = 2^k$.

It follows from Eq. (2) with consideration for representation of each square brackets in the form of the Newton binomial that

$$rest\ A\ mod\ (2^k - \lambda) = rest\ (\lambda \cdot (b_1 + b_2 + b_3 + \dots + b_{m-1}) + b_m)\ mod\ (2^k - \lambda) \quad (4)$$

This is stipulated by the fact that all constituents of square brackets, except for the last one, upon their representation in the form of the Newton binomial are divided exactly by $p_2 = (2^k - \lambda)$.

It follows from Eq. (3) with consideration for representation of each square brackets in the form of the Newton binomial that

$$rest\ A\ mod\ (2^k + \lambda) = rest\ (\lambda \cdot (b_1 - b_2 + b_3 - \dots) + b_m)\ mod\ (2k + \lambda) \quad (5)$$

This is stipulated by the fact that all constituents of square brackets, except for the last one, upon their representation in the form of the Newton binomial are divided exactly by $p_3 = (2^k + \lambda)$.

Journal of Theoretical and Applied Information Technology
30th April 2016. Vol.86. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Example. It is required to convert $A = 11000101000_2 = 1576_{10}$ into RNS to bases $p_1 = 2^k = 16_{10}$, $p_2 = 2^k - 1 = 15_{10}$, $p_3 = 2^k + 1 = 17_{10}$, where $k = 4$, and $\lambda = 1$.

1. We break up binary digits of the number A in its initial form $A = 11000101000_2$ into the groups containing by $k = 4$ binary digits. We obtain the following groups: 0110_2, 0010_2, 1000_2.

2. Summation and alternative summation these groups with respect to the bases $p_2 = 2^k - 1 = 15$ and $p_3 = 2^k + 1 = 17$, respectively, we obtain the required residues to bases $p_2 = 2^k - 1 = 15$ and $p_3 = 2^k + 1 = 17$:

$$rest\ A\ (mod\ 15) = rest\ (0110_2 + 0010_2 + 1000_2)\ mod\ 15 = 0001_2;$$

$$rest\ A\ (mod\ 17) = rest\ (0110_2 - 0010_2 + 1000_2)\ mod\ 17 = 1100_2.$$

3. The required residue to the base $p_1 = 2^k = 16$ should not be calculated. This residue is represented by $\boldsymbol{k}$ binary digits of least significant bits of the number A, that is, $rest\ A\ (mod\ 16) = 1000_2$.

Thus, $A_{16,15,17} = \{1000_2, 0001_2, 1100_2\}$.

Reverse conversion of numbers $A = \{\alpha_1, \alpha_2, \dots, \alpha_s\}$ from RNS into positional binary number system using the considered base values assumes execution of the following sequence of operations.

1. Reduction of the number $A = \{\alpha_1, \alpha_2, \dots, \alpha_s\}$ by $\alpha_1 = rest\ A(mod\ 2^k)$

$$A - \alpha_1 = \{0, (\alpha_2 - \alpha_1)\ mod\ p_2, (\alpha_3 - \alpha_1)\ mod\ p_3, \dots, (\alpha_s - \alpha_1)\ mod\ p_s\}$$
.

2. Using the values $(\alpha_2 - \alpha_1)\ mod\ p_2$, $(\alpha_3 - \alpha_1)\ mod\ p_3$, …, $(\alpha_s - \alpha_1)\ mod\ p_s$, for determination of reduced number $A - \alpha_1$ in positional number system with the base $p = 2$, where $\boldsymbol{k}$ least significant bits are zero.

3. Recovery of the number A by writing of the residue $\alpha_1 = rest\ A\ (mod\ 2^k)$ into its $\boldsymbol{k}$ least significant bits.

As mentioned above, all operations upon number conversion from RNS into binary positional system due to low digit capacity of residues $\alpha_i\ (i = 1, 2, \dots, s)$ can be readily executed using IC memory chips for storage of data spreadsheets.

Example. Let us assume that the number A, represented in RNS to bases $p_1 = 2^k = 16$, $p_2 = 2^k - 1 = 15$ and $p_3 = 2^k + 1 = 17$, is written as follows: $A = \{1000_2, 0001_2, 1100_2\}$. It is required to convert this number into positional number system with the base $p = 2$.

1. We reduce the number A, represented in RNS, by $\alpha_1 = 1000_2$. We obtain $A - 1000_2 = \{0000, 1000, 0100\}$.

2. We access memory chip with the capacity of $p_2 \times p_3 = 15 \times 17 = 255$ words containing conversion results for the numbers in the form of $\{0, \alpha_2 - \alpha_1, \alpha_3 - \alpha_1\}$ from RNS into positional binary system, at the address $(\alpha_2 - \alpha_1, \alpha_3 - \alpha_1) = (1000, 0100)$ and obtain $A - 1000_2 = 11000100000_2$.

3. We store the residue $\alpha_1 = 1000_2$ in $\boldsymbol{k} = 4$ least significant bits, thus obtaining finally $A_2 = 11000101000_2$.

3. RESULTS

Therefore, it follows from Eq. (1) that the residue to the base $p_1 = 2^k$ coincides with the digit b_m, which is represented by $\boldsymbol{k}$ least significant binary digits of the number A.

In order to determine the residues of number A to bases $p_2 = 2^k - \lambda$, as follows from Eq. (4), it is sufficient to sum the digits b_j of the number A to base p_2 upon multiplication of digits, except for the last one, by λ. All digits b_j, as mentioned above, are represented by groups of k binary digits, which is convenient for spreadsheet implementation of operations upon this conversion.

In order to determine the residues of number A to bases $p_3 = 2^k + \lambda$, as follows from Eq. (5), it is sufficient to alternatively sum the digits b_j of the number A to base p_3 upon their multiplication, except for the last one, by λ. Here all digits b_j are also represented by groups of k binary digits. It is convenient to execute all operations upon this conversion in spreadsheet form.

Conversion of number A from RNS into binary positional number system is reduced to execution of single subtraction in RNS and one access to memory, when higher bits of number A are

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

extracted from IC memory chip at the address $(\alpha_2 - \alpha_1,\ \alpha_3 - \alpha_1, \dots, \alpha_s - \alpha_1)$.

4. DISCUSSION

While applying the proposed base values, as follows from the considered information, the number conversion from positional binary system into RNS is significantly simplified. During such conversion arithmetic operations in positional number systems are not required. The conversion is reduced to summation and alternative summation of several groups of k binary digits. Due to low digit capacity of the mentioned groups summation and alternative summation can be readily executed in spreadsheet form using IC memory chips.

Reverse conversion, that is, number conversion from RNS into positional binary system, is also simplified. Upon such conversion searching for matching variants of numbers, represented in RNS and binary positional number system, respectively, is eliminated. The conversion is reduced to single operation of subtraction in RNS and to one access to memory. With such approach neither complete searching for possible variants of conversion, nor arithmetic operations in positional number system are required. The spreadsheet capacity in comparison with that for storage of all possible conversion results is reduced by 2^k times.

It its turn, the simplification of conversions from binary positional number system into RNS and reverse creates positive backgrounds for designing of efficient methods and tools for certain non-modular operations, the execution of which is difficult in RNS. These non-modular operations include number comparison, determination of sign, division and overflow control of dynamic range.

5. CONCLUSION

Therefore, selection of base values of RNS, one of which is set to $p_1 = 2^k$, and auxiliary bases are selected from the series $p_2 = 2^k - \lambda$ and $p_3 = 2^k + \lambda$, makes it possible to generate approach to establishment of efficient methods of data conversion from positional binary number system into RNS and reverse, thus facilitating spreadsheet implementation. Data conversions from positional binary number system into RNS and reverse using the mentioned methods are reduced to several accesses to spreadsheets in IC memory chip without arithmetic operations in positional number systems. In its turn, this creates positive backgrounds for designing of efficient methods and tools to execute such non-modular operations as comparison, determination of sign, division and overflow control of dynamic range and, hence, creation of computing tools of increased operation rate available in RNS.

REFERENCES:

[1] Anikueva O. V., Lyalhov P. A., and Chervyakov N. I. Implementation of discrete wavelet transformation in RNS of special type // Infokommunikatsionnye Tekhnologii. – 2014. – 12, No. 4. – pp.4 – 9.

[2] Boyarchuk A. A., Stepanov Yu. A., and Fanaskov V. S. Implementation of variable tables for DSL applied in specialized GIS // Information systems and technologies: Proceedings of International R&D conference, Krasnoyarsk, May 30, 2012. – Krasnoyarsk. – 2012. – pp. 103 – 107.

[3] Chervyakov N. I. and Averbukh V. M. Approximated method of non-modular procedures in RNS // Basic researches. – 2012. - No. 6. – pp. 189 – 193.

[4] Chervyakov N. I., Babenko M. G. and Lyakhov P.A., et al. Device for comparison of number represented in RNS. – 2014. – RF Patent, No. 2503992.

[5] Isupov K. S. On an algorithm of number comparison in RNS // Vestn. Astrakh. State Technical University. Series: Management and IT. – 2014. - No. 3. – pp. 40 – 49.

[6] Khokhlov I. I. Monitoring and forecasting of emergency situations. An example of implementation by means of spreadsheets // Urgent problems and innovations in provision of safety: Science Week, Ekaterinburg, December 2 – 6, 2013. - Ekaterinburg. - 2014. - pp. 160 – 168.

[7] Knyaz`kov V. S. and Osinin I. P. Method of multiplication arrangement of floating point numbers presented in RNS. – 2013. - RF Patent, No. 2485574.

[8] Lyubomudrov A. A. and Zaitsev A. V. Method of number conversion from positional number system into residual number system // Vestn. MEPhI. – 2014. – 3, No. 2. – pp. 252 – 253.

[9] Lyubomudrov A. A. Device for conversion of binary code into RNS code. – 2011. - RF Patent, No. 2413279.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[10] Magomedov Sh. G. Transformation of number presentation in modular arithmetic in RNS with different bases // Vestn. Astrakh. State Technical University. Series: Management and IT. – 2014. - No. 4. – pp. 32 - 39.

[11] Mal'chukov A. N. and Osorin A. N. Rapid computing of CRC: spreadsheet versus matrix // Applied informatics. – 2010. - No. 2. – pp. 58 - 63.

[12] Mytsko E. A. and Mal'chukov A. N. Study into hardware implementation of spreadsheet and matrix algorithm of CRC 32 computing // Izv. Tomsk Polytechnic University. – 2013. – 322, No. 5. – pp. 182 – 186.

[13] Pchel`nik V. K. and Revchuk I. N. Implementation of Gauss method in MS Excel spreadsheets // Proceedings of International R&D conference: Informational support of engineering equipment, Moscow, April 10-11, 2012. – Moscow. - 2012. – pp. 228 – 229.

[14] Polisskii Yu. D. Algorithm of complex procedures in RNS using number radix complement representation // Electronic simulation. – 2014. – 36, No. 4. – pp. 117 – 123.

[15] Romm Ya. E. and Aksaiskaya L. N. Spreadsheet algorithmic computing of functions, derivatives and integrals on the basis of interpolation Newton polynomial // Vestn. Taganrog State Pedagogical Institute. Series: Physical--mathematical and natural sciences. – 2009. - No. 1. – pp. 110 – 115.

[16] Samoilenko D. V., Evdokimov A. A., and Koldaev A.I., et al. Identification of ACS subjects in RNS // Informational and communication technologies in science, industry and education (Infokom - 6): Proceedings of 6th International R&D conference, Stavropol, April 21 – 27, 2014. Part 2. – Stavropol. – 2014. – pp. 395 – 398.