www.revistageintec.net
ISSN: 2237-0722
revista GEINTEC
Gestão, Inovação e Tecnologias

An Approach to Dividing Modules of Numbers by the Values of Bases in Number Systems in Residual Classes

Alexey Alexeevich Lyubomudrov[1]; Elman Said-Mokhmadovich Akhyadov[2]; Elena Victorovna Afanaseva[3]

[1]National Research Nuclear University «MEPhI», Moscow, Russia.

[2]Chechen state university, Grozny, Russia.

[3]Moscow Polytechnic University, Moscow, Russia.

Abstract

The paper considers an approach to division modules of numbers by bases in number systems in residual classes (RNS). This may be required when solving specific tasks.
The approach involves performing the following sequence of actions in the RNS:
- reducing the modulus of numbers by the value of the deduction corresponding to the base by which the division is made;
- dividing the reduced module by the value of the base;
- formation the correction value and its addition to the quotient obtained.
In total the division operation is performed through four accesses to the table memory two of which are overlapped in time.
If one of the bases of the RNS is equal to pn then the approach under consideration allows to reduce the capacity of table memory by pn times in relation to the capacity of table memory containing the full set of division results, where pn is the base of the RNS by which the division is performed.

Key-words: Number Systems in Residual Classes, Arithmetic Operations, Modules of Numbers, Division of Modules, Base Values, Tabular Calculations.

1. Introduction

Significant attention is currently being paid to the development and study of the principles of information processing in number systems in residual classes (hereinafter - RNS). [Boyarchuk et al., 2012; Liu et al., 2013; Khokhlov, 2014; Polisskii, 2014; Lyubomudrov and Zaitsev, 2014; Lyubomudrov and Bashkov, 2016; Yurdanov et al., 2016; Wojcik et al., 2018; Haojuan et al., 2019; Krasnobayev et al., 2019; Krasnobayev et al., 2021]. The development of computing tools in this area is underway [Lyubomudrov, 2011; Chervyakov et al., 2015; Knyaz`kov and Isupov, 2015; Chervyakov et al, 2017; Magomedov , 2017; Haojuan et al., 2019]. This is due to the possibility of parallelizing information processing at the level of arithmetic operations, as well as the convenience of using tabular computation methods, which together increases the speed and simplifies the design of the computers.

So if p_1, p_2,. ... ... , p_n are the bases of the RNS and the numbers A and B have the form A = $(\alpha_1, \alpha_2,\ldots, \alpha_n)$ and B = $(\beta_1, \beta_2,\ldots, \beta_n)$ in RNS, where α_i = rest A mod p_i and β_i = rest B mod p_i (i = 1, 2,..., n) are remainders, that is, the residues of dividing A and B by p_i, then arithmetic operations on the numbers A and B are carried out in accordance with formulas (1) - (3):

$$A + B = (\alpha_1 + \beta_1) \bmod p_1, (\alpha_2 + \beta_2) \bmod p_2 , \ldots , (\alpha_n + \beta_n) \bmod p_n \quad (1)$$

$$A – B = (\alpha_1 - \beta_1) \bmod p_1, (\alpha_2 - \beta_2) \bmod p_2 , \ldots , (\alpha_n - \beta_n) \bmod p_n \quad (2)$$

$$A \times B = (\alpha_1 \times \beta_1) \bmod p_1, (\alpha_2 \times \beta_2) \bmod p_2 , \ldots , (\alpha n \times \beta n) \bmod p_n \quad (3)$$

Some of the basic operations in computers which operate in a positional binary system are the operations of multiplication and division by the base of the number system p = 2. These operations are used for normalizing and denormalizing mantissas, for performing multiplication and division, and for scaling results of calculations. The implementation of these operations in computers using a positional binary number system does not cause difficulties. These operations are performed by shifting of the operands left or right one bit.

Performing of the operation of the multiplying of the number A = $(\alpha_1, \alpha_2,\ldots, \alpha_n)$ by the base pi in the RNS does not cause difficulties too. This operation in the RNS is performed in accordance with formula (3) and its execution has the following form

$$A \times p_i = (\alpha_1 \times p_i) \bmod p_1, (\alpha_2 \times p_i) \bmod p_2 , \ldots , (\alpha_n \times p_i) \bmod p_n$$

However, the performing of the operation of the dividing numbers in RNS by pi by using formula (3) is difficult.

The division operation, like operations (1) - (3), is the basic operation when performing calculations. Because of this, methods and hardware for performing the division operation are being developed, which allow maintaining high performance of computing tools in the RNS.

The best performance when performing a division operation is achieved when it is performed tabularly. When performing a tabular operation, the results are stored in the computer's memory and selected from memory by operands, as by addresses. However, this approach requires significant memory overhead. So, if on the bases p_1, p_2,..., p_n the divisible and the divisor are represented by deductions, then for the tabular execution of the division operation the computer memory must contain $N = p_1 \times p_2 \times . .. \times p_n$ words with bit depth $R = r_1 + r_2 + ... + r_n$, where r_i is the bit depth of the residues on the bases p_i , i = 1, 2,..., n.

So this article is aimed at the consideration of a variant of the approach to dividing of the modules of numbers which are presented in the RNS by the bases p_i, where i = 1, 2,…, n.

When considering the approach without violating generality, we assume that the division of numerical modules in RNS is performed by dividing them by the base p_n.

2. PROBLEM RESOLUTION

Let A is some positive or negative integer number the module of which |A| in RNS with bases $p_1, p_2, \dots, p_n$ has the following representation

$$|A| = (\alpha_1, \alpha_2, \dots, \alpha_n),$$

where α_i = rest |A| mod p_i; i = 1, 2, … , n.

Then the proposed approach to dividing |A| by pn assumes the following sequence of actions:

1. The module of number $|A| = (\alpha_1, \alpha_2, \dots, \alpha_n)$ is decreased by the value α_n = rest|A| mod p_n.

This decreasing is performed by carry out the following operation in the RNC

$$|A| - \alpha_n =$$

$$= \{(\alpha_1 - \alpha_n) \bmod p_1, (\alpha_2 - \alpha_n) \bmod p_2, . . . , (\alpha_n -1 - \alpha_n) \bmod p_n - 1, (\alpha_n - \alpha_n) \bmod p_n\}=$$

$$= \{(\alpha_1 - \alpha_n) \bmod p_1, (\alpha_2 - \alpha_n) \bmod p_2, . . . , (\alpha_n -1 - \alpha_n) \bmod p_n - 1, \ 0 \} \qquad (4)$$

From (4) it follows that the reduced module of number |A| - αn is divisible by p_n without remainder. The remainder αn of dividing the reduced number $|A| - \alpha_n$ by pn according to (4) is equal to zero α_n = rest($|A|- \alpha_n$) mod p_n = 0.

2. By the formed remainders in RNS$\{(\alpha_1 - \alpha_n) \bmod p_1, (\alpha_2 - \alpha_n) \bmod p_2, . . . , (\alpha_n -1 - \alpha_n) \bmod p_n - 1\}$, as a binary address, the computer's table memory is accessed and the accurate result of dividing $|A| - \alpha_n$ by p_n is selected from this memory

$$(|A| - \alpha_n) : p_n = (\alpha_1', \alpha_2', . . . , \alpha_n - 1', \alpha_n') \qquad (5)$$

3. Simultaneously with the execution of item 2, the correction value Θ is formed Θ = (0, 0,…, 0, 0), if $\alpha_n : p_n < 0.5$, or Θ = (1, 1,…, 1, 1), if $\alpha_n : p_n \geq 0.5$. Such a correction takes place due to the fact that $\alpha_n : p_n < 1$ and, accordingly, the value Θ by which it is necessary to increase the quotient is enclosed in the range $0 \leq \Theta < 1$. The correction value is selected from the table memory when it is accessed via α_n as a binary address.

4. The formation of the final result of dividing |A| by p_n is performed. It is done by adding to (5) the correction value Θ in RNS

$$|A| : p_n = (|A| - \alpha_n) : p_n + \Theta = (\gamma_1, \gamma_2, \ldots, \gamma_{n-1}, \gamma_n) \qquad (6)$$

When the correction is introduced the value of the absolute error Δ of the quotient does not exceed $\Delta \leq 0.5$.

The implementation of the dividing in RNS of an arbitrary number module |A| by p_n is illustrated by the following example.

Example.

Let the absolute value of the number A is equal to |A| = 41510 = 1100111112 and in the RNS with bases p_1 = 13, p_2 = 15, p_3 =16 has the following form |A| = (12, 10, 15) 13, 15, 16.

It is required to divide in RNS |A| = (12, 10, 15) 13, 15, 16 by p_3 = 16.

1. |A| = (12, 10, 15) 13, 15, 16 is decreased by α_3 = rest 415 mod 16

|A| - α_3 = (12, 10, 15) 13, 15, 16 - (15, 15, 15) 13, 15, 16 = (10, 10, 0) 13, 15, 16 =

= (10102, 10102, 00002).

2. With the binary address 1010 10102 the computer memory is accessed and the accurate result of dividing of the reduced module |A| - α_3 = 40010 by 16 is selected from the memory

(|A| - α_3): 16 = (12, 10, 9)13, 15, 16

3. To the result of dividing of the reduced module |A| - α_3 = 40010 by 16 a correction Θ = (1, 1, 1) is added since α_3: p_3 = 15: 16 > 0.5 and the final result is formed:

(|A| - α_3): 16 + Θ = (12, 10, 9)13, 15, 16 + (1, 1, 1) 13, 15, 16 = (0, 11, 10) 13, 15, 16

Summing up we note that a feature of the proposed approach is its orientation on tabular methods of calculations. This is due to the relatively low bit depth of the RNS bases. In this case the calculations of the results of dividing of the number modules presented in the RNS is performed by four accesses to the computer′s table memory two of which are overlapped in time.

3. RESULTS

The result of this work is the proposed approach to division of the modules of numbers by the values $p_1, p_2, \ldots, p_n$ which are RNS bases.

4. DISCUSSION

The proposed approach allows to divide modules of numbers represented in the RNS by the value of one of the bases by four accesses to the computer's table memory two of which are overlapped in time. That the division operation is performed by four accesses to the computer's table memory, two of which run simultaneously, causes a high speed of the operation.

In addition this approach reduces required memory capacity for storing the results of calculations. So if the bases of the RNS are $p_1, p_2, \ldots, p_n$ then for storing the full table of answers memory capacity equal to $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n$ words is required. With the proposed approach require memory capacity is reduced by p_n times and is equal to $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n\text{-}1$ words.

The increased performance and reduced require memory capacity create favorable conditions for the application of the approach under consideration when organizing computational processes and developing computational tools in RNS.

5. CONCLUSION

In the paper an approach for dividing modules of numbers presented in the RNS by the base values of the RNS is proposed. This may be required when solving specific tasks.

The approach involves the following sequence of actions in RNS:

- reducing the modulus of the number by the value of the deduction corresponding to the base by which the division is made;
- dividing the reduced module by the value of the base;
- formation of the correction value and its addition to the obtained quotient.

Due to the low bit depth of the bases all the above operations are convenient to perform tabular.

In total the division operation is performed through four accesses to table memory two of which are overlapped in time. This provides a high speed of the operation.

The proposed approach allows to reduce require memory capacity by p_n times in relation to the memory capacity containing the full set of division results, where p_n is the base of the RNS by which the division is performed.

References

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. P. 103 – 107.

Chervyakov N. I., Babenko M. G., Lyakhov P. A., Lavrinenko I. N. and Lavrinenko A.V. *Device for basic division of modular numbers in the format of a system of residual classes*. 2015. RF Patent, No 2559772.

Chervyakov N. I., Babenko M. G., Kuchukov V. A., Deryabin M. A., Lavrinenko I. N. and Lavrinenko A.V. *Device for dividing modular numbers*. 2017. RF Patent, No 2628179.

Haojuan M., Zhen G., Zhaohui G., Ming Z. and Jinsheng Y. *Storage mechanism optimization in blockchain system based on residual number system//* IEEE Access. 2019. Vol. 7. P. 114539 – 46.

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. P. 160 – 168.

Knyaz`kov V.S. and Isupov K.S. *Device for comparing numbers in RNS based on interval-positional characteristics*. 2015. RF Patent, No. 2557444.

Krasnobayev V., Kuznetsov A., Zub M. and Kuznetsova K. Methods for comparing numbers in non-positional notation of residual classes// *CEUR Workshop Proceedings*. 2019. No 2353. P. 581 – 595.

Krasnobayev V., Kuznetsov A., Kuznetsova T.,Yanko A. and Akhmetov B. *Processing of the residuals of numbers in real and complex numerical domains* // Lecture Notes on Data Engineering and Communications Technologies. 2021. No 48. P. 529 – 555.

Liu Y., Chang C. and Chang S. A residual number system oriented group key distribution mechanism// *International Journal of Information Processing and Management*. 2013. Vol. 4. No 3. P.146 – 155.

Lyubomudrov A. A. *Device for conversion of binary code into RNS code*. 2011. RF Patent, No. 2413279.

Lyubomudrov A. A. and Zaitsev A. V. *Method of number conversion from positional number system into residual number system* // Vestn. MEPhI. 2014. Vol. 3. No. 2. P. 252 – 253.

Lyubomudrov A. A. and Bashkov A.A. On Some Problems and Approach to Solution Thereof upon Computing in Residue Number System// *Journal of Theoretical and Applied Informational Technology*. 2016. Vol.86. P. 377 - 381.

Magomedov Sh. G. *Construction closed system of data exchange networks based on the use of residual classes of number systems*// Industrial Automatic Control Systems and Controllers. 2017. No 1. P. 42-46.

Polisskii Yu. D. *Algorithm of complex procedures in RNS using number radix complement representation* // Electronic simulation. 2014. Vol. 36. No. 4. P. 117 – 123.

Wojcik W., Kalimoldaev M., Biyashev R., Kapalova N., Akhmetova A., Nugmanova S.and Mergenbayev Y. *Creating an algorithm of encryption based on prime numbers in positional systems of calculating residual classes*// Przeglad Elektrotechniczny. 2018. Vol. 94. No 2. P. 164 – 169.

Yurdanov D.V., Gordenko D.V., Gordenko N.V., Petlina E.M. and Pavlyuk D.N. *To the question of applying the system of residual classes in modern digital signal processing devices* // Fundamental Researches. 2016. No 2-2. P. 318 – 322