An algorithm of calculation of degrees of numbers is in the delimited system of remaining classes (DSRC)

Orest Volinskiy

Abstract - **Information technology of realization of method of algorithm of getting up to the degree of numbers of large bit is expounded on the module on the basis of the delimited system of remaining classes.**

Keywords - **delimited system of remaining classes, multibasisd processors, interbase transformer.**

I. INTRODUCTION

The tasks of digital treatment of signals in the complex system can decide on the basis of universal and specialized processors. For application of universal processors the binary scale of notation is used, that in theory numerical base of Rademakhera. At the bit of numbers which go beyond the bit net of processors, n>32, 64, 128… $2n\cdot\tau$, where τ – time of switching of valve of the microelectronic system of processor. At implementation of increase an algorithm will have the appearance of quadratic function $2n^2\cdot\tau$. Thus, at working of signals or numbers presented by a large bit, this task will decide in cryptography where application of processors of base of Rademakhera is uneffective.

Principles of working of information are in-process [1] rotined on basis DSRC theory of numerical base of Krestensona, where marketabilities linear complication of algorithms of implementation of operations of addition and increase are rotined. Obviously, that application of this base will be especially effective at the decision of tasks getting up of numbers to the high degrees and implementation of module operations of XOR, what is realized in the processors of Rademakhera, by implementation of operations of division, which has algorithmic complication $4n^2\cdot\tau$.

II. THEORETICAL BASES DSRC

At the binary differentiating of binary numbers of base of Rademakhera, that k=0, a differentiating structure has next kind [2]:

As a result of such differentiating of binary code (X_{n-1}, X_{n-2}, …,X_i ,… ,X_1 ,X_0) the matrix of tailings is formed to the digitp i in the system of the simple between itself modulesy P_1, P_2, ... P_j, ... P_k .

For passing to the base of Krestensona above the elements of ribbons of matrix a next operation is executed : $res(b_{n-1,j}+b_{n-2,j}+...+b_{i,j}+...+b_{1,j}+b_{0,j}) \bmod P_i$.

For a rev-up module operation it is expedient to apply the pyramidal algorithm of addition. The fast-acting of such pyramidal module summator settles accounts after a formula: $m=\log_2 n^i$,n – bit of processor of base of Rademakhera.

Orest Volinskiy - Carpathians State center of informative tools and technologies of NASU. Ivano-Frankivsk, Pashnyckogo Str 43, E-mail: Orestsks@ukr.net

High fast-acting of such components of interbase transformation of Rademakhera – Krestensona needs plenty of summators depending on the bit of processor the number of which settles accounts after a formula:

$$S = n + n/2 + n/4 + ... + n/n .$$

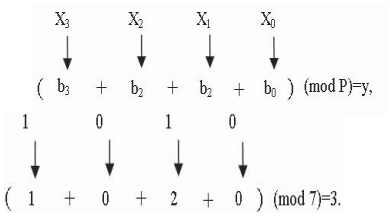
Thus the general volume of this interbase transformation can be estimated in obedience to expression $Q = K \cdot S$,where K – number of the simple between itself modules of base of Krestensona.

Volume of microelectronic equipment, interbase transformer, it is possible substantially to decrease due to information technology and structure of linear interbase transformation.

III. AN ALGORITHM OF GETTING UP TO THE DEGREE NUMBERS OF LARGE BIT IS ON THE MODULE ON THE BASIS OF BINARY DELIMITED SRC

The operation of getting up to the degree is described equalization $a^x \pmod p = y$, where a – base number, x – degree of number, p – module, y – the least inalienable remain.

Will consider the example of implementation in delimited SRC. Let a=10, x=1, 2,…, p=7. Will present a number $a_{(10)} = 1010_{(2)}$ in the delimited system:



In a next step for getting up of numbers a to the next degrees on the module p multiplying of codes of tailings is executed y in the delimited system. At what the delimited tailings are multiplied in the proper bats.

$3^2_{(10)} = 1001_{(2)}$ $\quad$ $2^4_{(10)} = 0010_{(2)}$

$(1+0+0+1) \pmod 7 = 2.$ $\quad$ $(0+0+2+0) \pmod 7 = 2.$

IV. CONCLUSION

As a result, from an example evidently, that tailings are got 3, 2, 3, on the module 7 it is considerably simpler to bring to the degree. Thus application of the binary delimited system will allow to reduce algorithmic complication of numbers on the module *p*.

REFERENCES

[1]. O.I. Volinskiy "Methods of comparison and addition in the delimited system a calculation. Advancement is in science." Collection of labours of Buchackogo of institute of management and audit. – Buchach. – 2009. - №4. T1. – S. – 91-94.

[2]. O.I. Volinskiy "Methods of interbase transformations are on the basis of the delimited scale of notation of remaining classes." – Collection of Lviv Polytechnic National University– Lviv – 2009.№4. T1. – Pp. 314-317.