DOI 10.15276/imms.v14.no4.305
УДК 004.056.55

Informatics and Mathematical Methods in Simulation
Vol.14 (2024), No. 4, pp. 305-313

A METHOD FOR POLYNOMIAL RECOVERY FROM ITS RESIDUES BASED ON ADDITION IN Z[x] RING

I. Yakymenko, M. Kasianchuk, I. Shylinska

West Ukrainian National University
11, Lvivska str., Ternopil, 46009, Ukraine
Emails: iyakymenko@ukr.net, kasyanchuk@ukr.net

The methods for polynomial recovery from its residues in Z[x] ring are presented in this paper. This problem is relevant due to important applications in asymmetric and symmetric cryptography, algorithms of noise resistant coding, in the process of transmitting data packets for error control and recovery in computer networks and distributed data storage. The theoretical foundations of polynomial recovery in a ring of polynomials based on known approaches, namely, on the Chinese Remainder Theorem and Garner's algorithm, are considered, and their advantages and disadvantages are highlighted. New methods of inverse transform from the Residue Number System based on addition of the product of moduli and the product of polynomial residues are developed. Analytical expressions of the time complexity of the proposed method and Garner's algorithm are created. The graphs of their dependences are presented, which show that the developed method for polynomial recovery from its residues in Z[x] ring is characterized by lower complexity. It was found that the time complexities of both methods increase with an increase in the dimensions of the input parameters. The efficiency of the use of the developed method in the ring Z[x] is studied, which shows a logarithmic growth with an increase in the degrees of the polynomial, and a proportional decrease when a number of moduli increases.

Key words: polynomial recovery, ring of polynomials, residues, Chinese Remainder Theorem, Garner's algorithm, time complexity, efficiency.

Introduction. Polynomial recovery from its residues in a ring of polynomials is an important problem of modern algebra and number theory [1,2]. In practice, similar to the case of integers [3-5], the application of this theory, namely the Residue Number System (RNS) in a polynomial ring (PR), allows working not with higher degree polynomials, but with sets of residues whose degree is less than or equal to the selected moduli (irreducible polynomials) [6, 7]. One of the main advantages of using RNS PR is that calculations can be performed in parallel for each module [8]. These properties make it possible to reduce the complexity of calculations and, accordingly, to increase the efficiency of computer systems due to the parallel process of performing arithmetic operations [9], to control and correct errors in noise resistant coding [10, 11], and etc. Polynomial Residue Number Systems (PRNS) are widely used in modern cryptography, in particular, in RSA [12, 13], Rabin [14], AES ciphers [15], and etc. In the RSA cryptosystem, residues on division by a high-order polynomial, which is the product of two irreducible polynomials, are calculated [13]. Accordingly, to increase performance, calculations can be carried out modulo irreducible polynomials of a significantly lower order. Therefore, the development of methods and algorithms that make it possible to reduce the time complexity when recovering a polynomial from its residues in a polynomial ring is currently a relevant problem.

Related Works. The main ideas of the PRNS were outlined in [9, 16]. The most important contribution of these works is the fundamental theorem on the modular number system. Due to the theorem, the coefficients of the polynomials used to represent the set Zp, are restricted. In [17], the requirements for the size of the parameters used to represent an integer modulo p were defined. Work [18] is devoted to the development of multiplication algorithms in PRNS. In [19], a modified Chinese Remainder Theorem (CRT) for cyclotomic polynomials was presented, which made it possible to simplify the polynomial recovery from its residues. After that, PRNS found its application in problems of noise resistant coding. In particular, in [20], the principles of generating redundant codes in the polynomial number system were considered, and the algorithm was developed, which made it possible to detect and correct errors without the inverse transform of the PRNS code into a positional one and without performing a division operation. It should be noted that the Chebyshev polynomials take an important role in data protection. For example, in [21], a scheme in the client-server environment was proposed on the basis of the Chebyshev polynomials. Although this scheme demonstrates a lower speed compared to the existing ones, it can resist some popular attacks. Recently, the Chebyshev polynomials have been actively used in asymmetric cryptography. Thus, in [22], two asymmetric cryptosystems were developed on the basis of the Chebyshev polynomials, the main feature of which is the generation of a semigroup with respect to the composition operation. An image encryption algorithm based on the Chebyshev polynomials was proposed in [23]. In [24], modified fast algorithms of asymmetric cryptography, i.e., matrix algorithm and algorithm based on the characteristic polynomial were developed and an efficient scheme for calculating the Chebyshev polynomials over a finite field was presented.

Methods for polynomial recovery. The theoretical basis for polynomial recovery from its residues in the corresponding ring, as for integer arithmetic [25], is algebra and number theory, in particular the CRT in a polynomial form. Any polynomial $N(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$ can be represented in the form of residues $b_i(x)=c_lx^l+c_{l-1}x^{l-1}+\ldots c_1x+c_0$ of division by irreducible polynomials $p_i(x)=s_zx^z+s_{z-1}x^{z-1}+\ldots+s_1x+s_0$, which are called polynomial moduli

$$b_i(x)=N(x)\bmod p_i(x)\,, \tag{1}$$

where $\deg b_i=\deg N-\deg p_i$.

At the same time, a necessary and sufficient condition is the inequality $N(x)<P(x)=\prod_{i=1}^{k}p_i(x)$, where k is the number of irreducible polynomials. Then, the original polynomial can be unambiguously recovered on the basis of the CRT:

$$N(x)=\left(\sum_{i=1}^{k}m_i(x)P_i(x)b_i(x)\right)\bmod P(x)\,, \tag{2}$$

where $P_i(x)=\dfrac{P(x)}{p_i(x)}$, $m_i(x)=P_i^{-1}(x)\bmod p_i(x)$.

Another method of a polynomial recovery from its residues in the corresponding ring is Garner’s algorithm, which is based on the relation:

$$N(x)=n_0(x)+n_1(x)p_1(x)+n_2(x)p_1(x)p_2(x)+\ldots+n_{n-1}(x)p_1(x)p_2(x)\ldots p_{i-1}(x)\,, \tag{3}$$

where $0\le n_i(x)<p_{i+1}(x)$, i=0, 1, …, k-1,

$$n_i(x)=\frac{b_{i+1}(x)-\left(n_0(x)+n_1(x)p_1(x)+\ldots+n_{i-1}(x)p_1(x)p_2(x)\ldots p_{i-1}(x)\right)}{p_1(x)p_2(x)\ldots p_i(x)}\bmod p_{i+1}(x)\,. \tag{4}$$

In this case, the polynomials $n_i(x)$ are calculated sequentially one after another based on the recurrence formula (4). In addition, both Garner's algorithm and CRT can be used for similar operations in integer arithmetic.

The main disadvantage of the above methods of a polynomial recovery from its residues is strictly sequential structure of polynomials, which makes it impossible to parallelize calculations, perform operations on polynomials of higher orders (in particular, calculate the residue modulo $P(x)$), and it is necessary to find modular multiplicative inverse in the ring of polynomials, which is a cumbersome task even for integer arithmetic [26]. To find it, the following methods are most commonly used [27]: sorting through all possible options, using the extended Euclidean algorithm, based on the Euler function. These approaches are characterized by significant computational complexity.

Therefore, the purpose of this work is to develop the methods for polynomial recovery from its residues in a ring of polynomials based on the product addition and the addition of moduli residues with the possibility of parallelizing calculations and avoiding the multiplicative inverse polynomial search procedure. At the same time, the results of intermediate calculations will not go beyond the set range, which eliminates the need to perform the operation of finding residue relatively large modulo $P(x)$.

Polynomial recovery method based on addition of the product of the polynomial moduli. Let us consider the system of congruences, which is built based on relation (1):

$$\begin{cases} b_1(x) \equiv N(x) \bmod p_1(x) \\ b_2(x) \equiv N(x) \bmod p_2(x) \\ \dots\dots\dots\dots\dots \\ b_k(x) \equiv N(x) \bmod p_k(x). \end{cases} \tag{5}$$

Any congruence modulo $p_1(x)$ with the residue $b_1(x)$ (e.g., $a(x) \bmod p_1(x) \equiv b_1(x)$) can be represented in the form of $a(x) = \gamma(x) p_1(x) + b_1(x)$, where $\gamma(x)$ is a polynomial that indicates how many times modulo $p_1(x)$ must be added to the residue $b_1(x) = N_1(x)$ to satisfy the relation $N_2(x) \bmod p_2(x) \equiv b_2(x)$. In this case $N_2(x) = N_1(x) + \gamma_1(x) p_1(x)$. Next, it is necessary to add the product $p_1(x)p_2(x)$ until the congruence $N_3(x) \bmod p_3(x) \equiv b_3(x)$, where $N_3(x) = N_2(x) + \gamma_2(x) p_1(x) p_2(x)$, is fulfilled. This procedure continues until the last equation (5) is satisfied. Analytically, it is written as follows:

$$\begin{gathered} N_1(x) = b_1(x); \\ N_2(x) = N_1(x) + \gamma_1(x)p_1(x) = b_1(x) + \gamma_1(x)p_1(x);\ N_2(x) \bmod p_2(x) \equiv b_2(x); \\ N_3(x) = N_2(x) + \gamma_2(x)p_1(x)p_2(x) = b_1(x) + \gamma_1(x)p_1(x) + \gamma_2(x)p_1(x)p_2(x);\ N_3(x) \bmod p_3(x) \equiv b_3(x); \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ N_i(x) = N_{i-1}(x) + \gamma_{i-1}(x)p_1(x)p_2(x)\dots p_{i-1}(x);\ N_i(x) \bmod p_i(x) \equiv b_i(x); \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ N_k(x) = N(x) = N_{k-1}(x) + \gamma_{k-1}(x)p_1(x)p_2(x)\dots p_{k-1}(x);\ N_k(x) \bmod p_k(x) \equiv r_k(x). \end{gathered} \tag{6}$$

The search for $\gamma_i(x)$ is carried out using the method of undetermined coefficients, and at each step of the algorithm, the degree of the polynomial $\gamma_i(x) = A_i x^i + A_{i-1} x^{i-1} + \ldots + A_1 x + A_0$ will be 1 degree less then $p_{i+1}(x)$: $\deg \gamma_i(x) = \deg p_{i+1}(x) - 1$.

Let us consider the following example. Let the given system of comparisons be:

$$\begin{cases} N(x) \bmod (x^2 + x + 1) \equiv x + 3 \\ N(x) \bmod (x^2 + x + 2) \equiv 2x + 5 \\ N(x) \bmod (x^3 + 2x + 1) \equiv x^2 + 4x + 1 \end{cases} \tag{7}$$

Without reducing the generality of the problem, we can assume that for polynomials $p_1(x), p_2(x), \ldots, p_k(x)$ their degrees satisfy the inequalities $\deg p_1 \geq \deg p_2 \geq \deg p_3 \geq \ldots \geq \deg p_k$. These conditions allow you to take larger steps when performing iterations.

Let us find the value of $a(x)$ in the relation $a(x) \bmod p_1(x) \equiv b_1(x)$. It can be presented in the form of $\left(\gamma(x)\left(x^2+x+1\right)+x+3\right) \bmod \left(x^2+x+2\right) = 2x+5$. Here, $\gamma(x)$ is a polynomial that indicates how many times modulo $p_1(x) = x^2 + x + 1$ must be added to the residue $x + 3 = N_1(x)$ in order to satisfy the relation $N_2(x) \bmod \left(x^2 + x + 2\right) \equiv 2x + 5$, where $N_2(x) = x + 3 + \gamma_1(x)\left(x^2 + x + 1\right)$. Since $p_1(x) = x^2 + x + 1$ is a polynomial of the second degree, it is advisable to present the found parameter $\gamma_1(x)$ in the form of a polynomial of the first degree: $\gamma_1(x) = A_1 x + A_0$. Then the product $\gamma_1(x)\left(x^2 + x + 1\right) = (A_1 x + A_0)\left(x^2 + x + 1\right) = A_1 x^3 + (A_1 + A_0)x^2 + (A_1 + A_0)x + A_0$ is obtained. To find the unknown coefficients A_i, consider the congruence $\left(A_1 x^3 + (A_1 + A_0)x^2 + (A_1 + A_0)x + A_0\right) \bmod \left(x^2 + x + 2\right) = \left(\left(x^2 + x + 2\right)(A_1 x + A_0) + (-A_1 x - A_0)\right) \bmod \left(x^2 + x + 2\right) = x + 2$. Therefore, taking into account the last expression, coefficients A_1 and A_0 take the values -1, -2, and, respectively, $\gamma(x) = -x - 2$, $N_2(x) = -x^3 - 3x^2 - 3x - 2$.

Next, it is necessary to add the product $p_1(x)p_2(x)=(x^2+x+1)(x^2+x+2)=(x^4+2x^3+4x^2+3x+2)$ until the congruence $N_3(x)\bmod p_3(x)=b_3(x)$ is satisfied, where $x^2+4x+1=((-x^3-3x^2-3x-2)+\gamma_2(x)(x^4+2x^3+4x^2+3x+2))\bmod(x^3+2x+1)$. First, the value of $(-x^3-3x^2-3x-2)\bmod(x^3+2x+1)=-3x^2-x-1$, which is placed on the left side of the latter equation, is calculated: $4x^2+5x+2=\gamma_2(x)(x^4+2x^3+4x^2+3x+2)\bmod(x^3+2x+1)$. Having reduced the modulo degree by 1, parameter $\gamma_2(x)$ should be searched for in the form of $\gamma_2(x)=A_2x^2+A_1x+A_0$, i.e., $4x^2+5x+2=(A_2x^2+A_1x+A_0)(x^4+2x^3+4x^2+3x+2)\bmod(x^3+2x+1)$. As $(x^4+2x^3+4x^2+3x+2)\bmod(x^3+2x+1)=2x^2-2x$, then $4x^2+5x+2=(A_2x^2+A_1x+A_0)(2x^2-2x)\bmod(x^3+2x+1)$ can be obtained. Next the value of $(A_2x^2+A_1x+A_0)(2x^2-2x)=2A_2x^4+2A_1x^3+(2A_0-2A_2)x^2-2A_1x-2A_0$ is calculated and the residue $(2A_2x^4+2A_1x^3+(2A_0-2A_2)x^2-2A_1x-2A)\bmod(x^3+2x+1)=(2A_0-6A_2)x^2+(-6A_1-2A_1)x-2A_0-2A_1$ is found. The search for unknown coefficients is reduced to the solution of the system of equations:

$$\begin{cases} 2A_0-6A_2=4 \\ -6A_1-2A_2=5 \\ -2A_0-2A_1=2 \end{cases}, \text{ or } \begin{cases} A_0-3A_2=2 \\ -6A_1-2A_2=5 \\ -A_0-A_1=1 \end{cases}.$$

Its solutions are the values of $A_2=-\frac{13}{16}, A_1=-\frac{9}{16}, A_0=-\frac{7}{16}$. So, by substituting A_2, A_1, A_0, we get the recovered polynomial from its residues according to the proposed algorithm:

$$N(x)=(-x^3-3x^2-3x-2)+(4x^2+5x+2)(x^4+2x^3+4x^2+3x+2)=4x^6+13x^5+28x^4+35x^3+28x^2+13x+2$$

Therefore, the solution to system (7) is a polynomial, which is obtained without the use of cumbersome operations and control over the overflow of the bit grid when performing intermediate calculations.

It should be noted that the proposed method is similar to Garner's algorithm, but the operation of finding the modular inverse in the ring of polynomials to obtain the corresponding coefficients is eliminated.

The method for decimal number recovery based on addition of the residue from the product of moduli. To simplify the calculations used in the proposed method, it is possible to add not the product of polynomials- moduli, but the residue from this product division by the corresponding polynomial. The mathematical notation of this method is as follows:

$$\begin{aligned}
&N_1(x)=b_1(x);\ p_{11}(x)=p_1(x)\bmod p_2(x);\\
&(N_1(x)+\gamma_1(x)p_{11}(x))\bmod p_2(x)=b_2(x);\\
&N_2(x)=N_1(x)+\gamma_1(x)p_1(x);\ p_{12}(x)=p_1(x)p_2(x)\bmod p_3(x);\\
&(N_2(x)+\gamma_2(x)p_{12}(x))\bmod p_3(x)=b_3(x);\\
&N_3(x)=N_2(x)+\gamma_2(x)p_1(x)p_2(x);\ p_{13}(x)=p_1(x)p_2(x)p_3(x)\bmod p_4(x);\\
&\qquad\qquad\qquad\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&(N_{i-1}(x)+\gamma_{i-1}(x)p_{1i-1}(x))\bmod p_i(x)=b_i(x);\\
&N_i(x)=N_{i-1}(x)+\gamma_{i-1}(x)p_1(x)p_2(x)p_3(x)\ldots p_{i-1}(x);\ p_{1i}(x)=p_1(x)p_2(x)\ldots p_i(x)\bmod p_{i+1}(x);\\
&\qquad\qquad\qquad\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&(N_{k-1}(x)+\gamma_{k-1}(x)p_{1k-1}(x))\bmod p_k(x)=r_k(x);\\
&N(x)=N_k(x)=N_{k-1}(x)+\gamma_{k-1}(x)p_1(x)p_2(x)p_3(x)\ldots p_{k-1}(x).
\end{aligned}\tag{8}$$

Let us consider an example of polynomial recovery from its residues adding the residue from the product of moduli based on system (7). Since $(x^2+x+1)\bmod(x^2+x+2)\equiv-1$, then from the first comparison (8) we obtain the congruence $(x+3-\gamma_1(x))\bmod(x^2+x+2)\equiv 2x+5$, in which it is necessary to determine a polynomial of the first degree $\gamma_1(x)=A_1x+A_0$ using the method of undetermined coefficients. Combining the last two equalities, it is possible to obtain $A_1=-1, A_0=-2$, respectively $\gamma_1(x)=-x-2$.

At the next stage, it is necessary to find the residue from the product $p_1(x)p_2(x)\bmod p_3(x)=((x^2+x+1)(x^2+x+2))\bmod(x^3+2x+1)=(x^4+2x^3+4x^2+3x+2)\bmod(x^3+2x+1)=2x^2-2x$ and then $N_2(x)=-x^3-3x^2-3x-2$. Thus, $-(x^3+3x^2+3x+2)+\gamma_2(x)(2x^2-2)\bmod(x^3+2x+1)=x^2+4x+1$ or $\gamma_2(x)(2x^2-2)\bmod(x^3+2x+1)=4x^2+5x+2$. As a result, a polynomial similar to the previous example is obtained.

Therefore, the developed methods for polynomial recovery from its residues in Z[x] ring make it possible to avoid complex operations, in particular, division with residues and finding the inverse element, as well as to perform calculations on polynomials of lower order in comparison with the classical CRT and Garner's algorithm.

Investigating the time complexity of the proposed methods. To calculate the time dependence of the developed methods, it is necessary to determine the most time-consuming basic arithmetic operations. The proposed algorithm includes multiplication, addition, and finding residues in a polynomial ring. In [28], it was proved that the multiplication problem $p(x)\cdot q(x)$ requires $O(4n\log n)$ bit operations (the logarithm is taken at base 2), where $n=\max\{\deg(p(x)),\deg(q(x))\}$ is the largest degree of the polynomial. Taking into account the complexity of finding residues [29], the total estimate is $O(5n\log n)$ of bitwise operations. It should be noted that the developed algorithms require $\frac{(k^2+k)}{2}$ multiplication operations, where k is the number of moduli, as well as finding the residue at each step. Therefore, the total complexity asymptotically approaches $O_1((k^2+k)n\log n)$.

In the classical Garner's algorithm, it is necessary to find the multiplicative inverse k times in the ring of polynomials. In [21] it is stated that the time complexity of the mentioned operation in the standard basis $GF(q^{\text{n}})$ over $GF(q)$ field, taking into account the complexity of the Euclidean algorithm $O(n\log^2 n)$ and its consequence $O(n\log^2 n\log\log n)$, is equal to $O(n\log^2 n(\log\log n+1))$. In addition, classical Garner's algorithm includes the same operations as the developed algorithms, that is, addition, multiplication, and finding residues. Due to this, its time complexity is $O_2((k^2+k)(n\log n)+kn\log^2 n(\log\log n+1))$.

Therefore, the proposed algorithm for number recovery from its residues allows reducing the time complexity from $O_2((k^2+k)(n\log n)+kn\log^2 n(\log\log n+1))$ to $O_1((k^2+k)n\log n)$. Figure 1 shows the graphs that indicate the dependences of the time complexities of the proposed and classical approaches to a polynomial recovery from its residues in the ring of polynomials when $k=10$ and n=1,…,1000.

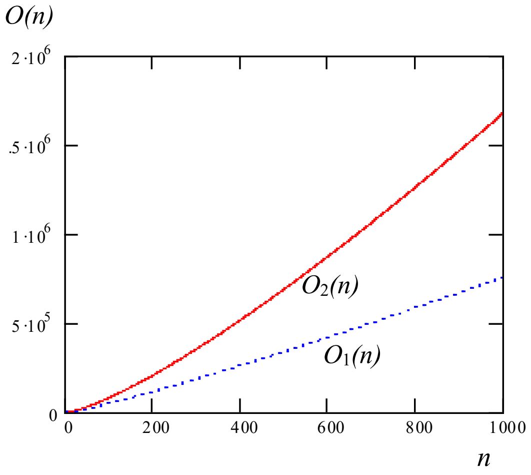

Fig. 1. Graphs of the time complexity dependences of the proposed method $O_1(n)$ and Garner's algorithm $O_2(n)$

It can be seen in Figure 1 that the use of the developed method of a polynomial recovery from its residues in the corresponding ring, which is based on the addition of the product of moduli-polynomials, allows us to reduce the time complexity. The results of the numerical experiment show an increase in both time complexities with an increase in dimensions of the input parameters.

The efficiency of the developed methods is determined by the ratio of the time complexities and in the general case is noted as follows:

$$E(n,k)=\frac{O_2(k,n)}{O_1(k,n)}=\frac{\left(\left(k^2+k\right)\left(n\log gn\right)+kn\log g^2 n\left(\log g\log gn+1\right)\right)}{\left(\left(k^2+k\right)n\log gn\right)}\approx 1+\frac{\log gn\left(\log g\log gn+1\right)}{k+1} \qquad (9)$$

Figure 2 shows a graph representing dependence of the proposed method efficiency in comparison with Garner's algorithm. Input parameters are selected within the following ranges: $1\le k\le 20$, a $1\le n\le 100($.

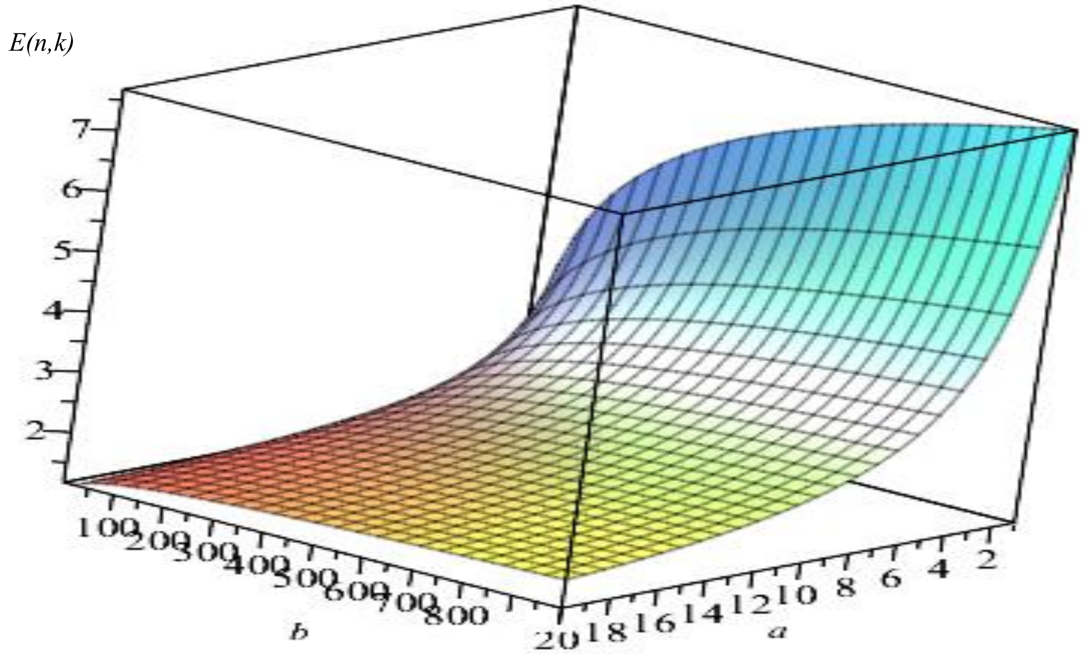

Fig. 2. Dependence of the proposed method efficiency in comparison with Garner's algorithm according to the number of moduli *k* and polynomial degrees *n*

It should be noted that the efficiency of the proposed method increases logarithmically with an increase in the degree of the polynomial, and decreases proportionally with an increase in the number of moduli.

Conclusions. Methods for the polynomial recovery in Z[x] ring are proposed, which make it possible to parallelize calculations and avoid the procedure of finding the polynomial multiplicative inverse due to the operations of adding the product of moduli and the product of residues from moduli that in turn leads to an increase in efficiency. As a result, the effect is achieved when the results of intermediate calculations go beyond the set range, which eliminates the need to find the residue from a polynomial of relatively high order. Analytical expressions of the time complexities of the proposed approach and Garner's algorithm due to the order of polynomials and the number of polynomials-moduli are obtained, which show that the use of the developed method makes it possible to reduce the time complexity. Graphs of the time complexity and efficiency dependences are presented. It is found that the efficiency of the proposed methods increases logarithmically with an increase in the degrees of polynomials, and decreases proportionally with an increase in the number of moduli.

References

1. Milne J.S. Algebraic Number Theory. MilneANT, 2020. 166p. URL: https://www.jmilne.org/math/CourseNotes/ANTc.pdf.
2. Narkiewicz W. Elementary and Analytic Theory of Algebraic Numbers. Berlin. Heidelberg: Springer, 2004. 712 p.
3. Kasianchuk M., Nykolaychuk Ya., Yakymenko I. Theory and Methods of Constructing of Modules System of the Perfect Modified Form of the System of Residual Classes. *Journal of Automation and Information Sciences*. 2016. V.48 (8). P.56-63. DOI: 10.1615/JAutomatInfScien.v48.i8.60.
4. Kasianchuk M., Yakymenko I., Nykolaychuk Y. Symmetric Cryptoalgorithms in the Residue Number System. *Cybernetics and Systems Analysis.* 2021. V. 57(2). P. 329–336. URL: https://doi.org/10.1007/s10559-021-00358-6.
5. Nykolaychuk Ya.M., Yakymenko I.Z.,. Vozna N.Ya, Kasianchuk M.M.. Residue Number System Asymmetric Cryptoalgorithms. *Cybernetics and Systems Analysis*. 2022. V. 58, No. 4, P.611-618. URL: https://doi.org/10.1007/s10559-022-00494-7.
6. Antoniou A., Nakato S., Rissner R. Irreducible polynomials in Int(Z). *ITM Web of Conferences International Conference on Mathematics*. 2018. V. 20, Article Number: 01004. URL: https://doi.org/10.1051/itmconf/20182001004.
7. Ivasiev S., Kasianchuk M., Yakymenko I., Shevchuk R., Karpinski M., Gomotiuk O. Effective algorithms for finding the remainder of multi-digit numbers. *Proceedings of the International Conference on Advanced Computer Information Technology.* 2019. P. 175-178. DOI: 10.1109/ACITT.2019.8779899.
8. Brandon M. M. Polynomial Functions over Rings of Residue Classes of Integers: Thesis. Georgia State University, 2007. 48 p. URL: https://doi.org/10.57709/1059690
9. Bajard J.C., Imbert L., Plantard T. Arithmetic operations in the polynomial modular number system. *Proceedings of the 17th IEEE Symposium on Computer Arithmetic*. 2005. P. 206–213. DOI: 10.1109/ARITH.2005.11.
10. Yatskiv V., Tsavolyk T. Improvement of Data Transmission Reliability in Wireless Sensor Networks on The Basis of Residue Number System Correcting Codes Using the Special Module System. *IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON).* 2017. P. 890 893. URL: https://doi.org/10.1109/UKRCON.2017.8100376
11. Su Jun, Yatskiv V. Method and Device for Image Coding & Transferring Based on Residue Number System. *Journal Sensors & Transducers*. 2013. Vol.148. P.60-65.
12. Freed M. RSA Encryption Using Polynomial Rings. Point Loma: Nazarene University< 2018. 17p. URL: https://www.whdl.org/sites/default/files/resource/academic/Freed-RSA%2520Encryption%2520Using%2520Polynomial%2520Rings-HP.pdf
13. Takagi T., Naito S. Construction of RSA Cryptosystem over the Algebraic Field Using Ideal Theory and Investigation of Its Security. *Electronics and Communications in Japan (Part III Fundamental Electronic Science)*. 2000. V. 83 (8). P. 19-29. DOI:10.1002/(SICI)1520-6440(200008)83:83.3.CO;2-S
14. Yakymenko I., Kasianchuk M., Shylinska I., Shevchuk R., Yatskiv V., Karpinski M. Polynomial Rabin Cryptosystem Based on the Operation of Addition. *12th International Conference on Advanced Computer Information Technology (ACIT)*. 2022. P. 345–350. DOI: 10.1109/ACIT54803.2022.9913089.
15. Chu J., Benaissa M. Error detecting AES using polynomial residue number systems. *Microprocessors and Microsystems*. 2013. V. 37. No 2. P. 228-234. URL: https://doi.org/10.1016/j.micpro.2012.05.010
16. Peter R. Turner Residue polynomial systems. *Theoretical Computer Science*. 2002. V.279 (1-2). P. 29–49. URL: https://doi.org/10.1016/S0304-3975(00)00425-4
17. Bajard J.C., Marrez J., Plantard T., Véron P. On Polynomial Modular Number Systems over Z/pZ. *Advances in Mathematics of Communications*. 2022. DOI: 10.3934/amc.2022018. URL: https://arxiv.org/abs/2001.03741

18. Skavantzos A., Stouraitis T. Complex multiplication using the polynomial residue number system: Advances in Computing and Control. *Lecture Notes in Control and Information Sciences*. 1989. V. 130. P. 61-70. URL: https://doi.org/10.1007/BFb0043257h
19. Mahatab K., Sampath K. Chinese remainder theorem for cyclotomic polynomials in Z[X]. *J. Algebra.* 2015. V. 435. P. 223-262. URL: https://doi.org/10.1016/j.jalgebra.2015.04.006.
20. Kalmykov I., Pashintsev V., Tyncherov K., Olenev A., Chistousov N. Error-Correction Coding Using Polynomial Residue Number System. *Appl. Sci.*. 2022. V. *12* (7). P.3365. URL: https://doi.org/10.3390/app12073365
21. Truong T.T., Tran M.T., Duong A.D. Improved Chebyshev Polynomials-Based Authentication Scheme in Client-Server Environment. *Security and Communication Networks*. 2019. V. 2019. Article ID 4250743. 11 p. URL: https://doi.org/10.1155/2019/4250743
22. Lawnik M., Kapczyński A. The application of modified Chebyshev polynomials in asymmetric cryptography. Computer Science. 2019. V. 20 (3). P. 367-381. URL: https://doi.org/10.7494/csci.2019.20.3.3307.
23. Vairachilai S., Kavithadevi M.K., Gnanajeyaraman R. Public Key Cryptosystems Using Chebyshev Polynomials Based on Edge Information. World Congress on Computing and Communication Technologies. 2014. P. 243-245. DOI: 10.1109/WCCCT.2014.21.
24. Li Z.H., Cui Y.D., Xu H.M.. Fast algorithms of public key cryptosystem based on Chebyshev polynomials over finite field. *The Journal of China Universities of Posts and Telecommunications*. 2011. V. 18 (2). P. 86-93. URL: https://doi.org/10.1016/S1005-8885(10)60049-0.
25. Karpinski M., Rajba S., Zawislak S., Warwas K., Kasianchuk M., Ivasiev S., Yakymenko I. A Method for Decimal Number Recovery from its Residues Based on the Addition of the Product Modules. *IEEE 10th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS*). 2019. V.1. P.13–17. DOI: 10.1109/IDAACS.2019.8924395.
26. Nykolaychuk Ya.M., Kasianchuk M.M., Yakymenko I.Z. Theoretical Foundations for the Analytical Computation of Coefficients of Basic Numbers of Krestenson's Transformation. *Cybernetics and Systems Analysis.* 2014. V. 50 (5). P. 649-654. DOI:10.1007/s10559-014-9654-0.
27. Rajba T., Klos-Witkowska AIvasiev., S., Yakymenko I., Kasianchuk M. Research of Time Characteristics of Search Methods of Inverse Element by the Module. IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). 2017. V.1. P.82–85. DOI: 10.1109/IDAACS.2017.8095054.
28. Harvey D., Hoeven J. Faster polynomial multiplication over finite fields using cyclotomic coefficient rings. *Journal of Complexity*. 2019. V. 54. P.101404. URL: https://doi.org/10.1016/j.jco.2019.03.004.
29. Aho A.V., Hopcroft J.E., Ullman J.D. The Design and Analysis of Computer Algorithms. Wesley Publishing Company, 1974. 480 p.

МЕТОД ВІДНОВЛЕННЯ ПОЛІНОМІВ ЗА ЇХ ЗАЛИШКАМИ НА ОСНОВІ ОПЕРАЦІЇ ДОДАВАННЯ В КІЛЬЦІ Z[X]

І. Якименко, М. Касянчук, І. Шилінська

Західноукраїнський національний університет
11, Львівська вул., Тернопіль, 46009, Україна
Emails: iyakymenko@ukr.net, kasyanchuk@ukr.net

Представлено методи відновлення поліномів за їх залишками в кільці Z[x]. Дана задача є актуальною для застосування в асиметричній та симетричній криптографії, алгоритмах завадозахищеного кодування, контролю та відновленню помилок в процесі передавання пакетів даних в комп’ютерних мережах та розподіленому зберіганню даних. Розглянуто теоретичні основи відновлення поліномів в кільці поліномів на основі відомих підходів, а саме, китайської теореми про залишки, алгоритму Гарнера, визначено їх переваги та недоліки. Розроблено нові методи зворотного перетворення з системи залишкових класів на основі операції додавання добутку модулів та добутку залишків поліномів. Побудовано аналітичні вирази часових складнощів запропонованого методу і алгоритму Гарнера. Представлено їх графічну залежність, яка вказує на те, що розроблений підхід відновлення полінома по його залишках у кільці Z[x] характеризується меншою складністю. Встановлено, що при збільшені розмірності вхідних параметрів зростають часові складності обох методів. Досліджено ефективність використання розробленого методу у кільці Z[x], яка вказує на логарифмічне зростання при збільшенні степенів полінома, і пропорційне зменшення у випадку збільшені кількості модулів.

Ключові слова: відновлення поліномів, кільце поліномів, залишки, Китайська теорема про алгоритм Гарнера, часова складність, ефективність.