Ihor Yakymenko
Mykhailo Kasianchuk
Mikolaj Karpinski
Ruslan Shevchuk
Inna Shylinska

FINDING THE INVERSE OF A POLYNOMIAL MODULO IN THE RING Z[X] BASED ON THE METHOD OF UNDETERMINED COEFFICIENTS

Abstract *This paper presents the theoretical foundations of finding the inverse of a polynomial modulo in the ring $Z[x]$ based on the method of undetermined coefficients. The use of the latter makes it possible to significantly reduce the time complexity of calculations avoiding the operation of finding the greatest common divisor. An example of calculating the inverse of a polynomial modulo in the ring $Z[x]$ based on the proposed approach is given. Analytical expressions of the time complexities of the developed and classical methods depending on the degrees of polynomials are built. The graphic dependence of the complexity of performing the operation of finding the inverse of a polynomial in the ring $Z[x]$ is presented, which shows the advantages of the method based on undetermined coefficients. It is found that the efficiency of the developed method increases logarithmically with an increase in the degrees of polynomials.*

Keywords inverse of a polynomial modulo, ring of polynomials, euclidean algorithm, degree of a polynomial, method of undetermined coefficients, time complexity, efficiency

Citation Computer Science 25(2) 2024: 1–14

1. Introduction

One of the most important and at the same time complex operation in the theory of algebra [1] and other mathematical applications [32] is the operation of finding the multiplicative inverse of a polynomial modulo in the ring $Z[x]$ [22,27]. The widespread use of this operation can be explained by its application in modern polynomial symmetric and asymmetric cryptography [24, 43] (in particular, post-quantum [11]), for solving problems of biometric identification of a person [3], in parallel and distributed calculations based on the Residue Number System [20, 34] in the ring $Z[x]$ [8, 36], data coding based on polynomial modular arithmetic [6, 38], signal and image processing [9, 17], for solving certain problems of linear programming [4] and in other applications of applied and discrete mathematics [25, 32, 41].

The methods of finding the multiplicative inverse of a polynomial in the ring $Z[x]$, as well as in the ring of integers [18, 19, 39], are characterized by significant computational complexities. Therefore, the development of new methods and improvement of the existing techniques for calculating the multiplicative inverse of a polynomial modulo in the ring $Z[x]$ is one of the most relevant problems.

One of the ways to solve this problem is the use of the method of undetermined coefficients. Nowadays, it is being successfully used for solving algebraic equations by factoring [10], decomposing a fraction, in which the numerator and denominator are polynomials, into simple fractions [5], finding the most optimal possible partial solutions to certain types of inhomogeneous ordinary differential equations [26], building some recurrent sequences [40], transforming logical functions, in particular, in Zhegalkin's algorithm [30], in integral calculus [29], in number methods [12].

According to the mentioned above, the purpose of our work is to develop a method for finding the inverse of a polynomial modulo based on the method of undetermined coefficients.

2. Related work

One of the most common methods for finding the multiplicative inverse of a polynomial in the ring $Z[x]$ is based on the extended Euclidean algorithm [7]. It should be noted that its application requires performing a large number of arithmetic operations on polynomials: division, finding residues [16], exponentiation [23], multiplication and substitution [14,44]. At the same time this method is characterized by the lowest time complexity compared to other known methods [21, 33].

When applying the Euclidean algorithm, finding the inverse of a polynomial is reduced to solving two problems: finding the greatest common divisor (GCD) of polynomials [28] and solving Diophantine equations [42] based on the extended Euclidean algorithm.

Let $f(x)$ and $g(x)$ be polynomials in the ring $Z[x]$ and $\deg(f(x)) > \deg(g(x))$, where the function *deg* denotes the degree of a polynomial. According to the main theorem of algebra for polynomials [31], there is a pair $q(x)$ and $r(x)$ from a ring $Z[x]$, for which $f(x) = q(x)g(x) + r(x)$, $0 < \deg r(x) < \deg g(x)$. Then, under the condition that $g(x)$ is not divisible by $r(x)$, for $g(x)$ the following equality is performed:

$$g(x) = r(x)q_1(x) + r_1(x), 0 < \deg r_1(x) < \deg r(x). \tag{1}$$

Next, if $r(x)$ is not divisible by $r_1(x)$, then:

$$r(x) = r_1(x)q_1(x) + r_2(x), 0 < \deg r_2(x) < \deg r_2(x). \tag{2}$$

This process is finite, that is, there exists such n, for which $r_{n-1}(x)$ will be divisible by $r_n(x)$.

As a result, a system of equations is obtained, on the basis of which, the GCD of two polynomials is found:

$$\begin{gathered} f(x) = q(x)g(x) + r(x), 0 < \deg r(x) < \deg g(x); \\ g(x) = r(x)q_1(x) + r_1(x), 0 < \deg r_1(x) < \deg r(x); \\ r(x) = r_1(x)q_2(x) + r_2(x), 0 < \deg r_2(x) < \deg r_1(x); \\ \cdots\cdots\cdots\cdots\cdots \\ r_{n-2}(x) = r_{n-1}(x)q_{n-1}(x) + r_n(x), 0 < \deg r_n(x) < \deg r_{n-1}(x); \\ r_{n-1}(x) = r_n(x)q_n(x). \end{gathered} \tag{3}$$

Sequence (3) determines the steps of applying the Euclidean algorithm, according to which the relationship of the GCD of polynomials comes true:

$$\begin{gathered} GCD(f(x), g(x)) = GCD(g(x), r(x)) = GCD(r(x), r_1(x)) = \dots \\ = GCD(r_{n-1}(x), r_n(x)) = r_n(x). \end{gathered} \tag{4}$$

Calculation of the inverse of a polynomial in the ring $Z[x]$ is reduced to solving the Diophantine equation, since the two relatively prime polynomials $f(x)$ and $g(x)$ can match the following polynomials $l(x)$, $s(x)\in$Z[x] for which the equality $f(x) \cdot l(x) + g(x) \cdot s(x)$ $=GCD(f(x), g(x))=w$ holds. If $f(x)$ and $g(x)$ are not relatively prime polynomials, then according to the definition of the ring, the inverse of a polynomial does not exist.

To simplify the procedure for finding the inverse of a polynomial, formula (4) must be written as follows:

$$\begin{gathered} r(x) = f(x) - q(x)g(x); \\ r_1(x) = g(x) - r(x)q_1(x) = g(x) - (f(x) - q(x)g(x))q_1(x) = \\ g(x)(1 + q(x)q_1(x)) - f(x)q_1(x); \\ \cdots\cdots\cdots\cdots\cdots \\ GCD(f(x), g(x)) = r_n(x) = f(x)l(x) + g(x)s(x). \end{gathered} \tag{5}$$

The notation $GCD(f(x), g(x))$ is called the Bezout relation for polynomials and the polynomials $l(x)$ and $s(x)$ are Bezout's polynomials. Then, $f(x)^{-1} \bmod g(x) = l(x) \bmod g(x)$.

In [45], the mathematical foundations of permutation polynomials, whose degrees do not exceed 6, and their inverse polynomials in finite fields were presented. It was noted that the results of the conducted research could be applied in cryptography, coding theory and combinatorial design theory.

Work [35] is devoted to the problem of finding the inverse of a polynomial in the Nth Degree Truncated Polynomial Ring. The method proposed in this work is based on finding the inverse of the polynomial using an adaptive inverse algorithm determined in the field of polynomials with binary and ternary coefficients. It was also noted that this algorithm could be extended for polynomials with coefficients of different fields, including $Z(x)$. The efficiency of the algorithm was studied in comparison with the inverse algorithm of Zhao and Su.

In [25], the method for inverse polynomial mappings was used to build the optimal interpolation nodes on discrete intervals. It was shown that this method was highly efficient for T-polynomials. In [13], it was noted that there was a length limitation for the inverse polynomial depending on the value of the acceptable error. In addition, five examples of polynomial inversion for solving physics and mathematics problems were presented. In [37], an algorithm generating the inverse elements over finite fields GF (3^m) was presented. Calculations were based on multiplication, squaring and cubing.

3. Method for calculating the inverse of a polynomial modulo in the ring Z(x)

Let us find the inverse of a polynomial modulo $m(x) = r^{-1}(x) \bmod g(x)$ in the ring of polynomials $Z(x)$, where $r(x)$ and $g(x)$ are relatively prime polynomials $(GCD(r(x), g(x)) = w, w \in Z)$ and $\deg r(x) = n$, $\deg g(x) = l$ for which the equality holds:

$$r(x) \cdot m(x) \equiv w \bmod g(x). \tag{6}$$

At the same time, the degree of a polynomial $\deg m(x) = l - 1$, since the residue modulo $g(x)$ will be a polynomial of $l - 1$ degree. Let $f(x) = r(x) \cdot m(x)$ and $r(x) = A_nx^n + A_{n-1}x^{n-1} + \ldots + A_1x + A_0$, $g(x) = B_lx^l + B_{l-1}x^{l-1} + \ldots + B_1x + B_0$, then $m(x) = C_kx^k + C_{k-1}x^{k-1} + \ldots + C_1x + C_0$, where $A_i, B_j, C_k \in Z$, $i = 0 \ldots n, j = 0 \ldots l, k = 0 \ldots l - 1$. Based on the method of undetermined coefficients, equality (6) for polynomials $r(x)$, $g(x)$ and $m(x)$ can be written as follows:

$$\begin{gathered} x^n + A_{n-1}x^{n-1} + \ldots + A_1x + A_0) \cdot (C_kx^k + C_{k-1}x^{k-1} + \ldots \\ +C_1x + C_0)) \bmod (B_lx^l + B_{l-1}x^{l-1} + \ldots + B_1x^1 + B_0) = w, \end{gathered} \tag{7}$$

or

$$\begin{gathered} ((A_nx^n + A_{n-1}x^{n-1} + \ldots + A_1x + A_0) \cdot (C_kx^k + C_{k-1}x^{k-1} + \ldots \\ +C_1x + C_0)) \bmod (B_lx^l + +B_{l-1}x^{l-1} + \ldots + B_1x^1 + B_0) - w = 0. \end{gathered} \tag{8}$$

First, we need to find the value $f(x) = r(x) \cdot m(x)$:

$$\begin{gathered} f(x) = A_n x^n \cdot (C_k x^k + C_{k-1} x^{k-1} + \ldots \\ +C_1 x + C_0) + A_{n-1} x^{n-1} (C_k x^k + C_{k-1} x^{k-1} + \ldots \\ +C_1 x + C_0) + \ldots + +A_1 x (C_k x^k + C_{k-1} x^{k-1} + \ldots \\ +C_1 x + C_0) + A_0 (C_k x^k + C_{k-1} x^{k-1} + \ldots + C_1 x + C_0) = \\ A_n C_k x^{n+k} + (A_n C_{k-1} + A_{n-1} C_k) x^{n+k-1} + \\ (A_n C_{k-2} + A_{n-1} C_{k-1} + A_{n-2} C_k) x^{n+k-2} + \ldots \\ +(A_0 C_1 + A_1 C_0) x + A_0 C_0. \end{gathered} \tag{9}$$

In expression (9), $\deg f(x) = n + k$. Let us introduce the notations: $F_{n+k} = A_n C_k$, $F_{n+k-1} = (A_n C_{k-1} + A_{n-1} C_k)$, $F_{n+k-2} = (A_n C_{k-2} + A_{n-1} C_{k-1} + A_{n-1} C_k)$, $\ldots$, $F_1 = (A_0 C_1 + A_1 C_0)$,$F_0 = A_0 C_0$. Then, equality (9) can be written as follows:

$$f(x) = F_{n+k} x^{n+k} + F_{n+k-1} x^{n+k-1} + \ldots + F_1 x + F_0. \tag{10}$$

The problem of determining the coefficients $C_k \in Z$ arises, for which condition (7) is fulfilled. Therefore, it is necessary to find the residue on division $f(x)$ by $g(x)$:

$$\begin{gathered} (F_{n+k} x^{n+k} + F_{n+k-1} x^{n+k-1} + \ldots \\ +F_1 x + F_0) \bmod (B_l x^l + B_{l-1} x^{l-1} + \ldots + B_1 x^1 + B_0). \end{gathered} \tag{11}$$

Let us consider the polynomial:

$$f(x) - \frac{F_{n+k}}{B_l} x^{n+k-l} g(x) = f_1(x), B_l \neq 0. \tag{12}$$

Given (10), expression (12) can be written as follows:

$$\begin{gathered} (F_{n+k} x^{n+k} + F_{n+k-1} x^{n+k-1} + \ldots \\ +F_1 x + F_0) - \frac{F_{n+k}}{B_l} x^{n+k-l} (B_l x^l + B_{l-1} x^{l-1} + \ldots \\ +B_1 x^1 + B_0) = f_1(x). \end{gathered} \tag{13}$$

Moreover, $\deg f(x) > \deg f_1(x)$ and the coefficient of the highest degree is determined according to the relation: $f_1(x) = (\frac{F_{n+k-1} \cdot B_l - F_{n+k} \cdot B_{l-1}}{B_l^2}) = F_{1nk}$, $\deg f_1(x) = n + k - 1 = n_1$.

If $\deg f_1(x) > \deg g(x)$, then the equality can be written as follows:

$$\begin{gathered} f_1(x) - (\frac{F_{n+k-1} \cdot B_l - F_{n+k} \cdot B_{l-1}}{B_l^2}) x^{n+k-l-1} g(x) = \\ f_1(x) - F_{1nk} x^{n+k-l-1} g(x) = f_2(x), \end{gathered} \tag{14}$$

where $\deg f_1(x) > \deg f_2(x)$, coefficient $f_2(x) = F_{2n}$ and $\deg f_2(x) = n_2$. It is not difficult to make sure that$\deg f_2(x) > \deg g(x)$, that is $n_2 \geq l$. Therefore, you can continue this procedure and write the following equality:

$$f_2(x) - \frac{F_{2nk}}{B_l} x^{n_2-l} g(x) = f_3(x), \tag{15}$$

where the condition $\deg f_2(x) > \deg f_3(x)$ is fulfilled for degrees of polynomials, the coefficient of the maximum degree of the polynomial $f_3(x)$ is F_{3nk} and $\deg f_3(x) = n_3$.

If $n_3 \geq l$, then the following equality is obtained in a similar way:

$$f_3(x) - \frac{F_{3nk}}{B_l} x^{n_3-l} g(x) = f_4(x), \tag{16}$$

where $\deg f_2(x) > \deg f_3(x)$. According to the above notations, $f_3(x) = F_{3nk}$ and $\deg f_3(x) = n_3$. It should be noted that the degrees of the created polynomials $f_1(x)$, $f_2(x)$, $f_3(x)$, $\ldots$ decrease ($n_1 > n_2 > n_3 > \ldots$), therefore, after a finite number of steps s the following polynomial is obtained:

$$f_s(x) - \frac{F_{snk}}{B_l} x^{n_s-l} g(x) = f_{s+1}(x). \tag{17}$$

The degrees of polynomials satisfy the inequality $\deg f_s(x) > \deg f_{s+1}(x)$. According to the above relationships, the value of the residue is as follows: $(F_{n+k}x^{n+k} + F_{n+k-1}x^{n+k-1} + \ldots + F_1x + F_0) \bmod (B_lx^l + B_{l-1}x^{l-1} + \ldots$
$+ B_1x^1 + B_0) = f_{s+1}(x)$.

This leads to the following relationship adding all the equations (14)–(17):

$$\begin{gathered}
f(x) - \frac{F_{n+k}}{B_l} x^{n+k-l} g(x) + f_1(x) - \\
\frac{F_{1nk}}{B_l} x^{n_1-l} g(x) + f_2(x) - \frac{F_{2nk}}{B_l} x^{n_2-l} g(x) + f_3(x) - \\
\frac{F_{3nk}}{B_l} x^{n_3-l} g(x) + \ldots + f_s(x) - \frac{F_{snk}}{B_l} x^{n_s-l} g(x) = \\
(f_1(x) + f_2(x) + f_3(x) + \ldots + f_s(x)) \Rightarrow \\
f(x) - (\frac{F_{n+k}}{B_l} x^{n+k-l} + \frac{F_{1nk}}{B_l} x^{n_1-l} + \\
\frac{F_{2nk}}{B_l} x^{n_2-l} + \frac{F_{3nk}}{B_l} x^{n_3-l} + \ldots + \frac{F_{snk}}{B_l} x^{n_s-l}) = f_{s+1}(x).
\end{gathered} \tag{18}$$

As a result of transformations (18), a polynomial $f_{s+1}(x) = L_{s-1}x^{s-1} + L_{s-2}x^{s-2} + \ldots + L_1x + L_0$ of $\deg f_{s+1}(x) = s - 1$ order is obtained. Taking into account condition (7), the method of undetermined coefficients for calculating values $C_k \in Z$, where $k = 1 \ldots l-1$, leads to a system of s equations and s unknowns, which must be found:

$$L_{s-1} = 0,\ L_{s-2} = 0, \ldots, L_1 = 0,\ L_0 = w. \tag{19}$$

According to these equations, the value $C_k \in Z$ is calculated. The scheme of finding the inverse of a polynomial in a ring $Z(x)$ based on the method of undetermined coefficients is presented in Figure 1.

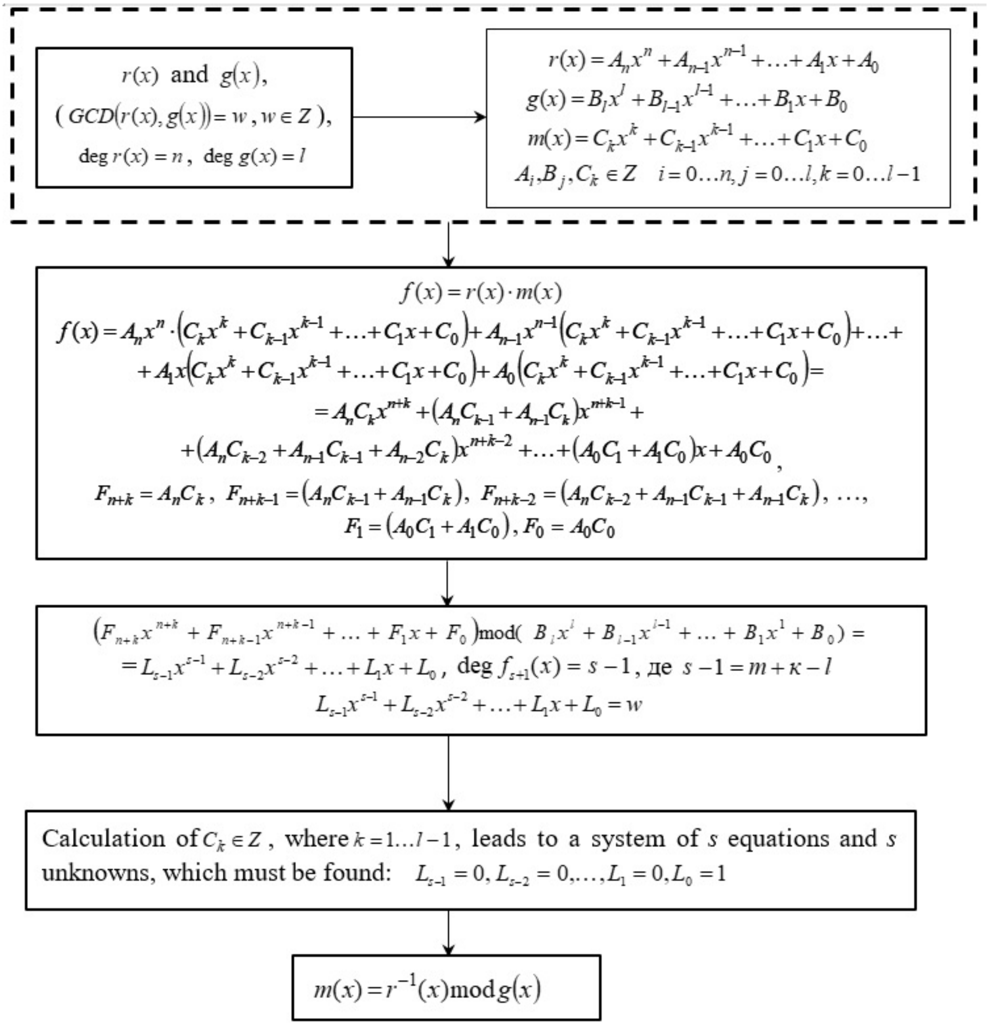
$r(x)$ and $g(x)$,
($GCD(r(x), g(x)) = w$, $w \in Z$),
$\deg r(x) = n$, $\deg g(x) = l$
$r(x) = A_n x^n + A_{n-1} x^{n-1} + \ldots + A_1 x + A_0$
$g(x) = B_l x^l + B_{l-1} x^{l-1} + \ldots + B_1 x + B_0$
$m(x) = C_k x^k + C_{k-1} x^{k-1} + \ldots + C_1 x + C_0$
$A_i, B_j, C_k \in Z \quad i = 0 \ldots n, j = 0 \ldots l, k = 0 \ldots l-1$
$f(x) = r(x) \cdot m(x)$
$f(x) = A_n x^n \cdot \left(C_k x^k + C_{k-1} x^{k-1} + \ldots + C_1 x + C_0\right) + A_{n-1} x^{n-1}\left(C_k x^k + C_{k-1} x^{k-1} + \ldots + C_1 x + C_0\right) + \ldots +$
$+ A_1 x\left(C_k x^k + C_{k-1} x^{k-1} + \ldots + C_1 x + C_0\right) + A_0\left(C_k x^k + C_{k-1} x^{k-1} + \ldots + C_1 x + C_0\right) =$
$= A_n C_k x^{n+k} + \left(A_n C_{k-1} + A_{n-1} C_k\right) x^{n+k-1} +$
$+ \left(A_n C_{k-2} + A_{n-1} C_{k-1} + A_{n-2} C_k\right) x^{n+k-2} + \ldots + \left(A_0 C_1 + A_1 C_0\right) x + A_0 C_0$,
$F_{n+k} = A_n C_k$, $F_{n+k-1} = \left(A_n C_{k-1} + A_{n-1} C_k\right)$, $F_{n+k-2} = \left(A_n C_{k-2} + A_{n-1} C_{k-1} + A_{n-1} C_k\right)$, ...,
$F_1 = \left(A_0 C_1 + A_1 C_0\right)$, $F_0 = A_0 C_0$
$\left(F_{n+k} x^{n+k} + F_{n+k-1} x^{n+k-1} + \ldots + F_1 x + F_0\right) \bmod \left(B_l x^l + B_{l-1} x^{l-1} + \ldots + B_1 x^1 + B_0 \right) =$
$= L_{s-1} x^{s-1} + L_{s-2} x^{s-2} + \ldots + L_1 x + L_0$, $\deg f_{s+1}(x) = s-1$, де $s-1 = m + \kappa - l$
$L_{s-1} x^{s-1} + L_{s-2} x^{s-2} + \ldots + L_1 x + L_0 = w$
Calculation of $C_k \in Z$, where $k = 1 \ldots l-1$, leads to a system of s equations and s unknowns, which must be found: $L_{s-1} = 0, L_{s-2} = 0, \ldots, L_1 = 0, L_0 = 1$
$m(x) = r^{-1}(x) \bmod g(x)$

Figure 1. The scheme of finding the inverse of a polynomial in the polynomial ring

4. An example of the application of the developed method

Let the polynomials be $r(x) = x^2 + 3x + 1$ and $g(x) = x^3 + 3x^2 + 2x + 1$. It is necessary to find $m(x) = r(x)^{-1} \bmod g(x) = (x^2 + 3x + 1)^{-1} \bmod (x^3 + 3x^2 + 2x + 1)$. According to the theoretical provisions presented above, the polynomial $m(x)$ is as follows: $m(x) = Ax^2 + Bx + C$. Taking into account (9), it is possible to obtain the product: $r(x) \cdot m(x) = (x^2 + 3x + 1) \cdot (Ax^2 + Bx + C) = Ax^4 + 3Ax^3 + Ax^2 + Bx^3 + 3Bx^2 + Bx + Cx^2 + 3Cx + C = Ax^4 + (3A+B)x^3 + (A+3B+C)x^2 + (B+3C)x + C$. Next, using the relationships (14)-(17), the residue of the division $r(x) \cdot m(x) \bmod g(x) = (Ax^4 + (3A + B)x^3 + (A + 3B + C)x^2 + (B + 3C)x + C) \bmod (x^3 + 3x^2 + 2x + 1)$ is obtained: $Ax^4 + (3A+B)x^3 + (2A+3B)x^2 + (A+2B)x + B = (Ax + B) \cdot (x^3 + 3x^2 + 2x + 1) + ((-A + C)x^2 + (-A - B + 3C)x + C - B)$.

As a result, a polynomial $f_3(x) = (-A+C)x^2 + (-A-B+3C)x + C - B$, whose degree is less than deg $g(x)$, is obtained as a residue. To simplify the calculations, let $f_3(x) = w = 1$, that, $(-A + C)x^2 + (-A - B + 3C)x + C - B = 1$. Then condition (19) for finding the unknown coefficients A, B and C leads to the following system of equations:

$$\begin{cases} C - A = 0 \\ 3C - A - B = 0 \\ C - B = 1 \end{cases} \tag{20}$$

Its solution determines the coefficients: $A = -1, B = -2, C = -1$.

Thus, the value of the inverse of a polynomial modulo in the ring Z[x] is calculated as follows: $m(x) = r(x)^{-1} \bmod g(x) = (x^2 + 3x + 1)^{-1} \bmod (x^3 + 3x^2 + 2x + 1) = -x^2 - 2x - 1$.

5. Estimating the computational complexity of the proposed algorithm for calculating the inverse of a polynomial in the ring Z[X]

When building analytical expressions for estimating the time complexity of calculating the inverse in a ring of polynomials according to the classical and proposed methods, it is necessary to determine the complexity of the most time-consuming operations, namely:

1. Product of two polynomials.
2. The residue of two polynomials.

At the first step of the implementation of the proposed method, according to (9), the most computationally complex operation is the multiplication of two polynomials $(A_nx^n + A_{n-1}x^{n-1} + \ldots + A_1x + A_0) \cdot (C_kx^k + C_{k-1}x^{k-1} + \ldots + C_1x + C_0)$. Its time complexity for polynomials of n degree was studied in [15] and consists of $O(n \log n)$ bit operations, where the logarithm is taken to the base 2. Given the complexity of finding residues [15], the general estimate is $O(2n \log n)$ of bit operations.

A well-known method of finding the inverse of a polynomial in a polynomial ring is based on the use of the Euclidean algorithm and its consequences. In [2], it was noted that the time complexity of finding the GCD $(p(x)$,$q(x))$ over the field $Z[X]$ according to the Euclidean algorithm has an upper limit $O(n \log^2 n)$, where

$n = \max\{\deg(p), \deg(q)\}$. In addition, the best known asymptotic estimate of the Euclidean inverse algorithm is equal to $O(n \log n \log \log n) \approx O(n \log n)$ [2].

Table 1 shows the basic operations and time complexities when using the proposed method for finding the inverse of a polynomial based on the method of undetermined coefficients and the classical method based on the extended Euclidean algorithm.

Table 1

Basic operations and time complexities of the proposed and classical methods for finding the inverse of a polynomial

Basic operations	Time complexity of the classical method, $O(n)$	Time complexity of the proposed method, $O(n)$
Computing the GCD (a, b) over the field by the Euclidean algorithm	$O(n \log^2 n)$, where $n = \max\{\deg(p), \deg(q)\}$	–
The extended Euclidean algorithm	$O(n \log n \log \log n) \approx O(n \log n)$	–
The product of two polynomials	–	$O(n \log n)$
Finding the residue of two polynomials	–	$O(n \log n)$

Taking into account the time complexities of the basic operations, the overall time complexity of the classical method of finding the inverse in the polynomial ring is $O1(n \log n \cdot (1 + \log n))$. Since, using the proposed method you do not need to find the GCD of polynomials, then the time complexity will decrease: $O2(2n \log n)$. Figure 2 shows the graphs that characterize the dependences of the time complexities of the proposed and classical methods for finding the inverse of a polynomial in the polynomial ring on the polynomial degrees.

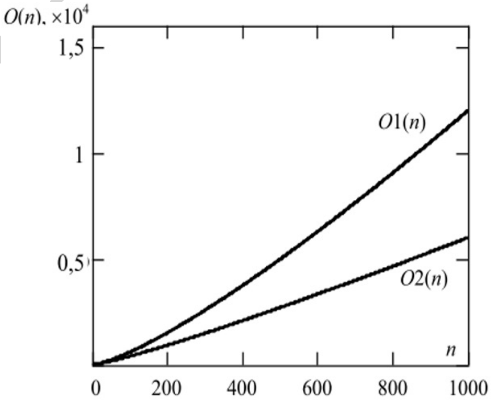

Figure 2. Time complexities of the classical $O1(n)$ and proposed $O2(n)$ methods

As a result of the numerical experiment, it was found that the complexity increases significantly with an increase in the degrees of polynomials.

The efficiency of the developed method in comparison with the classical one is defined as the relation of the respective complexities:

$$E(n) = \frac{O1(n)}{O2(n)} = \frac{n \log n \cdot (1 + \log n)}{2n \log n} = \frac{1 + \log n}{2}. \tag{21}$$

Due to expression (21), the found efficiency increases logarithmically with an increase in degrees of polynomials.

6. Conclusions

For the first time, an algorithm for finding the inverse of a polynomial in the ring $Z[x]$ based on the method of undetermined coefficients is proposed. A mathematical description of the developed method is presented and an example of its application is given. Analytical expressions of time complexities are built depending on the order of polynomials for the proposed method and the known one based on the Euclidean algorithm and its consequences. As a result of the conducted research, the higher efficiency of the algorithm based on the method of undetermined coefficients without finding the GCD of polynomials, has been proven. One of the main advantages of the proposed approach is the reduction of the time complexity from $O1(n \log n \cdot (1 + \log n))$ to $O2(2n \log n)$ compared to the known method. Graphic dependences of time complexities are presented. It is found that the efficiency of the proposed method increases logarithmically with an increase in the degrees of polynomials.

Further research in this field can be devoted to the development of the method for a polynomial recovery from its residues (Chinese Remainder Theorem for Polynomials), development of the theoretical foundations of the Residue Number System in the ring Z[x], its perfect and modified perfect forms, as well as the development of new polynomial encryption algorithms with increased resistance to cryptanalysis. In addition, we are currently working on the software and hardware implementation of the proposed algorithm, which will make it possible to detect limitations of the usage of some polynomial classes in the method of undetermined coefficients.

References

[1] Abdulazeez S.T., Hussein A.M.: The Existence of a Polynomial Inverse Integrating Factors and Studies About the Limit Cycles for Cubic, Quartic and Quintic Polynomial Systems, *Baghdad Science Journal*, vol. 18(2), pp. 0322–0322, 2021. doi: 10.21123/bsj.2021.18.2.0322.

[2] Aho A.V., Hopcroft J.E.: *The design and analysis of computer algorithms*, Pearson Education India, 1974.

[3] Andrijchuk V., Kuritnyk I., Kasyanchuk M., Karpinski M.: Modern algorithms and methods of the person biometric identification. In: *2005 IEEE Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, pp. 403–406, IEEE, 2005. doi: 10.1109/idaacs.2005.283012.

[4] Ashraphijuo M., Madani R., Lavaei J.: Inverse function theorem for polynomial equations using semidefinite programming. In: *2015 54th IEEE Conference on Decision and Control (CDC)*, pp. 6589–6596, IEEE, 2015. doi: 10.1109/cdc.2015.7403257.

[5] Beyer W.H.: CRC standard mathematical tables, *West Palm Beach*, 1978.

[6] Boucher D., Ulmer F.: Linear codes using skew polynomials with automorphisms and derivations, *Designs, codes and cryptography*, vol. 70, pp. 405–431, 2014.

[7] Calvez L., Azou S., Vilbé P.: Variation on Euclid's algorithm for polynomials, *Electronics Letters*, vol. 33(11), 1997. doi: 10.1049/el:19970658.

[8] Chu J., Benaissa M.: GF (2 m) multiplier using Polynomial Residue Number System. In: *APCCAS 2008-2008 IEEE Asia Pacific Conference on Circuits and Systems*, pp. 1514–1517, IEEE, 2008.

[9] Dadkhahi H., Gotchev A., Egiazarian K.: Inverse polynomial reconstruction method in DCT domain, *EURASIP Journal on Advances in Signal Processing*, vol. 2012, pp. 1–23, 2012. doi: 10.1186/1687-6180-2012-133.

[10] De Leon D.: Using undetermined coefficients to solve certain classes of variable-coefficient equations, *The American Mathematical Monthly*, vol. 122(3), pp. 246–255, 2015. doi: 10.4169/amer.math.monthly.122.03.246.

[11] Drucker N., Gueron S., Kostic D.: Fast polynomial inversion for post quantum QC-MDPC cryptography, *Information and Computation*, vol. 281, p. 104799, 2021. doi: 10.1016/j.ic.2021.104799.

[12] Dubeau F.: The method of undetermined coefficients: general approach and optimal error bounds, *Journal of Mathematical Analysis*, vol. 5(4), pp. 1–11, 2014.

[13] González-Cardel M., Díaz-Uribe R.: An analysis on the inversion of polynomials, *Revista mexicana de física E*, vol. 52(2), pp. 160–162, 2006.

[14] Goupil A., Palicot J.: Variation on variation on Euclid's algorithm, *IEEE Signal Processing Letters*, vol. 11(5), pp. 457–458, 2004. doi: 10.1109/lsp.2004.824053.

[15] Harvey D., van Der Hoeven J.: Faster polynomial multiplication over finite fields using cyclotomic coefficient rings, *Journal of Complexity*, vol. 54, p. 101404, 2019. doi: 10.1016/j.jco.2019.03.004.

[16] Ivasiev S., Kasianchuk M., Yakymenko I., Shevchuk R., Karpinski M., Gomotiuk O.: Effective algorithms for finding the remainder of multi-digit numbers. In: *2019 9th International Conference on Advanced Computer Information Technologies (ACIT)*, pp. 175–178, IEEE, 2019. doi: 10.1109/acitt.2019.8779899.

[17] Jassim W.A., Raveendran P., Mukundan R.: New orthogonal polynomials for speech signal and image processing, *IET Signal Processing*, vol. 6(8), pp. 713–723, 2012. doi: 10.1049/iet-spr.2011.0004.

[18] 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. In: *2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, vol. 1, pp. 13–17, IEEE, 2019. doi: 10.1109/idaacs.2019.8924395.

[19] Kasianchuk M., Nykolaychuk Y., 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*, vol. 48(8), 2016. doi: 10.1615/jautomatinfscien.v48.i8.60.

[20] Kasianchuk M., Yakymenko I., Nykolaychuk Y.: Symmetric cryptoalgorithms in the residue number system, *Cybernetics and Systems Analysis*, vol. 57(2), pp. 329–336, 2021. doi: 10.1007/s10559-021-00358-6.

[21] Kasianchuk M., Yakymenko I., Pazdriy I., Zastavnyy O.: Algorithms of findings of perfect shape modules of remaining classes system. In: *The experience of designing and application of CAD systems in microelectronics*, pp. 316–318, IEEE, 2015. doi: 10.1109/cadsm.2015.7230866.

[22] Katagiri Y., Iwamura K., Nakanishi Y., Takano S., Suzuki R.: Arbitrary polynomial chaos expansion and its application to power flow analysis-Fast approximation of probability distribution by arbitrary polynomial expansion. In: *Journal of Physics: Conference Series*, vol. 1780, p. 012025, IOP Publishing, 2021. doi: 10.1088/1742-6596/1780/1/012025.

[23] Kozaczko D., Ivasiev S., Yakymenko I., Kasianchuk M.: Vector module exponential in the remaining classes system. In: *2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, vol. 1, pp. 161–163, IEEE, 2015. doi: 10.1109/idaacs.2015.7340720.

[24] Krausz M., Land G., Richter-Brockmann J., Güneysu T.: Efficiently masking polynomial inversion at arbitrary order. In: *International Conference on Post-Quantum Cryptography*, pp. 309–326, Springer, 2022. doi: 10.1007/978-3-031-17234-2_15.

[25] Kroó A., Szabados J.: Inverse polynomial mappings and interpolation on several intervals, *Journal of Mathematical Analysis and Applications*, vol. 436(2), pp. 1165–1179, 2016. doi: 10.1016/j.jmaa.2015.12.032.

[26] Kwasniewski L.: An Improved Method of Undetermined Coefficients, *The Open Applied Mathematics Journal*, vol. 3(1), 2009. doi: 10.2174/1874114200903010033.

[27] Lasserre J.B.: Inverse polynomial optimization, *Mathematics of Operations Research*, vol. 38(3), pp. 418–436, 2013. doi: 10.1287/moor.1120.0578.

[28] Liu C.L., Horng G., Liu H.Y.: Computing the modular inverses is as simple as computing the GCDs, *Finite Fields and Their Applications*, vol. 14(1), pp. 65–75, 2008. doi: 10.1016/j.ffa.2007.08.004.

[29] Logan J.D.: *A first course in differential equations*, Springer, 2006. doi: 10.1007/978-1-4419-7592-8.

[30] Lombardi H., Quitté C., Lombardi H., Quitté C.: The Method of Undetermined Coefficients, *Commutative Algebra: Constructive Methods: Finite Projective Modules*, pp. 77–172, 2015. doi: 10.1007/978-94-017-9944-7_3.

[31] Milne J.S.: Algebraic Number Theory (v3.08), 2020. Available at www.jmilne.org/math/.

[32] Moreno J., Saiz A.: Inverse functions of polynomials and its applications to initialize the search of solutions of polynomials and polynomial systems, *Numerical Algorithms*, vol. 58(2), pp. 203–233, 2011. doi: 10.1007/s11075-011-9453-x.

[33] Nykolaychuk Y., Kasianchuk M., Yakymenko I.: Theoretical foundations for the analytical computation of coefficients of basic numbers of Krestensonś transformation, *Cybernetics and Systems Analysis*, vol. 50, pp. 649–654, 2014. doi: 10.1007/s10559-014-9654-0.

[34] Nykolaychuk Y., Yakymenko I., Vozna N., Kasianchuk M.: Residue Number System Asymmetric Cryptoalgorithms, *Cybernetics and Systems Analysis*, vol. 58(4), pp. 611–618, 2022. doi: 10.1007/s10559-022-00494-7.

[35] Nyokabi G.J., Salleh M., Mohamad I.: NTRU inverse polynomial algorithm based on circulant matrices using gauss-jordan elimination. In: *2017 6th ICT International Student Project Conference (ICT-ISPC)*, pp. 1–5, IEEE, 2017. doi: 10.1109/ict-ispc.2017.8075326.

[36] Paliouras V., Skavantzos A., Stouraitis T.: Low power convolvers using the Polynomial Residue Number System. In: *2002 IEEE International Symposium on Circuits and Systems. Proceedings (Cat. No. 02CH37353)*, vol. 2, pp. II–II, IEEE, 2002.

[37] Park C.M.: A Study on Constructing the Inverse Element Generator over GF (3 m), *Journal of information and communication convergence engineering*, vol. 8(3), pp. 317–322, 2010.

[38] Puchinger S., Wachter-Zeh A.: Fast operations on linearized polynomials and their applications in coding theory, *Journal of Symbolic Computation*, vol. 89, pp. 194–215, 2018. doi: 10.1016/j.jsc.2017.11.012.

[39] Rajba T., Klos-Witkowska A., Ivasiev S., Yakymenko I., Kasianchuk M.: Research of time characteristics of search methods of inverse element by the module. In: *2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, vol. 1, pp. 82–85, IEEE, 2017. doi: 10.1109/idaacs.2017.8095054.

[40] Rosen K.H.: *Handbook of discrete and combinatorial mathematics*, CRC press, 1999.

[41] Shams M., Rafiq N., Kausar N., Ahmed S.F., Mir N.A., Chandra Saha S.: Inverse Family of Numerical Methods for Approximating All Simple and Roots with Multiplicity of Nonlinear Polynomial Equations with Engineering Applications, *Mathematical Problems in Engineering*, vol. 2021, pp. 1–9, 2021. doi: 10.1155/2021/3124615.

[42] Xiao F., Lu D., Wang D.: Solving multivariate polynomial matrix Diophantine equations with Gröbner basis method, *Journal of Systems Science and Complexity*, vol. 35(1), pp. 413–426, 2022.

[43] Yakymenko I., Kasianchuk M., Shylinska I., Shevchuk R., Yatskiv V., Karpinski M.: Polynomial Rabin Cryptosystem Based on the Operation of Addition. In: *2022 12th International Conference on Advanced Computer Information Technologies (ACIT)*, pp. 345–350, IEEE, 2022. doi: 10.1109/acit54803.2022.9913089.

[44] Yakymenko I., Kasyanchuk M., Nykolajchuk Y.: Matrix algorithms of processing of the information flow in computer systems based on theoretical and numerical Krestensonś basis. In: *2010 International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET)*, pp. 241–241, IEEE, 2010.

[45] Zheng Y., Wang Q., Wei W.: On inverses of permutation polynomials of small degree over finite fields, *IEEE Transactions on Information Theory*, vol. 66(2), pp. 914–922, 2019. doi: 10.1109/tit.2019.2939113.

Affiliations

Ihor Yakymenko
West Ukrainian National University, Department of Cyber Security, 46009 Ternopil, Ukraine

Mykhailo Kasianchuk
West Ukrainian National University, Department of Cyber Security, 46009 Ternopil, Ukraine

Mikolaj Karpinski
University of the National Education Commission, Institute of Security and Computer Science, 30-084 Krakow, Poland
Ternopil Ivan Puluj National Technical University, Department of Cyber Security, 46001 Ternopil, Ukraine

Ruslan Shevchuk
University of Bielsko-Biala, Department of Computer Science and Automatics, 43-309 Bielsko-Biala, Poland
West Ukrainian National University, Department of Computer Science, 46009 Ternopil, Ukraine

Inna Shylinska
West Ukrainian National University, Foreign Languages and Information Communication Technologies Department, 46009 Ternopil, Ukraine

Received: 10.09.2023
Revised: 02.03.2024
Accepted: 21.03.2024