Factorization of the Degree of Sphenic Polynomials over the Galois Fields of Arbitrary Characteristics

ANATOLY BELETSKY
Department of Electronics
National Aviation University,
Kyiv-03058, av. Cosmonaut Komarov, 1,
UKRAINE

Abstract: By sphenic polynomials, we mean polynomials formed by the product of three (not necessarily different) irreducible polynomials with a priori unknown degree. The study's main goal is to develop a practical algorithm for factorizing degrees of sphenic polynomials with minimal computational complexity. Various options for the factorization of degree sphenic polynomials depend on the ratio degree and the cycle period of these polynomials. The sphenic polynomial cycle period defines as a parameter equal to the number of non-repeating subtractions computed on the linear-logarithmic scale of the group formed by the sphenic polynomial. The proposed algorithm is invariant to the Galois fields' characteristics generated by the sphenic polynomials' multipliers. Numerous numerical examples confirm the correctness of the results. Directions for further research outlines.

Key-Words: irreducible polynomials, sphenic polynomials, modulo comparability.

Received: June 25, 2021. Revised: March 19, 2022. Accepted: April 21, 2022. Published: May 18, 2022.

1 Introduction

The construction of the term *sphenic polynomial* (not yet used in mathematics, perhaps) is based on the closely related term *sphenic number* [1] from number theory, according to which

Definition 1. A *sphenic number* is an integer representing a product of three different simple non-negative numbers.

Sphenic numbers are *free of squares* [2] because all the prime factors must be varied. The concept of a sphenic polynomial (SP) is somewhat broader than the concept of a sphenic number.

Definition 2. A *sphenic polynomial* is a polynomial that can represent a product of three irreducible polynomials, *not necessarily distinct*.

It follows from the proposed definition that in sphenic polynomials, both two and three elements of the polynomial expansion can be the same. The removal in sphenic polynomials of the constraints in SPs typical for sphenic numbers expands the area of their possible applications.

In this paper, the research object is polynomials f_n of a degree of one variable over the Galois field of characteristic $p \geq 2$. To write the polynomial, we will use the *vector form* — the set of coefficients α_k of the polynomial, assuming

$$f_n = \alpha_n \alpha_{n-1} \ldots \alpha_k \ldots \alpha_1 \alpha_0 .$$

Polynomials f_n of *n*-degree in vector form can perceive as $(n+1)-$digit numbers in the $p-$ number system. Let us pay attention to the following properties of products of numbers and polynomials, formulating them (to make the text structured) as Axioms.

Axiom 1: The digit capacity of an arithmetic product of numbers does not exceed the sum of the digits of the product's factors.

Axiom 2: The degree of a modular product of polynomials is equal to the sum of degrees of the product's factors.

Let us illustrate the fundamental differences between products of numbers and products of polynomials (in vector form) by numerical examples.

Example 1. Let $f^{(1)} = 1101_2$ and $f^{(2)} = 111_2$ is a pair of irreducible polynomials and , $d^{(1)} = 13_{10}$,

$d^{(2)} = 7_{10}$ — their numerical equivalents, here $(a)_m$ is the number a in $m-$th number system.

The products of numbers are formed by means of the usual arithmetic operations of multiplication $(\times)$ and subsequent addition of digits $(+)$ with an inter-digit carry. For the chosen example, $d = d^{(1)} \times d^{(2)}$ the expanded form of which is:

$$\begin{array}{r} 1101 - d^{(1)} \\ \times \quad 111 - d^{(2)} \\ \hline 1101 \\ + \quad 1101 \\ \quad 1101 \\ \hline 1011011 - d \end{array} . \qquad (1)$$

According to (1) $d = 1011011_2 = 91_{10}$. Consequently, the multiplication of non-negative integers with carrying performs according to the rules of the natural number multiplication Table.

The modular operations of multiplication $\overset{p}{\otimes}$ and addition $\overset{p}{\oplus}$, in which $p-$is a field characteristic, are used for the product of polynomials over the $GF(p)$. If the operands are binary, the parameter p can exclude. For the example under consideration, we obtain

$$\begin{array}{r} 1101 \\ \otimes \quad 111 \\ \hline 1101 \\ \oplus \quad 1101 \\ \quad 1101 \\ \hline 100011 \end{array} . \qquad (2)$$

From a comparison of expressions (1) and (2) we see that the results of calculations, let us denote them R (at R lower indices are possible), are different, as they should be. In particular $R_1 = 1011011_2 = 91_{10} = (13 \cdot 7)_{10}$, whereas $R_2 = 100011_2 = 35_{10}$.

Example 2. Let $d^{(1)} = 23_8$ and $d^{(2)} = 12_8$. We have $R = d^{(1)} \cdot d^{(2)} = 23_8 \cdot 12_8 = 276_8$. That is, the product of two-digit numbers is a three-digit octal number. Thus, the values of R_1 and R confirm the definition formulated by Axiom 1.

One of the most critical issues related to polynomials f_n is the type of polynomial expansion (factorization).

Definition 3. By the *type of decomposition* of a compound polynomial f_n, we will understand [3] the number of k and degree n_i, $i = \overline{1,k}$, of irreducible polynomials $f_{n_1}, f_{n_2}, \ldots, f_{n_k}$ (possibly repeated) whose product over forms a given polynomial f_n of degree $n = \sum_{i=1}^{k} n_i$.

If a natural number is $k-$*almost prime*, it has k prime factors [4]. Similarly, we shall call a polynomial f_n $k-$almost prime if it forms by the product of k prime (irreducible) polynomials. Their multiplication, restoring f_n, is performed over the field $GF(p)$.

For $k-$almost prime polynomials of $n-$ degree, let us introduce the notation $f_n^{[k]}$. Thus, a polynomial f_n is prime if and only if it is $1-$ almost prime, and semisimple if it is $2-$almost prime [5]. The problem of factorization of semisimple polynomials $f_n^{[2]}$ considers in [6].

The main task of this paper is to develop efficient algorithms for the degree decomposition of sphenic polynomials $f_n^{[3]}$ of one variable over Galois fields of arbitrary characteristics p.

Vector (numeric) forms of sphenic polynomials, in general, represent p-th numbers, formed by the product of three prime polynomials. In this case, the multiplication of the multipliers carries out without inter-digit transfers, similar to that shown by transformation (2). Unfortunately, as mentioned above, this modular transformation has not yet found proper coverage in the literature. At the same time, as it seems to the author of this paper, such transformation can find worthy application in such a direction as the factorization of extra-large semisimple numbers. However, this assumption remains as a hypothesis, the confirmation of which will require additional research.

Possible applications of the research results include the theory of factorization of integers [7], including factorization using polynomials [8], cryptography [9], and the algebraic theory of modular calculations [10, 11], etc.

2 Mathematical Foundations

Let it $f_n^{[3]}$ be a polynomial formed by the product over $GF(p)$ three, not necessarily different, irreducible polynomials (IP) with a priori unknown degree x, y and z such that

$$f_n^{[3]} = f_x \overset{p}{\otimes} f_y \overset{p}{\otimes} f_z . \quad (3)$$

Thus, the problem to be solved is reduced to the determination degrees of IPs jointly generating a sphenic polynomial $f_n^{[3]}$. The mathematical basis for factorization of degrees of polynomials $f_n^{[3]}$ base on the results obtained earlier in [6, 12], a summary of which (taking into account the specificity of IPs) give below.

In the classic version, to determine the three unknown variables x, y and z, it is necessary to make a system of three equations, each functionally dependent on these variables. As the first equation, according to (3), we take

$$x + y + z = n . \quad (4)$$

The second equation can be derived from the parameter introduced in [6, 12] and called the *cycle period* (Cord — cycle order) of the compound polynomial $f_n^{[3]}$. Let us define this parameter.

Definition 4. The cycle period $\mathrm{Cord}(f_n^{[k]})$ of an arbitrary $k-$almost prime polynomial will be named the number of non-repeating subtractions $\boldsymbol{S}$ computed on the linear-logarithmic scale of the group generated by the polynomial $f_n^{[k]}$.

Let us move on to an explanation of the term "linear-logarithmic group scale". For this purpose, we will need to involve two additional parameters: the order of IP f_n, denoted by $\mathrm{ord}(f_n)$, and the order of the composite polynomial — $\mathrm{ord}(f_n^{[k]})$. According to Theorem 6.11, [8], the order of the polynomial $f_n^{[k]}$ determines by the expression

$$\mathrm{ord}(f_n^{[k]}) = \mathrm{LCM}(\mathrm{ord}(f_{x1}), \mathrm{ord}(f_{x2}), \ldots, \ldots, \mathrm{ord}(f_{xl}), \ldots, \mathrm{ord}(f_{xk})), \quad n = \sum_{i=1}^{k} x_i . \quad (5)$$

In (5), the designations are slightly different from those in the original but equivalent to them.

The order P_{pr} of the primitive over $GF(p)$ polynomial f_n calculate by the formula

$$P_{pr} = \mathrm{ord}(f_n) = p^n - 1 .$$

If f_n not primitive, then order P_{ir} belongs to a subset of non-trivial divisors P_{pr}. Under conditions of a priori uncertainty about x, y and z the only estimation option $\mathrm{ord}(f_n^{[3]})$ is the sequential exponentiation of the generating element θ. The most straightforward way to calculate the order of SPs is when element $\theta = 10$ chose as the group generator, which is the minimal derivative element of the group of deductions modulo $f_n^{[3]}$. In this case, regardless of the field characteristic p, the formation of the following component g_{k+1} of group $GF^*(p^n)$ is reduced to a shift of one digit to the left of the previous element g_k with subsequent reduction g_{k+1} (if necessary) to the remainder modulo $f_n^{[3]}$.

Even for small parameters x, y and z values, not exceeding several tens, the estimation of SP $f_n^{[3]}$ orders encounters possibly insurmounTable obstacles associated with the need to perform calculations of a considerable volume. To overcome the "nightmare of large numbers," we will use the method of replacing the "linear scale" in the definition $\mathrm{ord}(f_n^{[3]})$ with a "linear-logarithmic scale.

The essence of the method is as follows. Let us paraphrase classical Lemma 2.3, [12] without changing its meaning, thus

Lemma 1. For each nonzero element $\alpha > 1$ of $GF(p)$, generated by IP f_n, the equality is satisfied $\alpha^{p^n-1} (\mathrm{mod}\, f_n) = 1$.

From Lemma 1, it follows

Consequence 1. Arbitrary irreducible over the field $GF(p)$ polynomials f_n (both primitive and non-primitive) support the comparison

$$1(0)^{[p^n-1]} \equiv 1 \pmod{f_n}, \qquad (6)$$

where $(a)^{[m]} = \underbrace{aa\ldots aa}_{m \text{ раз}}$.

Comparison (4) holds if and only if f_n — IP. It is convenient to use relation (6) as one of the criteria for the irreducibility of the tested polynomials. The irreducible criterion (6) is necessary but not sufficient for all degrees n of polynomials f_n [13].

Let us further formulate the two most critical formal specifications [6].

Definition 5. The sequence of natural numbers $k = 0, 1, 2, ..., p^n - 1$, which are measures of the degree of the forming element of the multiplicative group of maximum order (MGMO)

$$GF^*(p^n) = \left\{\theta^0, \theta^1, \ldots, \theta^k, ..., \theta^{p^n-1}\right\} \pmod{f_n}$$

let's call it the *linear scale* of the group.

Definition 6. The sequence of natural numbers $r = 1, 2, ..., n$, which are measures of the degree of the characteristic p of group $GF^*(p^n)$ of elements $t_{r,p} = p^r - 1$, is called the *logarithmic scale* of the group.

Let us summarize the numerical parameters in Table 1.

Table 1. Auxiliary parameters MGMO over $GF(2)$

r	1	2	3	4	5	6	7	8	…
$t_{r,2}$	1	3	7	15	31	63	127	255	…

Let us "tie" the parameters from Table 1 to the characteristics of the so-called *fiducial grid* (Fig. 1), which consists of a set of parallel straight lines (*grid steps*).

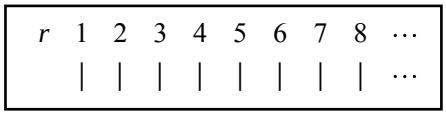

Fig. 1. Fiducial grid

In Table 1, the following designations adopt: $r-$ the number of the step of the fiducial grid; $t_{r,2}-$ the degree of the binary polynomial CV_r, let's call it the *Coordinate Vector*, the left bit of which is 1, and the rest filled with zeros, i.e.,

$$CV_r = \underset{t_{r,2}}{100...0}. \qquad (7)$$

The term "coordinate vector" in (7) is nothing but the word "round number" [14] mentioned above. However, after this, we will refer to it as a "coordinate vector", believing it to be more appropriate to the context.

The marks $t_{r,2}$, being evenly spaced on some axis, form "linear-logarithmic scale" mentioned earlier. The parameter $t_{r,2}$ is nothing more than the order (length) of the zero vector of the polynomial, the number of zero digits determined by the formula $t_{r,2} = 2^r - 1$.

We represent the fiducial grid (Fig. 1), corresponding to the polynomial f_n, in the form of a vector $1^{[n]} = \underbrace{11\ldots11}_{n \text{ бит}}$. Each $r-$th unit in $1^{[n]}$ symbolizes a coordinate vector CV_r calculated at the $r-$th step of the fiducial grid. The law of changing the order $t_{r,2}$ of zero digits of a binary vector CV_r can be quickly established by analyzing the data in the bottom line of Table 1. Namely

$$t_{r,2} = 2 \cdot t_{r-1,2} + 1,\ t_0 = 0,\ r = \overline{1,n}. \qquad (8)$$

Let us introduce some notations. Let $\boldsymbol{S}_r = Res(CV_r)_{f_n}$ denote the residue of the coordinate vector CV_r modulo a polynomial f_n. Relations (8) form the fundamental basis of the proposed algorithm for factorizing semisimple polynomials [6], which reduced to a sequence of simple recurrent computations

$$\boldsymbol{S}_r = Res(\boldsymbol{S}_{r-1} \cdot s_k)_{f_n},\ s_r = \boldsymbol{S}_{r-1}0,\ \boldsymbol{S}_0 = 1,\ r = \overline{1,n},$$

or else (for polynomials over field $GF(2)$)

$$\boldsymbol{S}_r = Res(\boldsymbol{S}_{r-1}^2 0)_{f_n},\ \boldsymbol{S}_0 = 1,\ r = \overline{1,n}. \qquad (9)$$

When the index r reaches the last rung of the fiducial ladder n if it turns out that $\boldsymbol{S}_n = 1$, this

will fulfill the comparison conditions (6). The sequence of residues $\boldsymbol{S}_r$ on the steps of the fiducial grid, formed by an arbitrary polynomial f_n, will be called a $\boldsymbol{S}-$*sequence of residues*.

To explain the previously introduced notion of "polynomial cycle period", let us turn to numerical examples. For this purpose, let us compare sequences of $\boldsymbol{S}-$residues formed by two polynomials belonging to different subclasses. As the first polynomial, let us choose a binary primitive polynomial of the sixth-degree $f_6^{(1)}=1000011$ and a simple IP $f_6^{(2)}=1001001$ — as the second polynomial. Calculating by formula (9), we obtain

Table 2. The sequence of $\boldsymbol{S}-$residues generated by $f_6^{(1)}$

$\boldsymbol{S}_1=10;$	$\boldsymbol{S}_4=101000;$
$\boldsymbol{S}_2=1000;$	$\boldsymbol{S}_5=100101;$
$\boldsymbol{S}_3=110;$	$\boldsymbol{S}_6=\boldsymbol{1}.$

Table 3. The sequence of $\boldsymbol{S}-$residues generated by $f_6^{(2)}$

$\boldsymbol{S}_1=10;$	$\boldsymbol{S}_4=1001;$
$\boldsymbol{S}_2=1000;$	$\boldsymbol{S}_5=10000;$
$\boldsymbol{S}_3=10010;$	$\boldsymbol{S}_6=\boldsymbol{1}.$

As follows from Tables 2 and 3, *periods of cycles* polynomials $f_6^{(1)}$ and $f_6^{(2)}$ coincide with the degree of IP, $\mathrm{Cord}(f_6^{(1)})=\mathrm{Cord}(f_6^{(2)})=6$. In contrast, $\mathrm{ord}(f_6^{(1)})=63$ and $\mathrm{ord}(f_6^{(2)})=9$ are different and determine the *orders* of the same polynomials.

Now let's turn to IP over $GF(p)$, $p>2$. Let's make Table 4 similar to Table 1, but for characteristics $p=3$.

Table 4. Auxiliary parameters MGMO for $GF(3)$

r	1	2	3	4	5	6	7	…
$t_{r,3}$	1	8	26	80	242	728	2186	…

From a comparison of data in Tables 1 and 4, we arrive at such generalized relations for degree $t_{r,p}$ and residue $\boldsymbol{S}_{r,p}$ of coordinate vector CV_r

$$t_{r,p}=p\cdot t_{r-1,p}+(p-1),\ t_{0,p}=0,\ r=\overline{1,n};$$
$$\boldsymbol{S}_{r,p}=Res(\boldsymbol{S}^{\,p}_{r-1,p}\underbrace{0\ldots0}_{p-1})_{f_n},\ \boldsymbol{S}_{0,p}=1,\ r=\overline{1,n}. \quad (10)$$

Let's look at a numerical example. Let the chosen IP of the sixth degree $f_6^{(3)}=1323401$ over the field $GF(5)$. The sequence of $\boldsymbol{S}-$ residues, calculated by the formula (10), is presented in Table 5

Table 5. The sequence of $\boldsymbol{S}-$residues generated by $f_6^{(3)}$

$\boldsymbol{S}_1=10000;$	$\boldsymbol{S}_4=414114;$
$\boldsymbol{S}_2=40240;$	$\boldsymbol{S}_5=130222;$
$\boldsymbol{S}_3=302403;$	$\boldsymbol{S}_6=\boldsymbol{1}.$

As in the previous versions of IP $f_6^{(1)}$ and $f_6^{(2)}$, for the polynomial $f_6^{(3)}$, we have $\mathrm{Cord}(f_6^{(3)})=6$, whereas $\mathrm{ord}(f_6^{(3)})=3906$, is the value obtained from the results of computer calculations.

Based on the examples considered, we arrive at the following Axiom.

Axiom 3. The cycle period of a simple and primitive polynomials f_n over a field $GF(p)$ is invariant to the field characteristic p and coincides with the degree of the polynomial, i.e., $\mathrm{Cord}(f_n)=n$.

Axiom 3 makes it possible, without loss of generality in the following numerical calculations, to restrict ourselves to considering polynomials over fields $GF(2)$.

3 Factorization Algorithm for Sphenic Polynomials

Factorization of degrees of sphenic polynomials (as is customary in classical methods) reduces to solving a system of three equations for the a priori unknown variables that are the degrees of the polynomial factors. Two equations (of the necessary three) are trivial and written in this form

$$\begin{aligned} x+y+z&=n,\\ \mathrm{LCM}(x,y,z)&=C, \end{aligned} \tag{11}$$

where for the sake of brevity $C=\mathrm{Cord}(f_n^{[3]})$.

The expression for the cycle period $\mathrm{Cord}(f_n^{[3]})$ of compound polynomials is similar to (3), which determines the order of the same polynomials. In particular, for sphenic polynomials

$$\mathrm{Cord}(f_n^{[3]})=\mathrm{LCM}(\mathrm{Cord}(f_x),\mathrm{Cord}(f_y),\dots \dots\mathrm{Cord}(f_z))$$

Equations (11) form an incompatible system, which, at first sight, seems a priori unsolvable. But it is not as bad as it looks. The problem becomes surmount if we involve in its solution the relation between the parameters n and C, and a subset of non-trivial divisors (NTDs) in the cycle period of $f_n^{[3]}$.

If, for example, it turns out that $C=n/3$, then this would mean that all three polynomials forming the SP are polynomials of degree $n/3$. On the other hand, if it is equal to the square of a natural number, then the solution of the system of equations (9) is as follows:

$$x=\sqrt{C};\ z=C;\ y=n-(x+z).$$

The structural-logical scheme in Fig. 2 represents the complete set of solutions for the system (9).

We turn to the analysis of ways to overcome the incompatibility of the system of equations (9). Let us pay attention to the following fact. Suppose that the binary SP form by the product over three irreducible polynomials whose a priori unknown degree $x=3$, $y=4$ and $z=6$. The cycle period of such an SP is defined by the expression

$$C=\mathrm{LCM}(x,y,z)=\mathrm{LCM}(3,4,6)=12.$$

Let us write out the set of NTDs, equal to $\{2,3,4,6\}$. From this example, all unknown degrees of the polynomial $f_n^{[3]}$ contained a subset C of non-trivial divisors of the cycle period of the polynomial.

The above relationship between the degrees of SPs and NTDs of the cycle period $f_n^{[3]}$ is not necessarily fully observed for all sphenic polynomials and their cycle periods. Nevertheless, it turns out to be very useful when solving the factorization of degrees in the general case of $k-$ almost simple polynomials.

Let us turn to the previously mentioned example, which assumes that all three components of an SP are polynomials of degree $n/3$. It is possible for the set of IPs f_x, f_y and f_z in this case. In the first version, we will assume that all polynomials are different. Let $f_x=1010111$, $f_y=1100111$ and $f_z=1101101$ answer by the sphenic polynomial $f_{18}^{[3]}=1001110000101011001$, which lead to Table 6.

Let $\boldsymbol{S}k$ be the eldest subtraction of the sequence (in bold in the Tables). If $\boldsymbol{S}k=1$, then all SP components are different and do not necessarily have to have the same degree (as in Table 6). Let us support this conclusion with an example.

Table 6. The sequence of $\boldsymbol{S}-$residues generated by the first variant of the $f_{18}^{[3]}$

$\boldsymbol{S}_1=10;$	$\boldsymbol{S}_4=1000000000000000;$
$\boldsymbol{S}_2=1000;$	$\boldsymbol{S}_5=11111010101001010;$
$\boldsymbol{S}_3=10000000;$	$\boldsymbol{S}_6=\boldsymbol{1}.$

Let $f_x=111$, $f_y=1101$ and $f_z=10011$. Then $f_9^{[3]}=1001010101$, $C=12$. $\boldsymbol{S}-$residues are summarized in Table 7.

Table 7. The sequence of $\boldsymbol{S}-$residues generated by the $f_9^{[3]}$

$\boldsymbol{S}_1=10;$	$\boldsymbol{S}_7=110010110;$
$\boldsymbol{S}_2=1000;$	$\boldsymbol{S}_8=110011100;$
$\boldsymbol{S}_3=10000000;$	$\boldsymbol{S}_9=100010100;$
$\boldsymbol{S}_4=100010111;$	$\boldsymbol{S}_{10}=10000011;$
$\boldsymbol{S}_5=10001001;$	$\boldsymbol{S}_{11}=100011101;$
$\boldsymbol{S}_6=110010101;$	$\boldsymbol{S}_{12}=\boldsymbol{1}.$

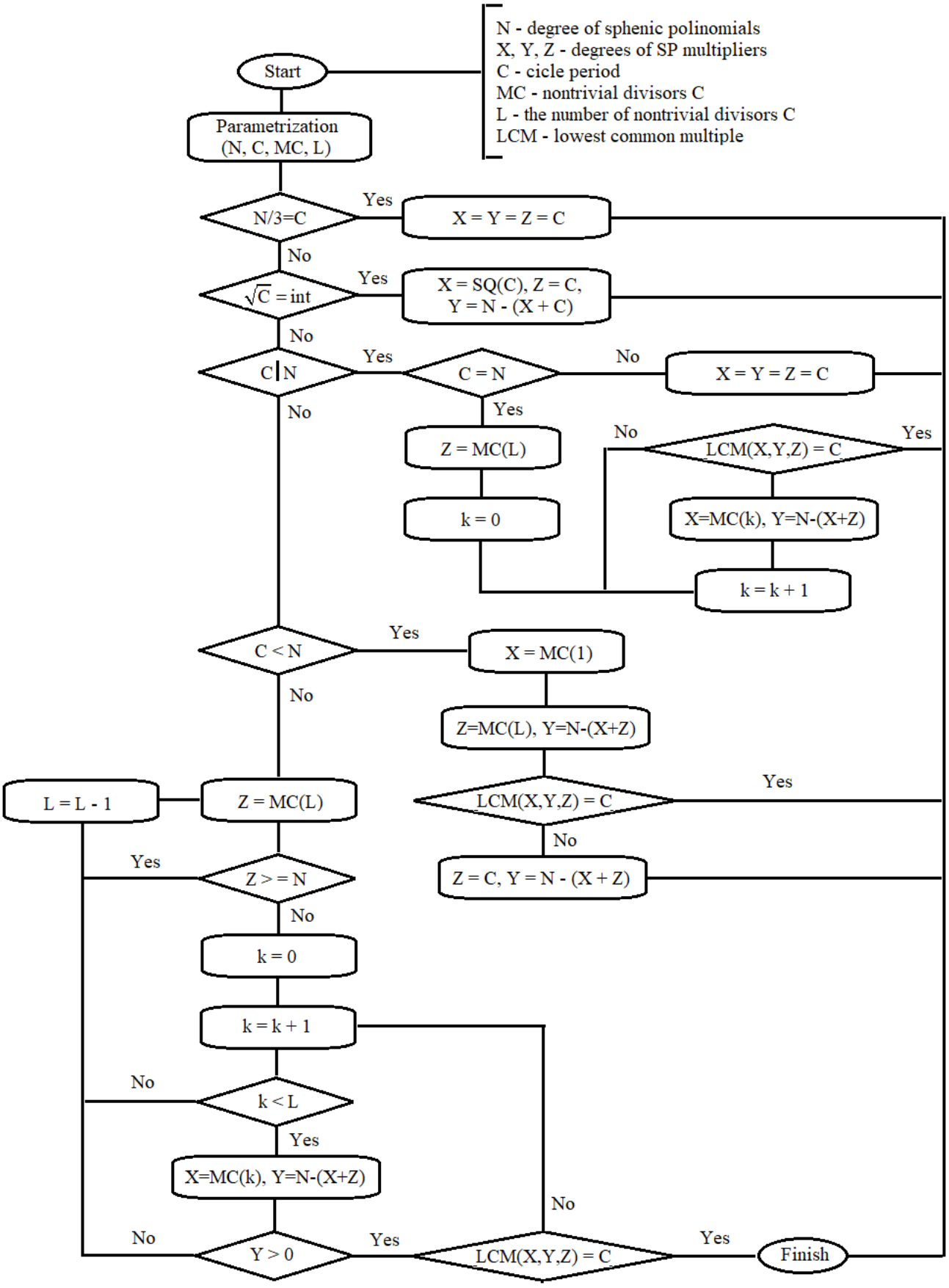

Fig. 2. Structural-logical scheme of the algorithm for factorization of degrees of sphenic polynomials

We will assume that two of the three IPs are the same in the second version. Let $f_x = f_y = 1100111$ and $f_z = 1101101$. Based on the selected parameters we have $f_{18}^{[3]} = 1110110001100001001$, $C = 6$ which leads to Table 8.

Table 8. The sequence of $\boldsymbol{S}-$residues generated by the second variant of the $f_{18}^{[3]}$

$\boldsymbol{S}_1 = 10;$	$\boldsymbol{S}_5 = 100101100011011100;$
$\boldsymbol{S}_2 = 1000;$	$\boldsymbol{S}_6 = 10110100111010010;$
$\boldsymbol{S}_3 = 10^{[7]};$	$\boldsymbol{S}_7 = \mathbf{10}.$
$\boldsymbol{S}_4 = 10^{[15]};$	

We obtain a similar result (by the value of $\boldsymbol{S}k$) when the degree of polynomial f_z is different from the degree of polynomials f_x, f_y.

Let $f_x = f_y = 1011$ and $f_z = 11001$. Then $f_{10}^{[3]} = 11000111101$, $C = 12$, and the sequence of $\boldsymbol{S}-$residues give in Table 9. Note that the sequence of $\boldsymbol{S}-$residues in Tables 8 and 9 ends with the value $\boldsymbol{S}k = 10$.

Table 9. The sequence of $\boldsymbol{S}-$residues generated by the $f_{10}^{[3]} = 11000111101$

$\boldsymbol{S}_1 = 10;$	$\boldsymbol{S}_7 = 1100111110;$
$\boldsymbol{S}_2 = 1000;$	$\boldsymbol{S}_8 = 101011001;$
$\boldsymbol{S}_3 = 10000000;$	$\boldsymbol{S}_9 = 1110111100;$
$\boldsymbol{S}_4 = 100010110;$	$\boldsymbol{S}_{10} = 1000111;$
$\boldsymbol{S}_5 = 1001101;$	$\boldsymbol{S}_{11} = 1101110001;$
$\boldsymbol{S}_6 = 1111111001;$	$\boldsymbol{S}_{12} = 1010101000;$
	$\boldsymbol{S}_{13} = \mathbf{10}.$

Finally, the third option assumes all three sphenic polynomials factors are the same. Let $f_x = f_y = f_z = 1101101$. We obtain the following parameter values $f_{18}^{[3]} = 1110111100111111101$ and $C = 6$. The sequence of $\boldsymbol{S}-$residues showed in Table 10.

Table 10. The sequence of $\boldsymbol{S}-$residues generated by the third variant of the $f_{18}^{[3]}$

$\boldsymbol{S}_1 = 10;$	$\boldsymbol{S}_5 = 1110111100111110110;$
$\boldsymbol{S}_2 = 1000;$	$\boldsymbol{S}_6 = 111011110001111110;$
$\boldsymbol{S}_3 = 10^{[7]};$	$\boldsymbol{S}_7 = 110011110011111110;$
$\boldsymbol{S}_4 = 10^{[15]};$	$\boldsymbol{S}_8 = \mathbf{1000}.$

Thus, according to Table 6-10, the value of senior residues $\boldsymbol{S}k$ can indicate the quality of the SP components. Namely, if $\boldsymbol{S}k = 1$, it means that all the factors of the sphenic polynomial are different. If $\boldsymbol{S}k = 10$, two of the three SP factors are the same. And finally, if $\boldsymbol{S}k = 1000$, it means that all three SP factors are the same.

Let's return to the structural and logical scheme of the factorization algorithm (Fig. 2). Consider the situation in which $\sqrt{C}$ is an integer. Such a condition imposed on the SP cycle period allows for determining the minimum $x = \sqrt{C}$ and maximum degrees $z = C$ of f_x and f_z factors. For degree y there remains the possibility of choosing one of the alternative solutions $y = x$ or $y = z$. Both of these values y retain C. Consider an example. Let $x = y = 3$ and $z = 9$, that is, $n = 15$ and $C = 9$. Let us choose the SPs as such: $f_x = f_y = 1011$, $f_z = 1010110111$, and thus we obtain $f_{15}^{[3]} = 1010010110101011$. We come to Table 11.

Table 11. The sequence of $\boldsymbol{S}-$residues generated by the $f_{15}^{[3]} = 1010010110101011$

$\boldsymbol{S}_1 = 10;$	$\boldsymbol{S}_6 = 101010101011110;$
$\boldsymbol{S}_2 = 1000;$	$\boldsymbol{S}_7 = 110010101100101;$
$\boldsymbol{S}_3 = 10000000;$	$\boldsymbol{S}_8 = 110001111011000;$
$\boldsymbol{S}_4 = 10010110101011;$	$\boldsymbol{S}_9 = 110110101000111;$
$\boldsymbol{S}_5 = 1101110000101;$	$\boldsymbol{S}_{10} = \mathbf{10}.$

Naturally, if the polynomials f_x and f_y are different, but their degrees are the same, then in the sequence of $\boldsymbol{S}-$residues, the parameter $\boldsymbol{S}k = 1$.

Let's move to the analysis of the algorithm for factorization of degree SP under the condition that the cycle period C of the polynomial is such that

$f_n^{[3]}$. The simplest solution obtains when $C \mid n$. This case empirically established $C = n/2$, $x = y = MC(L)$ and $z = C$, where MC and L are a subset and the number of NTDs of the cycle period C. Let $f_{16}^{[3]} = 10001100001101001$. Let us compose (Table 12) the sequence of $\boldsymbol{S}-$ residues

Table 12. The sequence of $\boldsymbol{S}-$residues generated by the $f_{15}^{[3]} = 1010010110101011$

$\boldsymbol{S}_1 = 10;$	$\boldsymbol{S}_5 = 11010111100011;$
$\boldsymbol{S}_2 = 1000;$	$\boldsymbol{S}_6 = 1101001110000000;$
$\boldsymbol{S}_3 = 10^{[7]};$	$\boldsymbol{S}_7 = 111110000001001;$
$\boldsymbol{S}_4 = 10^{[15]};$	$\boldsymbol{S}_8 = 1010000010100000$
	$\boldsymbol{S}_9 = \mathbf{10}.$

Since $n = 16$, $C = 8$ and $MC = \{2, 4\}$, $L = 2$, then $x = y = MC(2) = 4$, and $z = C = 8$. Because $\boldsymbol{S}k = 10$, the polynomials f_x and f_y are the same. The polynomials $f_x = f_y$ of the fourth-degree 10011 and $f_z -$ the IP of the eighth degree 100011101 chose.

Suppose that the polynomials f_x and f_y are different, such as $f_x = 10011$ and $f_y = 11001$, which form $f_{16}^{[3]} = 11010101000111111$. Then, subtraction $\boldsymbol{S}_8 = \boldsymbol{S}k = 1$ becomes the oldest in the sequence (see Table 13).

Table 13. The sequence of $\boldsymbol{S}-$residues generated by the $f_{15}^{[3]} = 1010010110101011$

$\boldsymbol{S}_1 = 10;$	$\boldsymbol{S}_5 = 100100100100110;$
$\boldsymbol{S}_2 = 1000;$	$\boldsymbol{S}_6 = 1011010110100100;$
$\boldsymbol{S}_3 = 10^{[7]};$	$\boldsymbol{S}_7 = 111110000001001;$
$\boldsymbol{S}_4 = 10^{[15]};$	$\boldsymbol{S}_8 = \mathbf{1}.$

We complete our analysis of algorithms for factorization of degrees of sphenic polynomials. The structural logic diagram, which showed in Fig. 2, fully contains all the necessary information explaining the factorization technology.

A natural direction for further research is to generalize the results to solve the problem of factorization of degrees of $k-$almost simple polynomials whose order k exceeds 3.

4 Conclusions

The study's main result is the development of a practical algorithm of factorization $n-$degrees sphenic polynomials $f_n^{[3]}$ formed by the product of three IPs over a Galois field of arbitrary characteristic. Of the three equations functionally dependent on the unknown degrees of the sphenic polynomials, they can represent only two equations explicitly. One of them is trivial and boils down to the sum of the unknown degrees of the polynomial co-dominants equals the a priori given degree of that polynomial.

The second equation relies on a calculated parameter, called the cycle period C of the sphenic polynomial, equal to the lowest common multiple of the degrees of the factors $f_n^{[3]}$. The incompatibility system of two equations for the three unknowns has overcome the fact that the calculated degrees of the denominators of the sphenic polynomials either coincide with the non-trivial divisors of C or are functionally related to them.

They have reviewed different variants of the solution to the problem of factorizing degrees of sphenic polynomials depending on the ratios of parameters n and C. The volume of calculations reduces by switching from the linear scale to determine the polynomial's $f_n^{[3]}$ period cycle C to the logarithmic scale. The proposed factorization algorithm is invariant to the characteristic of the field generated by the multipliers of the sphenic polynomial.

References:

[1] Sphenic number. Wikipedia [online], Available at: https://dic.academic.ru/dic. nsf/ruwiki/1644009

[2] Sphenic number. Wikipedia [online], Available at: https://wikisko.ru/wiki/ Sphenic_number

[3] Shparinsky I.E. *On Some Questions in the Theory of Finite Fields*, UMN, 46:1(277) (1991). — C. 165-200. Wikipedia [online], Available at: https://www.mathnet.ru/links/c42de5a12c7ae9608284aece3963a1fa/rm4570.pdf

[4] Gerald Tenenbaum. *Introduction to Analytic and Probabilistic Number Theory*. Cambridge University Press, (2004). ISBN 978-0-521-41261-2.

[5] Semi-prime number. Wikipedia [online], Available at: https://wiki5.ru/wiki/ Semiprime

[6] Anatoly Beletsky. *Factorization of the Degree of Semisimple Polynomials of one Variable over the Galois Fields of Arbitrary Characteristics.* WSEAS Transactions on Mathematics. Vol. 21, 2022, Art. #23, p.p. 160-172. DOI: 10.37394/23206.2022.21.23

[7] Ishmukhametov Sh.T. *Methods of factorization of natural numbers*. - Kazan: Kazan University. (2001). – 190 p.

[8] Bach E., Shallit J. *Factoring with cyclotomic polynomials.* – Math. Comp. (1989). v.52(185), p. 201–219.

[9] Schneier B., *Applied cryptography, Second Edition: Protocols, Algorithms, and Source Code in* C+. John Wiley & Sons, New York (1996).

[10] Chervyakov N.I., Kolyada A.A., Lyakhov P.A. *Modular arithmetic and its applications in Infocommunication technologies*. – M.: Fizmatlit, (2017). – 400 p.

[11] Henri Cohen. *A course in computational algebraic number theory*. Berlin, Springer, (1996). – 545 p.

[12] Lidl R., Niederreiter H. *Finite Fields*. Cambridge University Press (1996).

[13] Beletsky A. *An Effective Algorithm for the Synthesis of Irreducible Polynomials over a Galois Fields of Arbitrary Characteristics*. WSEAS Transactions on Mathematics, Vol. 20, (2021), Art. #54, pp. 508-519.

[14] Round number. Wikipedia [online], Available at: https://dic.academic.ru/dic.nsf/ruwiki/180635