Factorization of the Degree of Semisimple Polynomials Over the Galois Fields of Arbitrary Characteristics

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

Abstract: To semisimple polynomials over a Galois field of arbitrary characteristics we mean polynomials formed by the product of two coprime irreducible polynomials with a priori unknown degrees. The main task of this study is to develop an efficient algorithm for factorizing the degree of semisimple polynomials. The efficient factorization algorithms are those that provide a minimum of computational complexity. The proposed algorithm is reduced to solving a system of two equations for the unknown degrees of the factors of a semisimple polynomial. The right-hand sides of the system of equations are as follows: one of them is the degree n of a semisimple polynomial, known a priori, and the second, the cycle period C of the polynomial, is calculated using the so-called fiducial grid. At each rung of the ladder, the simplest recurrent modular computations are carried out, after which the cycle period C of the semisimple polynomial is determined, which is equal to the least common multiple of the degrees of the factors of the polynomial. Reducing the amount of calculations is achieved by switching from a linear scale when determining the cycle period C to a logarithmic one. The proposed factorization algorithms are invariant to the characteristic of the field generated by irreducible polynomials. Various options for the relationship between the parameters n and C are considered.

Key-Words: irreducible polynomials, semisimple polynomials, fiducial grids, modulo comparability.

Received: May 14, 2021. Revised: January 16, 2022. Accepted: February 22, 2022. Published: March 26, 2022

1 Introduction

One of the most important questions related to polynomials $f_n(x)$ of degree n in one variable x with coefficients over a finite Galois field $GF(p)$ is the question of the type of expansion (factorization) of the polynomial $f_n(x)$.

Definition 1. By the *type of decomposition* of a polynomial $f_n(x)$, we will mean [1] the number K and degrees n_I of *irreducible polynomials* $f_{n_1}, f_{n_2},\ldots, f_{n_k}$ (possibly repeating), the product of which forms a given polynomial f_n, $n=\sum_{i=1}^{k} n_i$.

For the sake of completeness, we recall some facts and definitions related to irreducible polynomials (IP).

A. Irreducible polynomials can be represented in two forms. The first of these is the so-called *polynomial form*, which we will call the *algebraic form*:

$$f_n(x)=\sum_{k=0}^{n}\alpha_k x^k=\alpha_n x^n+\alpha_{n-1}x^{n-1}+\ldots$$
$$\ldots+\alpha_k x^k+\ldots+\alpha_1 x+\alpha_0 \qquad (1)$$

and the second is the *vector form*, which is a set of coefficients α_k of the polynomial, including zero coefficients of the absent monomials of series (1):

$$f_n=\alpha_n\alpha_{n-1}\ldots\alpha_k\ldots\alpha_1\alpha_0. \qquad (2)$$

Expressions (1) and (2) are *natural forms* of writing IP, widely used, for example, in *positional*

number systems [2], in which the most significant digits are located on the left side of the number.

B. Polynomials are characterized by some numeric parameters. One of these is the *degree of the polynomial*, which is equal to the maximum degree of the monomial included in the polynomial with a nonzero coefficient and is denoted $\deg(f(x))$ — for an algebraic and $\deg(f)$ — for a vector form. The second most important parameter of the IP is its *order*, also called the *period* or *exponent* — this is the smallest natural number m at which $f(x)$ it turns out to be a divisor of a binomial $x^m - 1$, that is displayed as follows:

$$f_n(x) \mid x^m - 1. \qquad (3)$$

The order of the polynomial is denoted as $\mathrm{ord}(f_n(x))$ or $\mathrm{ord}(f_n)$ for the algebraic and vector forms, respectively. Where it seems more convenient, along with $\mathrm{ord}(f_n)$ we will also use the notation L_n.

C. Finally, a distinction is made between *primitive polynomials* (PrP) and polynomials that are not primitive. For convenience, the latter will be called *simple irreducible polynomials* (SIP). Primitive polynomials are irreducible polynomials with the maximum order $L_{n,\max}$, which is determined by the relation

$$L_{n,\max} = p^n - 1, \qquad (4)$$

where n — is the degree of the polynomial f_n, and p — is the characteristic of the extended Galois field generated by the IP f_n.

Along with *semiprime*, that is, numbers formed by the product of two primes [3], algebra [4] also considers *semisimple polynomials* (SiM-polynomials).

Definition 2. A polynomial $f_n^{[2]}(x)$ over $GF(p)$ is called semisimple if, for any of its decomposition into a product of irreducible polynomials, the factors $f_{n_1}(x)$ and $f_{n_2}(x)$ are coprime

The superscript 2 in square brackets just indicates that a SiM-polynomial $f_n^{[2]}(x)$ is formed by the product of two relatively simple irreducible polynomials.

The main task of this article is to develop efficient algorithms for the expansion of the degree of SSP $f_n^{[2]}(x)$ in one variable over Galois fields $GF(p)$ of arbitrary characteristics p. Effective will include algorithms for factorizing the degree of polynomials $f_n^{[2]}(x)$ that provide a minimum of computational complexity.

The formulated research problem is a special case of a more general problem of factorization of polynomials, which is reduced to the representation of a given polynomial in the form of a product of polynomials of lower degrees. To date, a large number of papers have been published devoted to the factorization of composite polynomials [5 – 9]. At the same time, insufficient attention has been paid to the assessment of quantitative characteristics such as the expansion of polynomials. We can only cite the survey article [1] as an example, in which it is noted that there is an algorithm of polynomial complexity to answer the question about the type of decomposition of polynomials. At the same time, no clarifications regarding the essence of this algorithm are given in the cited work. This circumstance turned out to be the motive that predetermined the direction of this research.

The problem statement can be explained as follows. Suppose that a SiM-polynomial $f_n^{[2]}(x)$ of degree n is given over the field $GF(p)$, formed by the product of two coprime Ips $f_{n_1}(x)$ and $f_{n_2}(x)$ with a priori unknown degrees n_1 and n_2 such that

$$f_n^{[2]} = f_{n_1} \overset{p}{\otimes} f_{n_2}, \quad n_1 + n_2 = n. \qquad (5)$$

Thus, the problem to be solved is reduced to determining the degrees n_1 and n_2 IP, which together form a polynomial $f_n^{[2]}$. The mathematical basis of this research was formed by the results presented in the article [10].

There are various areas of fundamental and applied research, for which the problem of factorization of degrees of SiM-polynomials, considered in this article, plays an important role. Let us point out, for example, such areas as

cryptography [11], the algebraic theory of modular computing [12, 13], intelligent computing [14, 15], artificial intelligence [16, 17], etc.

2 Axiomatic Foundations of Factorization of the Degree of DSemisimple Polynomials

Let us present simple, often obvious (or well-known) statements, formulated in the form of axioms, which, as we will see below, simplify the solution of the problem of factorization of semisimple polynomials. Such axioms will be denoted by $\boldsymbol{A}$k, where is $k-$the number of the axiom.

Axiom $\boldsymbol{A}$1. Arbitrary irreducible polynomials over a field (both simple and primitive) support comparison

$$1(0)^{[p^n-1]} \equiv 1 \,(\mathrm{mod}\, f_n), \quad n \geq 2, \tag{6}$$

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

The axiom $\boldsymbol{A}$1 is a consequence of Lemma 2.3 from [6], according to which the equality $\alpha^{p^n-1}(\mathrm{mod}\, f_n) = 1$ holds for each nonzero element $\alpha > 1$ of the field $GF(p^n)$ generated by the IP f_n.

$$Res(1(0)^{[p^n-1]})_{f_n} = 1, \quad n \geq 2, \tag{7}$$

where $Res(a)_b -$ is the residue of the number a by modulo b.

Computational operations of algorithms for factorization of semisimple polynomials (see Section 3) inherit some features of operations from relation (7). The main problem that manifests itself in the implementation of scheme (7) is associated with the large number of calculations required to confirm the comparison. Indeed, the number of successive calculation steps at the stage of the formation of the multiplicative group $GF^*(p^n)$, as well as the number of zero bits of the component $(0)^{[p^n-1]}$ on the left-hand side of equality (7), obeys the law of the *exponential function* of the degree of the polynomial in base, that is, it grows faster than any *polynomial function*. To overcome the "nightmare of large numbers", which arises as soon as the degree exceeds several tens, let us pass in (7) from a *linear* to a *logarithmic* "time scale", the explanations for which are given below.

Definition 3. A sequence of natural numbers $k = 0, 1, ..., p^n - 1$ that are exponents of a generating element θ of a multiplicative group of maximum order (MGMO)

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

will be called the "linear scale" of the group.

It is quite obvious that the number of equidistantly spaced points $0, 1, ..., p^n - 1$ on a linear scale, for a degree n, which, for example, in cryptographic applications is often several thousand, can reach nightmarishly large values. To overcome such a nightmare, we will perform the transition from a linear to a logarithmic scale, at each equidistantly spaced point of which $r = 1, 2, ..., n$ the corresponding component of the MGMO is calculated.

Definition 4. A sequence of natural numbers $r = 1, 2, ..., n$, which are indicators of the degree of characteristics p of a group $GF^*(p^n)$ in an element $t_{r,p} = p^r - 1$, will be called the *logarithmic scale* of the group.

Let us introduce (Table 1) for $p = 2$ auxiliary numerical parameters r and $t_{r,2}$. The subscript 2 corresponds to characteristic p of the field $GF(p)$.

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

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).

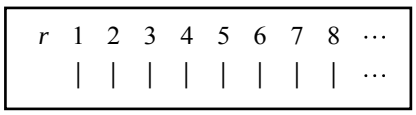

Fig. 1. Fiducial grid

Table 1 the following designations are adopted: $r-$ 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 are filled with zeros, i.e.

$$CV_r = \underset{t_{r,2}}{100...0}. \qquad (8)$$

The marks $t_{r,2}$, being evenly spaced along with the index r on a certain axis, just form the aforementioned "logarithmic time scale". The parameter $t_{r,2}$ is nothing more than the order (length) of the zero vector of the polynomial, the number of zero digits of which is 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 $1^{[n]} = \underbrace{11...11}_{n \text{ бит}}$. 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 easily established by analyzing the data in the bottom line of Table 1. Namely

$$t_{r,2} = 2 \cdot t_{r-1,2} + 1,\ t_0 = 0,\ r = \overline{1,n}. \qquad (9)$$

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 (9) form the fundamental basis of the proposed algorithm for factorizing semisimple polynomials, which is 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 a field $GF(2)$)

$$\boldsymbol{S}_r = Res(\boldsymbol{S}_{r-1}^2 0)_{f_n},\ \boldsymbol{S}_0 = 1,\ r = \overline{1,n}. \qquad (10)$$

When the index r reaches the last rung of the fiducial ladder n, if it turns out that $\boldsymbol{S}_n = 1$, then this will mean, by $A1$, the fulfillment of 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.

We introduce an additional numerical characteristic of polynomials f_n, which we call the cycle order generated by the polynomial f_n. We will call this characteristic the "polynomial cycle period", sometimes omitting the word polynomial, and denoting it $\mathrm{Cord}(f_n)$.

Definition 5. The cycle period of an arbitrary polynomial f_n is the number of non-repeating residues $\boldsymbol{S}_r$ generated by the polynomial f_n on the steps of the fiducial grid.

Let us explain the concept of "cycle period" by numerical examples, choosing as the first tested polynomial binary PrP of the sixth degree $f_6^{(1)} = 1000011$, and the second — SIP $f_6^{(2)} = 1001001$. After performing calculations by formula (10), we obtain

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

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

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

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

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

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

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

r	1	2	3	4	5	6	7	…
t_r	1	8	26	80	242	728	2186	…

Let's equip (to disambiguate) the character $\boldsymbol{S}_r$ with an additional subscript p. From a comparison of the data in Table 1 and 4, we arrive at such generalized relations for the degree $t_{r,p}$ and residue $\boldsymbol{S}_{r,p}$ of the coordinate vector CV_r

$$t_{r,p}=p\cdot t_{r-1,p}+(p-1),\ t_{0,p}=0,\ r=\overline{1,n};$$

$$\boldsymbol{S}_{r,p}=Res(\boldsymbol{S}^{\,p}_{r-1,p}\underbrace{0...0}_{p-1})_{f_n},\ \boldsymbol{S}_{0,p}=1,\ r=\overline{1,n}. \quad (11)$$

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 deductions, calculated by the formula (11), is presented in Table 5

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

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

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

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

Axiom $\boldsymbol{A}2$. The cycle period Cord of both simple and primitive irreducible polynomials f_n is invariant to the characteristic p of a simple Galois field $GF(p)$ to which the IP coefficients α_k belong, and coincides with the degree of the polynomial, that is $\mathrm{Cord}(f_n)=n$.

The axiom $\boldsymbol{A}2$ makes it possible, without loss of generality, in the subsequent numerical examples to be limited to considering only polynomials over $GF(2)$.

3 General Solution to the Problem of Factorization of the Degree of Semisimple Polynomials

Let us introduce $SP_n(p)$ the notation for the subset of polynomials $f_n^{[2]}$ over a field $GF(p)$ that belongs to the set of SiM-polynomials. Recall that the main problem considered in this work is to determine, for a given value $f_n^{[2]}\in SP_n(p)$, the unknown values of the degrees $x=n_1$ and $y=n_2$ IP f_{n_1} and f_{n_2} satisfying equalities (5). To solve the problem of factorizing polynomials $f_n^{[2]}$, it is necessary to compose a system of two equations with two unknowns x and y.

The first of these equations is contained in (5) and is written as

$$x+y=n. \quad (12)$$

The second equation can be constructed based on Theorem 3.11, [6], according to which (as a special case for a finite field of characteristic p) if $f_n^{[k]}=\bigotimes_{i=1}^{k} f_{n_i}$, then

$$\mathrm{ord}(f_n^{[k]})=\mathrm{LCM}(\prod_{i=1}^{k}\mathrm{ord}(f_{n_i})). \quad (13)$$

In (13), the designations are used that are somewhat different from the designations adopted in the original but are equivalent to them. For SiM-polynomials we obtain

$$\mathrm{ord}(f_n^{[2]})=\mathrm{LCM}(\mathrm{ord}(f_{n_1}),\mathrm{ord}(f_{n_2})). \quad (14)$$

The order of the cycle Cord of the polynomial $f_n^{[2]}$ is determined by the same relation (14), which determines the order of the polynomial, i.e.

$$\text{Cord}(f_n^{[2]}) = \text{LCM}(\text{Cord}(f_{n_1}), \text{Cord}(f_{n_2})) = \\ = \text{LCM}(n_1, n_2). \quad (15)$$

Changing places of the components that close equality (15) and using the substitutions $x = n_1$ and $y = n_2$ introduced above, we arrive at the missing equation of the second-order system

$$\text{LCM}(x, y) = C, \quad (16)$$

in which for brevity it is indicated $C = \text{Cord}(f_n^{[2]})$.

Expressions (12) and (16) together form the system of equations

$$\begin{cases} x + y = n \\ \text{LCM}(x, y) = C \end{cases}, \quad (17)$$

using which the problem of factorization of the degree of SiM-polynomials is uniquely solved.

Depending on the relationship between the degree n and the cycle period C of the polynomials $f_n^{[2]}$ (see Table 6), there are five alternative options (options) for solving the system of equations (17). In the right column of the table. 6 explains the nature of the relationship between degrees n_1 and n_2 factors $f_n^{[2]}$. Option 5* is a special one, the characteristics of which will be given at the end of this section of the work.

Table 6. System solution options equations (17) for semisimple polynomials

Variant number	Ratio between n and C	Consequence
1	$C > n$, $\text{GCD}(C, n) = 1$	$n_1 \neq n_2$
2	$C > n$, $\text{GCD}(C, n) > 1$	$n_1 \nmid n_2$
3	$n > C > n/2$	$n_1 \mid n_2$
4	$C = n/2$	$n_1 = n_2$
5*	$C \mid n$	$n_k = C$

Where it seems convenient, we will supplement the subscript of the set $SP_n(p)$ with a parameter that determines ν which of the options $\nu = \overline{1,5}$ the polynomial $f_n^{[2]}$ belongs to.

Option 1 assumes that the cycle period of the polynomial $f_n^{[2]} \in SP_{n,1}(p)$ exceeds its degree, that is $C > n$, moreover $\text{GCD}(C, n) = 1$. The latter means that the degrees n_1 and n_2 factors $f_n^{[2]}$ — are different coprime numbers and.

According to the conditions of option 1: $\text{LCM}(x, y) = x \cdot y$, and system (17) takes the form:

$$\begin{cases} x + y = n \\ x \cdot y = C \end{cases}, \quad (18)$$

which is reduced to the quadratic equation

$$x^2 - n \cdot x + C = 0. \quad (19)$$

The classical solution (19) consists in determining the unknowns

$$x_1 = \frac{n + \sqrt{D}}{2}; \quad x_2 = \frac{n - \sqrt{D}}{2}, \quad (20)$$

where the discriminant

$$D = n^2 - 4C. \quad (21)$$

The roots x_1 and x_2 equations (19) presented in (20) are precisely the required powers n_1 and n_2 of factors of the SiM-polynomial $f_n^{[2]}$. The indicator of the relative simplicity of the degrees of the factors of the polynomial $f_n^{[2]}$ is the discriminant (21) of equation (19). Let us show that the following holds.

Statement 1. If the degrees n_1 and n_2 factors of the polynomial are coprime, moreover $n_1 \neq n_2$ and $n_1 > n_2$, then the square root of the discriminant D of equation (19) is a natural number N such that $N = (n_1 - n_2) \geq 1$.

Indeed, setting in (18) $x = n_1$ and $y = n_2$, from equality (21) it follows that

$$D=(n_1+n_2)^2-4n_1n_2=(n_1-n_2)^2\in N^2. \quad (22)$$

Thus, firstly, the provisions of Statement 1 are confirmed and, secondly, substituting the value of the discriminant D calculated by the formula (21) into (20), we arrive at the desired values of the degrees n_1 and n_2 factors of the polynomial $f_n^{[2]}\in SP_{n,1}(p)$.

Let's take an example. Let us choose a SiM-polynomial $f_8^{[2]}=101000111$ formed by the modular product of PrP of the fifth $f_5=100101$ and third $f_3=1011$ degree. The polynomial $f_7^{[2]}$ forms the residues on the ladder steps, shown in Table 7.

Table 7. The sequence of $\boldsymbol{S}-$residues generated by $f_7^{[2]}$

$\boldsymbol{S}_1=10;$	$\boldsymbol{S}_8=10100101;$
$\boldsymbol{S}_2=1000;$	$\boldsymbol{S}_9=10001011;$
$\boldsymbol{S}_3=10000000;$	$\boldsymbol{S}_{10}=10010101;$
$\boldsymbol{S}_4=11111;$	$\boldsymbol{S}_{11}=10110011;$
$\boldsymbol{S}_5=100100;$	$\boldsymbol{S}_{12}=101101;$
$\boldsymbol{S}_6=10010110;$	$\boldsymbol{S}_{13}=10100;$
$\boldsymbol{S}_7=10111001;$	$\boldsymbol{S}_{14}=1010110;$
	$\boldsymbol{S}_{15}=\boldsymbol{1}.$

We pass to factorization of the degree of SiM-polynomials $f_n^{[2]}$, which belong to the subset $SP_{n,2}(p)$.

Thus, we have: $n=8$, $C=15$, and, according to (21), $D=4$ that is $N=2$. And, as a result, from (20) we get: $n_1=5$ and $n_2=3$, which coincides with the initial data, which we assumed to be unknown for the polynomial $f_7^{[2]}$ a priori.

We pass to factorization of the degree of SiM-polynomials $f_n^{[2]}$, which belong to the subset $SP_{n,2}(p)$.

Option 2 assumes, firstly, that (as in option 1) the cycle period C of the polynomial exceeds its degree n, that is $C>n$, and, secondly, $\mathrm{GCD}(C,n)>1$. The last condition means that the degrees n_1, n_2 factors $f_n^{[2]}$ (assuming $n_1<n_2$) are not coprime numbers and, moreover, $n_1\nmid n_2$.

Statement 2. Semisimple polynomials $f_n^{[2]}$ belong to a subset $SP_{n,2}(p)$ if and only if the degrees n_1 and n_2 of factors $f_n^{[2]}$ are representable in the form of generalized expansions into natural factors

$$n_1=\alpha\cdot\beta;\ n_2=\alpha\cdot\gamma;\ \beta<\gamma, \quad (23)$$

each of which exceeds 1, and besides β, γ — coprime numbers.

Proof. By expressions (17) and (23), the parameters $n=\alpha\cdot(\beta+\gamma)$ and $C=\alpha\cdot\beta\cdot\gamma$, firstly, ensure the inequality $C>n$, since for any natural numbers $\beta>1$, $\gamma>1$ and $\beta\neq\gamma$, the relation $\beta\gamma>(\beta+\gamma)$ is observed. And, secondly, they support condition $\mathrm{GCD}(C,n)>1$, since $\mathrm{GCD}(\alpha\beta\gamma,\alpha(\beta+\gamma))=\alpha>1$. Therefore, all conditions of option 2 are satisfied, which completes the proof of Statement 2.

The algorithm for factorizing the degree of polynomials $f_n^{[2]}\in SP_{n,2}(p)$ is reduced to such transformations. Using substitutions (23) and substitutions $x=n_1$ and $y=n_2$, we reduce the general solution of problem (17) to the form

$$\begin{cases}\alpha(\beta+\gamma)=n\\ \alpha\beta\gamma=C\end{cases}. \quad (24)$$

The form of representation of the degrees n_1 and n_2 in (23) and the system of equations (23) determines the following sequence of calculations. First, we determine the common factor of the known parameters n and C. We have

$$\mathrm{GCD}(n,C)=\alpha. \quad (25)$$

Dividing and in (24) by α, we arrive at a system of equations (similar to the system (18)) with two unknowns β and γ

$$\begin{cases} \beta + \gamma = \bar{n} \\ \beta \cdot \gamma = \bar{C} \end{cases}, \qquad (26)$$

where $\bar{n} = n / \alpha$ and $\bar{C} = C / \alpha$.

The solution of the system of equations (26) repeats the solution of the system (18) and, according to (20), leads to the following results

$$\beta = \frac{\bar{n} + \sqrt{D}}{2}; \quad \gamma = \frac{\bar{n} - \sqrt{D}}{2}, \qquad (27)$$

where

$$D = \bar{n}^2 - 4\bar{C}.$$

The numerical parameters α, β and γ, calculated by formulas (25) – (28), being substituted in (24), lead to the desired solution.

Let us support the theoretical results on the factorization of the degree of semisimple polynomials corresponding to option 2 with a numerical example. We will consider the polynomial $f_n^{[2]} = 10110001001$ formed by the product of two polynomials with a priori unknown degrees. The $\boldsymbol{S}-$sequence of residues generated by the polynomial $f_n^{[2]}$ is shown in Table 8.

Table 8. The sequence
$\boldsymbol{S}-$residues generated by $f_{10}^{[2]}$

$\boldsymbol{S}_1 = 10;$	$\boldsymbol{S}_7 = 1101001000;$
$\boldsymbol{S}_2 = 1000;$	$\boldsymbol{S}_8 = 1101000010;$
$\boldsymbol{S}_3 = 10000000;$	$\boldsymbol{S}_9 = 1111001010;$
$\boldsymbol{S}_4 = 1011110;$	$\boldsymbol{S}_{10} = 1100010100;$
$\boldsymbol{S}_5 = 1111011;$	$\boldsymbol{S}_{11} = 1100110001;$
$\boldsymbol{S}_6 = 1101001011;$	$\boldsymbol{S}_{12} = \boldsymbol{1}.$

Thus, we have two initial parameters: the degree of the polynomial $n = 10$ and the cycle period $C = 12$ of the polynomial. Since the square root of the determinant defined by expression (21) is not a natural number and, in addition $C > n$, this allows us to assume that $f_{10}^{[2]}$ is a SiM-polynomial belonging to option 2. Let us check the stated hypothesis. Using relations (24) – (28), we obtain the values of the degrees $n_1 = 4$ and $n_2 = 6$ factors of the polynomial $f_{10}^{[2]}$. This means that the above assumption is true and the degree of the polynomial $f_{10}^{[2]}$ is uniquely factorized.

Let us turn to the construction of algorithms for factorizing the degree n of polynomials $f_n^{[2]} \in SP_n(p)$ for the case when the cycle period C of the polynomials $f_n^{[2]}$ is less than the degree of these polynomials, that is, when $C < n$. The unknown variables $x = n_1$ and $y = n_2$, as in the previous two versions, are determined based on the solution of the system of equations (17). In this case, two alternative options are possible, which we will call, increasing the numbers, options 3 and 4, respectively.

Option 3 assumes that the cycle period C of the polynomial $f_n^{[2]} \in SP_{n,3}(p)$ is less than the degree n of the polynomial, but more than $n/2$, that is, the following condition is met $n/2 < C < n$.

The factorization of the degree of semisimple polynomials belonging to variant 3 is quite simple. Let us show that the following is true.

Statement 3. The cycle period C of the polynomial $f_n^{[2]} \in SP_{n,3}(p)$ satisfies the inequality $n/2 < C < n$ if and only if factor β of the degree n_1 in (24) turns out to be equal to 1.

Indeed, let us turn to relations (23). Let's put $\beta = 1$. In this case

$$n_1 = \alpha; \quad n_2 = \alpha \cdot \gamma; \qquad (29)$$

and, as a consequence (29), we get

$$n_2 = C; \quad n_1 = n - C. \qquad (30)$$

Expressions (29) and (30) lead directly to the inequality $n/2 < C < n$, which completes the proof of Statement 3.

Note that, according to (29), for polynomials $f_n^{[2]} \in SP_{n,3}(p)$, the lower degrees n_1 of the factors $f_n^{[2]}$ divide the higher degrees n_2, that is $n_1 \mid n_2$, as noted in the right column of Table 6.

Example. Let them $f^{(2)} = f_8 = 100011011$ be considered as a priori unknown, generating $f_{12}^{[2]} = 1001010011101$. Let us calculate (Table 9)

the $\boldsymbol{S}-$residues corresponding to the polynomial $f_{12}^{[2]}$. Since the cycle period $C=8$ is less than the degree $n=12$ of the polynomial being tested $f_{12}^{[2]}$, let us check the hypothesis about the correspondence $f_{12}^{[2]}$ to variant 3 of SiM-polynomials. For this purpose, we define, according to solutions (29), the degrees of the factors: $n_1=4$ and $n_2=8$. Because $n_1 \mid n_2$ this means that the polynomial $f_{12}^{[2]} \in SP_{12,3}(2)$.

Table 9. The sequence of $\boldsymbol{S}-$residues generated by $f_{12}^{[2]}$

$\boldsymbol{S}_1=10;$	$\boldsymbol{S}_5=101000101000;$
$\boldsymbol{S}_2=1000;$	$\boldsymbol{S}_5=100000100000;$
$\boldsymbol{S}_3=10000000;$	$\boldsymbol{S}_7=1010000010;$
$\boldsymbol{S}_4=11001110101;$	$\boldsymbol{S}_8=\boldsymbol{1}.$

Since the cycle period $C=8$ is less than the degree $n=12$ of the polynomial being tested $f_{12}^{[2]}$, let us check the hypothesis about the correspondence $f_{12}^{[2]}$ to variant 3 of SiM-polynomials. To this end, we use formulae (29) to determine the degrees of the factors $n_1=4$ and $n_2=8$. Since $n_1 \mid n_2$, it means that the polynomial $f_{12}^{[2]} \in SP_{12,3}(2)$.

Let's look at it further.

Option 4, which assumes that the cycle period C of the polynomial $f_n^{[2]} \in SP_{n,4}(p)$ is equal $n/2$, that is $C=n/2$, and as a consequence (see Table 6) $n_1=n_2$, and n is an even number.

For this option, it is true

Statement 4. If the cycle period C of a polynomial f_n of an even degree $n=2k$ is equal k, then this means that the polynomial f_n is a product of two different coprime factors of the degree k.

Proof. Taking into account the conditions formulated and the notation adopted in Statement 2, we rewrite the system of equations (18), presenting it in the form

$$\begin{cases} x+y=2k \\ x\cdot y=k^2 \end{cases}. \tag{31}$$

System (31) corresponds to the quadratic equation

$$x^2-2k\cdot x+k^2=0,$$

whose discriminant is equal to zero. Substituting $D=0$ in (20), we get $x_{1,2}=k$. ■

Let us illustrate option 4 with a numerical example. Suppose that the polynomial $f_{12}^{[2]}$ is formed by the modular product of two different IPs (which predetermines their mutual simplicity) of the eighth degree over the field, for which we take $f_8^{(1)}=100011011$ and $f_8^{(2)}=100011101$. Thus, we have $f_{16}^{[2]}=10000011100011111$, the sequence of $\boldsymbol{S}-$residues of which is presented in Table 10.

Table 10. The sequence of $\boldsymbol{S}-$residues generated by $f_{12}^{[2]}$

$\boldsymbol{S}_1=10;$	$\boldsymbol{S}_5=11010111100011;$
$\boldsymbol{S}_2=1000;$	$\boldsymbol{S}_6=1110000110;$
$\boldsymbol{S}_3=10000000;$	$\boldsymbol{S}_7=1011011011101110;$
$\boldsymbol{S}_4=10^{15};$	$\boldsymbol{S}_8=\boldsymbol{1}.$

The considered options for solving the system of equations (15) are reduced to an algorithm, a simplified structural and logical diagram of which is shown in Fig. 2.

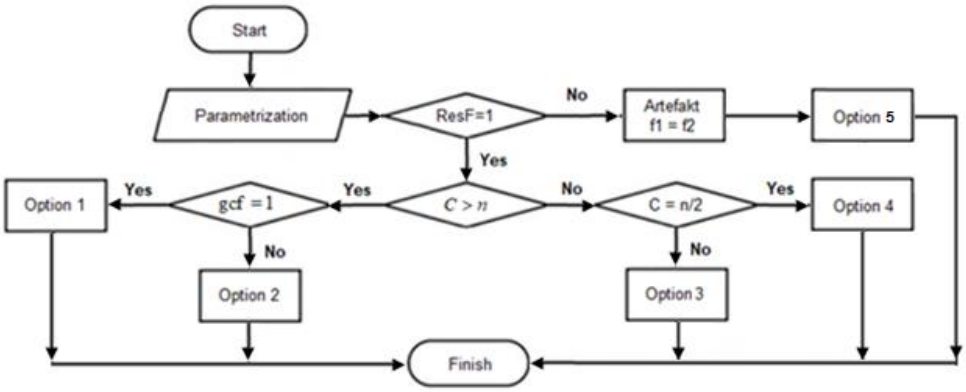

Fig. 2. Block diagram of the computational algorithm

And at the end of the section, let us turn to the analysis of the last version of the relationship between the degree n of the composite polynomial f_n and the cycle period C of the polynomial noted in Table. 6 as option 5*. Let us show the consequences of the case when not only the degrees but also the factors of the polynomial f_n are the same, the number k of which may exceed two. Let us denote $f_n^{\odot} = (f_{n/k})^k$. Let us choose, for example, an irreducible sixth-degree polynomial $f_6 = 1213423$ over $GF(5)$. Let $k = 3$. We have $f_{18}^{\odot} = 1104344001442323442$, which corresponds to

Table 11. The sequence of $\boldsymbol{S}-$residues generated by $f_{18}^{\odot}$

$\boldsymbol{S}_1 = 10000;$
$\boldsymbol{S}_2 = 321311413243311004;$
$\boldsymbol{S}_3 = 43314440231014043;$
$\boldsymbol{S}_4 = 32143422342430214;$
$\boldsymbol{S}_5 = 201231134140402114;$
$\boldsymbol{S}_6 = 123040101343120034;$
$\boldsymbol{S}_7 = \mathbf{10000.}$

Summarizing the data table. 11, we come to the following conclusion. First, the cycle period C of the polynomials $f_n^{\odot}$, as in option 4, turns out to be equal to the degree of the factors. And secondly, the cycle of $\boldsymbol{S}-$residues generated does not end with one. The fact that the residue $\boldsymbol{S}$ that completes the cycle generated by the polynomial f_n is not terminated by 1 is a clear indication of that $f_n \notin SP_n(p)$.

4 Direction for Further Research

One can point at least to such an obvious direction for further research. Its essence is to expand the number of factors of the so-called hyper-simple polynomials.

Definition 6. By *hypersimple polynomials*, we mean composite polynomials $f_n^{[k]}$ over $GF(p)$ formed by products of at least three coprime irreducible polynomials f_{n_i}, $i = \overline{1,k}$, $k \geq 3$, that is

$$f_n^{[k]} = \overset{k}{\underset{i=1}{\otimes}} f_{n_i}.$$

The above definition of hypersimple polynomials excludes the possibility of two or more identical irreducible polynomials appearing in their composition as factors.

The problems associated with the analysis of hypersimple polynomials will be briefly denoted by the example of the so-called *sphenic polynomials* (Sp-polynomial) $f_n^{[3]}$ containing three coprime IPs as factors, that is

$$f_n^{[3]} = f_{n_1} \overset{p}{\otimes} f_{n_2} \overset{p}{\otimes} f_{n_3}.$$

The solution to the problem of factorizing the degree of sphenic polynomials can be reduced to the sequential execution of such operations. At first, you need to compose a system of three equations for the unknown degrees $x = n_1$, $y = n_2$

and $z = n_3$, and the factors of the polynomial $f_n^{[3]}$. We arrive at the first two of them, generalizing system (17) for three variables

$$\begin{matrix} x + y + z = n \\ \mathrm{LCM}(x, y, z) = C \end{matrix}, \quad (32)$$

and represent the third equation in the form of a functional

$$F(x, y, z) = G.$$

The classical solution of the system of equations (32) is hindered by a seemingly unsolvable uncertainty to the functional $F(\cdot)$. But not everything is as hopeless as it may seem at first sight. Under certain conditions, solutions of the system (32) are achievable even in the case when there is no information about the functional $F(\cdot)$ and its right part G.

The simplest (but far from effective) way to get rid of the third extra unknown in the system of two equations (32) is to sequentially replace one of the variables, for example, with the values of the natural series 1, 2, ... Thus (32) transforms into a system of two equations concerning two unknowns where C is a parameter that is specified later.

$$\begin{matrix} x + y = n - z \\ \mathrm{LCM}(x, y) = C^* \end{matrix}. \quad (33)$$

If the current value $z = t$ does not satisfy the system (33), we pass to the next value $z = t + 1$ of the variable. This procedure of sequential search is interrupted at some $k-$th step, $k < n$, at which the system (33) becomes solvable. An alternative (and more efficient) solution of the system of equations (32) is based on a decomposition of the cycle period C of the Sp-polynomial $f_n^{[3]}$ into simple multipliers. Let us illustrate the alternative way to get rid of the "third extra" in (32) by numerical examples.

Let us turn to the analysis of the partial relations between n and C for the Sp-polynomials $f_n^{[3]}$, which are either similar to, or somewhat broader than, the variants listed in Table 6. Let us keep the numbering of the solution variants for polynomials $f_n^{[3]}$ the same as that chosen in Table 6 for polynomials $f_n^{[2]}$, adding the number 3 to the right. If necessary, we will supply the variant number with an additional alphabetic symbol.

Option 13 assumes that the cycle period C of the Sp-polynomial $f_n^{[3]}$ exceeds its degree n, that is $C > n$, with $\mathrm{GCD}(C, n) = 1$.

Note that, first, the required conditions ($C > n$ and $\mathrm{GCD}(C, n) = 1$) are not reached at any values of n, as in variant 1 of Table 6, but only when n it is a prime number. There are two special cases for variant 13, the first of which we denote as variant 13-A. This case assumes that the group of three unknown degrees x, y and z the quotients of the Sp-polynomial $f_n^{[3]}$ contain a pair of even or odd numbers (let them be y and z) such that $z \mid y$. Note that firstly, a degree n can be simple if x it is only mutually simple with y and z. And secondly, if y and z are even numbers, x it must be an odd number, and vice versa. Thus, the equality of

$$\mathrm{LCM}(x, y, z) = \mathrm{LCM}(x, y) = x \cdot y = C. \quad (34)$$

Taking into account the conditions from relations (33) and (34) we come to the following mathematical model for option 13-A

$$\begin{matrix} x + y = n - z \\ x \cdot y = C \end{matrix}. \quad (35)$$

Let us consider an example. Suppose that $f_n^{[3]}$ it is formed by the product of the polynomials $f_5^{(1)} = 100101$, $f_4^{(2)} = 10011$ and $f_2^{(3)} = 111$. We obtain the Sp-polynomial $f_{11}^{[3]} = 111010111101$, whose sequence of $\boldsymbol{S}-$residues is summarized in Table 12.

Assuming the cycle period C of the Sp-polynomial $f_n^{[3]}$ to be a posteriori calculated (i.e., deriving it from Table 12), we present $C = 20$ it as a decomposition

$$C = 2 \cdot 2 \cdot 5. \quad (36)$$

According to (36) possible values of the parameter can be the numbers 2, 4, or 5. The lowest variable $n_3 = z = 2$ Model (35) is reduced to the system

$$x + y = 9$$
$$x \cdot y = 20,$$

whose solution predetermines the remaining two degrees $n_1 = 5$ and $n_2 = 4$ factors of the polynomial $f_{11}^{[3]}$.

Table 12. The sequence of $\boldsymbol{S}-$residues generated by the polynomial $f_n^{[3]}$

$\boldsymbol{S}_1 = 10;$	$\boldsymbol{S}_{11} = 11111001;$
$\boldsymbol{S}_2 = 1000;$	$\boldsymbol{S}_{12} = 11110011;$
$\boldsymbol{S}_3 = 10000000;$	$\boldsymbol{S}_{13} = 1111011;$
$\boldsymbol{S}_4 = 1101000010;$	$\boldsymbol{S}_{14} = 1110111001;$
$\boldsymbol{S}_5 = 10001011010;$	$\boldsymbol{S}_{15} = 10010100001;$
$\boldsymbol{S}_6 = 10010100010;$	$\boldsymbol{S}_{16} = 10001011001;$
$\boldsymbol{S}_7 = 10001010011;$	$\boldsymbol{S}_{17} = 10010101000;$
$\boldsymbol{S}_8 = 10000100000;$	$\boldsymbol{S}_{18} = 10011011011;$
$\boldsymbol{S}_9 = 11100011001;$	$\boldsymbol{S}_{19} = 11111100010;$
$\boldsymbol{S}_{10} = 11111010;$	$\boldsymbol{S}_{20} = \boldsymbol{1};$

One can also get rid of an extra variable (e.g., z) in the system of equations (32) when the cycle period C of the polynomial $f_n^{[3]}$ is decomposed into the product of three prime numbers, and their sum must be a prime number. This variant (let us call it variant 13-B) corresponds to the mathematical model

$$\begin{aligned} x + y &= n - z \\ x \cdot y &= C / z \end{aligned}. \qquad (37)$$

The numerical prototype of variant 13-B can be, for example, the degrees of $n_1 = 3$, $n_2 = 5$ and $n_3 = 11$, and the factors of $f_{19}^{[3]}$. Variants 13-A and 13-B constitute a complete group in the set of variants of 13 Sp-polynomials. Relying on models (35) and (37), it seems possible to construct mathematical models for all the remaining variants of the system of equations (32) and thereby to solve the problem of factorization of degrees of sphenic polynomials.

5 Conclusions

The main result of the research is the development of an effective algorithm for factorizing the degree of semisimple polynomials formed by the product of two coprime polynomials over a Galois field of arbitrary characteristic. The proposed algorithm is reduced to solving a system of two equations for the unknown degrees of the factors of a semisimple polynomial. The right-hand sides of the equations are the a priori known degree n of a semisimple polynomial and the cycle period C of the polynomial, calculated using the so-called reference ladder. At each rung of the ladder, the simplest recurrent modular computations are carried out, after which the cycle period C of the semisimple polynomial is determined, which is equal to the least common multiple of the degrees of the factors of the polynomial. Various options for solving the system of equations are considered depending on the ratios of the parameters n and C. Reducing the number of calculations is achieved by switching from a linear scale when determining the cycle period C of a semisimple polynomial to a logarithmic one. The proposed factorization algorithms turn out to be invariant to the characteristic of the field generated by irreducible polynomials. Directions for further research are outlined.

References:

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

[2] *Positional number systems*. Wikipedia [online], Available at: https://www.foxford.ru/wiki/inf ormatika/pozitsionnye-sistemy-schisleniya-schisleniya

[3] *A semi-simple number*. Wikipedia [online], Available at: https://ru.wikipedia.org > wiki

[4] *Collection of Problems in Analytical Geometry and Linear Algebra* / Edited by Yu.M. Smirnov. Electronic edition. – M.: ICNMO, 2016. – 391 p. ISBN 978-5-44-39-3003-9

[5] Prasolov V. V. *Polynomials*. – M.: ICNMO, 2001. – 336 c. ISBN 5-900916-73-1

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

[7] Vasilenko O.N. *Theoretical and numerical algorithms in cryptography*. – M.: ICNMO, – 355 p. – ISBN 5-94057-103-4

[8] Fomichev, V. M. *Discrete mathematics and cryptography*. – M.: Dialog-MIFI, (2013). – 397 p. – ISBN 5-86404-185-8

[9] B.L. van der Varden. *Algebra*. – M.: GRFML, (1976).

[10] 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.

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

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

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

[14] Sergienko I.V., Molchanov I.N., Khomich A.N. *Intelligent Technologies of high-performance technologies*. // Cybernetics and system analysis., 2010, № 5. – P. 164-176.

[15] Taranchuk V.B. *Intelligent Computing, Analysis, Visualization of Big Data* – Minsk: BSUIR, 2019. – P. 337-346.

[16] Zaitsev A. *Trends in Artificial Intelligence. Modern methods machine learning*. Wikipedia [online], Available at: https://videonauka.ru/stati/32-vystavkikon ferentsii-seminary/182-tendentsii-v-oblastii skusstvennogo-intellekta-sovremennye-met odymashinnogo-obucheniya

[17] *Artificial Intelligence: Problems and Solutions*. Wikipedia [online], Available at: https:// www.raai.org/library/books/Konf_ II_ problem – 2018/book1_

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)