Ministry of Science and Education of Ukraine
National Aviation University

A. Beletsky
N. Glazunov
D. Navrotskyi

Algebraic foundations of coding theory and cryptography

Textbook

Kiev, 2018

UDK 512.54:512.8
B-24

Recommended for publication by the Department of Electronics National Aviation University of the Ministry of Education and Science of Ukraine (Protocol # 5 of 08.09.2018 city)

Reviewers:

A. Borysenko, Ph.D., Professor
A. Kuznetsov, Ph.D., Professor

A. Beletsky, N. Glazunov, D. Navrotskyi
B-24 Algebraic foundation of coding theory and cryptografy. — Kiev, NAU, 2018. — 160 p.

ISBN

The textbook contains an accessible summary of the theory of numbers and modular arithmetic, irreducible polynomials, the most important algebraic structures, including groups, rings and Galois fields, as well as pseudo-random number generators in classical and generalized Galois and Fibonacci configurations, that constitute the mathematical basis of modern coding theory and cryptography.

The manual is aimed to students of technical universities.

UDK 512.54:512.8
BK

ISBN

© A. Beletsky,
N. Glazunov,
D. Navrotskyi, 2018

CONTENTS

INTRODUCTION

Mathematical objects called *algebraic structures* play the fundamental role in theory and applications of error-correcting coding and cryptographical protection of information.

In a broad sense, under an **algebraic structure** $\mathbb{S}$ we understand any set $\mathfrak{M}$ of elements of any kind, called a *carrier*, on which a certain operations (*signature* Ω), define laws that assign to one or more elements belonging to $\mathfrak{M}$ another element of this set. Briefly algebraic structure may be denoted as $\mathbb{S} = (\mathfrak{M}, \Omega)$.

Typically, algebraic structures are correlated with such objects *groups*, *rings*, and *fields*. In the proposed training tutorial, which is basically an introduction to the algebraic foundations of the theory of error-correcting coding and cryptographic protection of information, we expanded the algebraic structures by adding to them *irreducible polynomials* (Section 2) and *matrices*, *pseudo-random* generators of Galois and Fibonacci sequences (Section 4). Listed algebraic objects characterized by the peculiarity that they are all in the explicit or indirect way involved in the so-called *modulo operations*, which, as a rule, are reduced to the determination of residues (residue) of the results of calculations by a certain modulus. As a modulus usually used non-negative integers (usually - prime), or irreducible polynomials.

The book consists of four chapters. The first section is devoted to a brief presentation of the elements of number theory, minimally sufficient for understanding all the remaining chapters and include: basic concepts and definitions, characteristics of various positional number systems, comparison of integers for the selected modulus, quadratic residues and non-residues, basic modular arithmetic and algebraic operations on modular arrays. The final section is closed by the definition of the Kronecker product of matrices modulo natural number.

Crucial to the understanding of the material contained in the tutorial is the content of the small second section. The section introduces the fundamental concepts of *irreducible* and *primitive polynomials*, represented by *algebraic polynomial* and their *vector forms*. Explained in detail how to perform modular arithmetic of irreducible polynomials, and sets out the engineering algorithms for synthesis of irreducible polynomials of small degrees.

Central in the tutorial is its third section, which on the readily available level explains the basic objects of algebraic structures such as *groups*, *rings* and *finite fields*, called *Galois fields*.

The final fourth section deals with the synthesis of classical and generalized *Galois* and *Fibonacci matrices* and on their basis - the construction of generators of pseudo-random sequences (numbers) in Galois and Fibonacci configurations. We introducing the so-called *spatial matrices*, *Galois fields*, and a number of other original concepts.

Each section concludes with a brief summery outlining the main results and is accompanied by a list of questions for self-examination.

Tutorial "Algebraic basics of coding theory and cryptography" is self-contained. This means that it contains intelligible and detailed exposition, which does not requiring reference to other sources. By the reason, and based on the desire to minimize the reader's distraction by references, a list of additional recommended literature is given at the end of tutorial.

The book is intended for researchers, teachers and students of higher technical educational institutions and serves as a basis for mathematical disciplines such as the theory of error-correcting coding and cryptographic protection of information and a number of others.

1. ELEMENTS OF NUMBER THEORY AND MODULAR ARITHMETIC

This section of the tutorial contains only the most elementary information from *number theory* and matrix algebra, the minimum required, but sufficient for the successful development of the basics related to *the coding theory and cryptography*.

1.1. Basic concepts and definitions

The most important concepts of number theory are the concepts of *natural numbers*, *numbers* and *mathematical symbols*. However, if the mathematical encyclopedia, and not only defines the concept of numbers as *the symbols for the definition of the* ***numbers***, in the same encyclopedia definition of the concept of number is missing.

To *bridge the gap* offered an option of determining the number.

Number – *is an abstract quantitative measure of the set of elements of an arbitrary nature*.

Finally, the **mathematical signs** (*symbols, letters*) – *a notation for writing mathematical concepts (including the concept of number) and calculations*.

In the tutorial, we will deal *exclusively* (unless otherwise specified) with *integer numbers* and with their residues modulo natural numbers n. Integer numbers and residues modulo n form respectively various *sets* (subsets).

The concept of a *set* is one of the basic undefined concepts of mathematics. Under a variety of understanding the *totality* of (set, class, family ...) *some objects united by some criterion*. Therefore, we can speak of the set of all integers, the set of all non-degenerate (0, 1)-matrices $n-$th order, and so on.

The objects that make up the set are called its elements. Sets are usually denoted by capital letters of the alphabet $A, B, \ldots, X, Y, Z$ and their elements - small letters $a, b, \ldots, x, y, z$. If the element x belongs to X, the record $x \in X$; record

$x \notin X$ means that the element x does not belong X. The set which does not contain any elements, called empty and is denoted $\varnothing$.

Elements of the set written in curly braces, inside of which they are listed and separated by commas. For example, the entry $A = \{1, 3, 15\}$ means that the set A consists of three numbers 1, 3 and 15; record $A = \{x : 0 \le x \le 2\}$ means that the set A consists of all valid (unless otherwise specified) numbers satisfying the inequality $0 \le x \le 2$.

In the future under the term **number** we mean the *integer number* and use, as a rule, following the common notation of basic sets of integers:

$\mathbb{N}$ – the set of natural numbers: $\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$;

$\mathbb{Z}$ – the set of integers: $\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$;

$\mathbb{Z}^+$ – set of non-negative integers: $\mathbb{Z}^+ = \{0, 1, 2, \ldots,\}$;

$\mathbb{Z}_n$ – set of residues modulo n: $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.

Natural number *is a number used in a natural way with the score*. The sequence of all natural numbers arranged in ascending order, called natural numbers.

There are two approaches to the definition of natural (natural) numbers – are numbers that arise when:

- **counting** (*enumeration*) of items (first, second, third, ...);
- **designation number** (no objects, one object, the two subjects, ...).

In the first case, a number of positive integers starting with one, the second - From scratch. There is no consensus on the preference of the first or the second approach (that is, we consider vanishing natural number or not?). In the vast majority of sources (as in this manual) have traditionally adopted the first approach, in which zero is not included in the natural series. In the second approach zero is the lowest number of natural numbers, forming, together with the natural numbers, the so-called **advanced natural number**, denoted $\mathbb{N}_0$ or $\mathbb{Z}^+$.

The set $\mathbb{Z}_n$ is a *subset* of the set $\mathbb{Z}^+$ and both sets $\mathbb{Z}_n$ and $\mathbb{Z}^+$ are subsets of the set $\mathbb{Z}$, which are represented by the relations

$$\mathbb{Z} \supset \mathbb{Z}^+ \supset \mathbb{Z}_n.$$

Among the natural numbers is the *smallest element*, which is 1 for the set $\mathbb{N}$, and 0 if the numbers make a number of advanced natural $\mathbb{N}_0$ or $\mathbb{Z}^+$. At the same time, there is no (there is not exists), the *largest element* of the natural numbers, because after an arbitrarily large integer n is an even greater number $n+1$, etc.

Definition 1.1. *We say that a natural number n is divisible by a natural number m, if there is a natural number k that*

$$n = m \cdot k. \tag{1.1}$$

Numbers m in k in (1.1) are called the *divisors of a natural number n*. This relationship can be expressed as

$$n / m = k. \tag{1.2}$$

In (1.2) operand n is called the *dividend, m – divider,* and k — *quotient.* Notation $n \mid m$ means that the integer n divided by m without a residue.

Obviously, any integer other than one, has at least two dividers - unit and itself, as far as $n = 1 \cdot n$. Dividers of natural number n, different from unity and the number n, are called *proper divisors,* and 1 and n *– improper divisors* of a natural number n. Numbers have their own dividers, are called *composite* or *decomposable*, and having only improper dividers – *prime* or *irreducible*. Thus, we have

Definition 1.2. *Natural number p is called prime if it is greater than 1 and has no positive divisors other than 1 and p; anyway – a number that that has exactly two different divisors.*

The first prime numbers are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ... Read Is a prime number 1 - a matter of convention, but it's convenient yet 1 do not apply to the set of prime numbers. Prime numbers are usually denoted by the letter p (From the word *prime*).

Definition 1.3. *A positive integer n is a composite if it is greater than 1 and has at least one positive divisor δ, other than 1 and n.*

We also introduce the following definitions:

Definition 1.4. *Integer $\delta \neq 0$ is called a common divisor of integers $a_1, a_2, \ldots, a_n$, if each of these numbers is divided by δ.*

Definition 1.5. Integer d *is called the greatest common divisor* (GCD) *of integers $a_1, a_2, \ldots, a_n$ if:*

1) d *it is a common divisor of the numbers*;
2) d *is divisible by any common divisor of* $a_1, a_2, \ldots, a_n$.

GCD is usually designated as follows:

$$d = \text{НОД}(a_1, a_2, \ldots, a_n) \text{ or simply } d = (a_1, a_2, \ldots, a_n).$$

Consider, for example, three numbers 12, 18 and 30. We write all the divisors δ_a of these numbers. We have

$$\delta_{12} = 1, 2, 3, 4, 6, 12;$$

$$\delta_{18} = 1, 2, 3, 6, 9, 18;$$

$$\delta_{30} = 1, 2, 3, 5, 6, 10, 15, 30.$$

The intersection of these sets is the set of common divisors

$$\delta_{12} \cap \delta_{18} \cap \delta_{30} = \{1, 2, 3, 6\}.$$

Number 6 is a common divisor of the numbers 12, 18, 30 and divided by all other common divisors of these numbers, i.e. 1, 2 and 3. Consequently, 6 is the GCD of numbers 12, 18 and 30; or otherwise: $6 = (12, 18, 30)$.

Each non-zero integer can be represented as a product of prime numbers, or, equivalently, *any number greater than 1, is prime or decomposes into a product of primes one and only one way*.

Definition 1.6. *Two non-negative integers a and b are called coprime if their only common devisor is one, that is* $(a, b) = 1$.

1.2. Number systems

Under the *number system* is commonly understood as a set of numbers recording techniques through digital characters (digits). *Number* – a term used to describe the amount, while the *digit* is a sign (symbol) to denote numbers. For example, 43 - the number represented by digits 4 and 3.

A variety of number systems, which existed before and which are used in our time, can be divided into *nonpositional* and *positional number systems*.

Nonpositional number systems are characterized by the fact that each character (from the set of marks, adopted in this system to refer to the numbers) always refers to the same number regardless of the location (*position*) occupied by

this sign in a record number. The *Roman system* can serve as an example nonpositional number system.

1.2.1. Positional number systems

In **positional number system** the same sign may represent different numbers depending on the location (position) occupied by this sign in a record number. Examples of such systems may be the most common *decimal* and *binary* number system.

The number of different digits used in a positional number system (PNS) is called its *base* or *radix*. Taking as a base the number of PNS 2, 3, 5, 10, 16, and other natural numbers can be obtained, respectively, binary, ternary, quaternary, decimal, hexadecimal and another numeral systems.

We will call *elementary digits* of any m-ary PNS numbers from 0 (zero) to $m-1$. Consequently, any m-ary number system contains m elementary digits. For example, in a five-ary number system elementary are the digits 0, 1, 2, 3 and 4. The set of m basic numbers $\overline{0,m-1}$ form the *alphabet* m-ary number system, which is usually denoted $\mathbb{Z}_m$ (We will often use the notation Z_m), i.e

$$Z_m = \{0, 1, 2, \ldots, m-1\}.$$

Each position of a number with the assigned sequence number is called the *digit number*. Take the following numbering sequence of digits if the number is n digits, the youngest (right) digit assigned number 0, and the older (left) digit – number $n-1$.

Any integer in positional notation is written as a sequence of elementary digits. With these digits, the number written in the *abbreviated form*. For example, the number 7365 in the decimal system is the sum of:

$$7365 = 7 \cdot 10^3 + 3 \cdot 10^2 + 6 \cdot 10^1 + 5 \cdot 10^0.$$

To the left of the equal sign the number recorded in the abbreviated form, to the right - as a sum of powers of ten (radix m = 10) with appropriate coefficients, which are the numbers from the set of elementary digits (*alphabet*) of the decimal number system.

Comparing the records that are on both sides of the equal sign, we see that, in abbreviated form, the number is represented in the form of coefficients placing before degrees of the radix.

If the general form

$$A_{(m)} = \sum_{i=1}^{n} \alpha_{n-1} m^{n-1}, \qquad (1.3)$$

where $A_{(m)}$ the number A in $m-$ary PNS; $m-$radix; $n-$the number of digits of A ; $\alpha_j \in Z_m -$coefficient standing in the j-th digit, then the abbreviated form of the numbers $A_{(m)}$ will be:

$$A_{(m)} = \alpha_{n-1}\alpha_{n-2} \ldots \alpha_1 \alpha_0 .$$

Consider the examples of the numbers in some commonly used numerical systems.

1.2.2. Binary number system

In the binary number system base $m = 2$, and the elementary digits of the alphabet Z_2 are 0 and 1. This is the minimum number of digits that can be taken in a number system. Any number is written as a combination (sequence) of the digits 0 and 1. The number 2 (radix) in the binary system appears as two digits 10.

In accordance with the representation (1.3) of the number in the binary system can be written as:

$$A_{(2)} = \sum_{i=1}^{n} \alpha_{n-i} 2^{n-i}, \quad a_j = 0 \text{ or } 1 .$$

Using this formula, you can find the decimal value of a given binary number. For example,

$$A_{(2)} = 101011_{(2)} = 1\cdot 2^5 + 0\cdot 2^4 + 1\cdot 2^3 + 0\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0 = 43_{(10)}.$$

1.2.3. Ternary number system

In *ternary number system* the redix $m = 3$. To record all kinds of numbers in this system uses three basic numbers: 0, 1 and 2. The number 3 (redix of the system) also recorded a two-digit number 10. 4 is written as three plus one, i.e number 5 is written as 12 (three plus two). And finally, the number 6 in the ternary notation is written as 20.

If radix m is greater than ten, the Arabic numerals is not enough to write all the elementary alphabet and numbers necessary to introduce additional symbols for the missing numbers. As these characters are used, as a rule, large letters of the alphabet. For example, for recording of all possible numbers in the 16-ary notation, together with ten numerals 0, 1, 2, 3, 4, 5, 6, 7, 8 and 9 is selected additional letters A, B, C, D, E and F, symbolizing the numbers from 10 to 15, respectively. All of the numbers and letters of the alphabet are elementary numeric 16-hexadecimal number system.

Do not confuse the number of 10, equal to the base of the number system, with the number 10 (to indicate that the symbol adopted A) in the radix $m > 10$.

The following Table. 1.1 provides for comparison of the numbers from zero to ten in some positional number systems.

Table 1.1. Representation of numbers in different number systems

Decimal	Binary	Ternary	Seventh	Eighth-digit
0	0	0	0	0
1	1	1	1	1
2	**10**	2	2	2
3	11	**10**	3	3
4	100	11	4	4
5	101	12	5	5
6	110	20	6	6
7	111	21	**10**	7
8	1000	22	11	**10**
9	1001	100	12	11
10	1010	101	13	12

Thus, in any system radix (number m) is written as a combination of 10 digits. These combinations are highlighted in Table. 1.1 in bold.

1.2.4. The relationship of number systems

To convert an integer from one positional system to another it is need to consequently divide it on the base m of the system in which it is translated. This base m is represented as a combination of numbers (in the particular case it may be a single digit) is an elementary alphabet numerals numbering system original number. The division is performed until the *quotient* becomes less than m. The number in the

new system takes the form of division residues, read from right to left starting with last residue to the first.

We explain this rule on specific examples of the translation of the number A at m_1- ary number system to the number B at m_2- ary number system

$$A_{(m_1)} \circ\!\!\rightarrow B_{(m_2)}.$$

There are two options for the conversion algorithm. In a first case, the radix m_1 exceeds m_2, and in the second – less then m_2.

To illustrate the first case of the conversion set $m_1 = 10$, $m_2 = 8$, $A_{(10)} = 135$; that is, the decimal number 135 must be set to the octal number system. Execute a sequence of long division number $135_{(10)}$ on the base $m_2 = 8$.

$$\begin{array}{rl|l} 135 & 8 & \\ \underline{128} & 16 & 8 \\ \textit{residue} \rightarrow 7 & \underline{16} & 2 \leftarrow \textit{last} \\ \textit{residue} \rightarrow & 0 & \textit{quotient} \end{array}$$

Reading residue of the division from right to left, starting with the last quotient, have

$$135_{(10)} = 207_{(8)}$$

Now we perform the inverse transform 207 octal number to a decimal number. We draw attention to the fact that the divisor – a decimal number $m_2 = 10$, octal number system displayed numbers 12, ie, $10_{(10)} = 12_{(8)}$. As a result of successive division octal number 207 on the base $m_2 = 12_{(8)}$ We obtain by performing all operations in octal,

$$\begin{array}{rl|l} 207 & 12 & \\ \underline{202} & 15 & 12 \\ \textit{residue} \rightarrow 5 & \underline{12} & 1 \leftarrow \textit{last} \\ \textit{residue} \rightarrow & 3 & \textit{quotient} \end{array}$$

Reading residues of the division, beginning from the last quotient, from right to left, get $207_{(8)} = 135_{(10)}$, as it should be. By the example we have illustrated a second version of the algorithm that converts numbers from one number system to another.

Assuming that the above algorithm for converting an octal number to a decimal number may cause certain difficulties, we present a more detailed explanation of the last example.

The task of translation $207_{(8)}$ to a decimal number $X_{(10)}$ solved in several stages. In the first phase by the usual rules of arithmetic octal produce division of $207_{(8)}$ on the base $m_2 = 10_{(10)}$, which shows the number 12. We have octal

$$\begin{array}{rl} & 207 \mid 12 \\ \underline{-} & \underline{12} \mid \underline{\quad 1} \\ \textit{residue} \cdots\cdots\rightarrow & 67 \end{array}$$

The process of division is not finished, as an octal number 67 can be divided into octal divider 12. Continuing the division, we get

$$\begin{array}{rl} & 67 \mid 12 \\ \underline{-} & \underline{62} \mid \underline{\quad 5} \\ \textit{residue} \cdots\cdots\rightarrow & 5 \end{array}$$

So, as a result of the first phase of the division we arrive at the interim results contained private $15_{(8)}$ 5 and the residue, i.e.

$$\begin{array}{rl} & 207 \mid 12 \\ \underline{-} & \underline{202} \mid \underline{15} \cdots\cdots \textit{quotient} \\ \textit{residue} \cdots\cdots\rightarrow & 5 \end{array}$$

In the second stage we divide octal 15 per module $m_2 = 12_{(8)}$

$$\begin{array}{rl} & 15 \mid 12 \\ \underline{-} & \underline{12} \mid \underline{\quad 1} \cdots\cdots \textit{quotient} \\ \textit{residue} \cdots\cdots\rightarrow & 3 \end{array}$$

Reading through the residues of the division of numbers $207_{(8)}$ per module $m_2 = 12_{(8)}$, since the *last quotient to* the first residue already come to the well-known result $135_{(10)} = 207_{(8)}$.

1.2.5. Binary-power notations

The most widely used in various fields of science and technology, especially computer devices, received now the number systems, for which the radix of the number system is a natural number. We call such radix of number systems the

binary-power. The numbers in these systems are interrelated by rather simple transformations, which will be illustrated by concrete examples.

Given a binary number

$$A_{(2)} = 101100011.$$

In order to move from the number $A_{(2)}$ to quaternary number $A_{(4)}$ it is sufficient to initially isolate (handy temples) from right to left pair of bits $A_{(2)}$, renumbering them (pairs) sequentially, starting with 0,

$$A_{(2)} = \overset{4}{1}\overset{3}{0}\overset{2}{1}\overset{1}{1}\overset{0}{0}0011.$$

Then, presenting pairs of binary digits by quaternary symbols, we obtain

$$A_{(4)} = 11203.$$

By the same way easy to obtain next numerical values

$$A_{(8)} = 543 \text{ and } A_{(16)} = 163.$$

It is equally easy to make transfers of numbers from one number system to another within an arbitrary binary-power bases.

A generalization of the binary-power radix is $p-$*adic power radix*, when $m = p^n$, where $p-$ prime, a $n \geq 1-$ natural number.

1.3. Representation of integers

In modular (modulo m) arithmetic, as well as in ordinary arithmetic, there are both positive and negative numbers. Further simple examples explain the algorithm for calculating such numbers for a given modulo *m*.

Put integers on a coordinate (numerical) axis, as shown in Fig. 1.1.

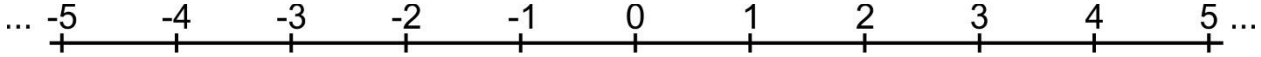

Figure 1.1. A graphical representation of the real axis

We choose, for example the radix of the number system equal $m = 6$. We map (Fig. 1.2) a large circle, in which six small circles, placing the beginning of the axis 0 in the upper circle to coordinate Shaded placed evenly.

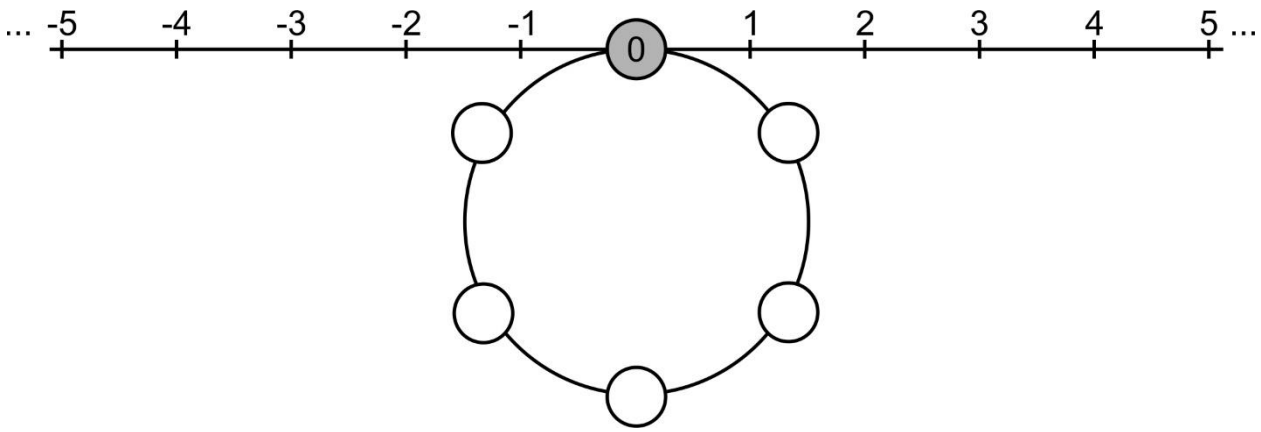

Figure 1.2. Supplement number axis

Conventionally, "wrapping" in the big circle (drum) positive semiaxis clockwise, place the numbers 1 to 5 in small circles as shown in Fig. 1.3.

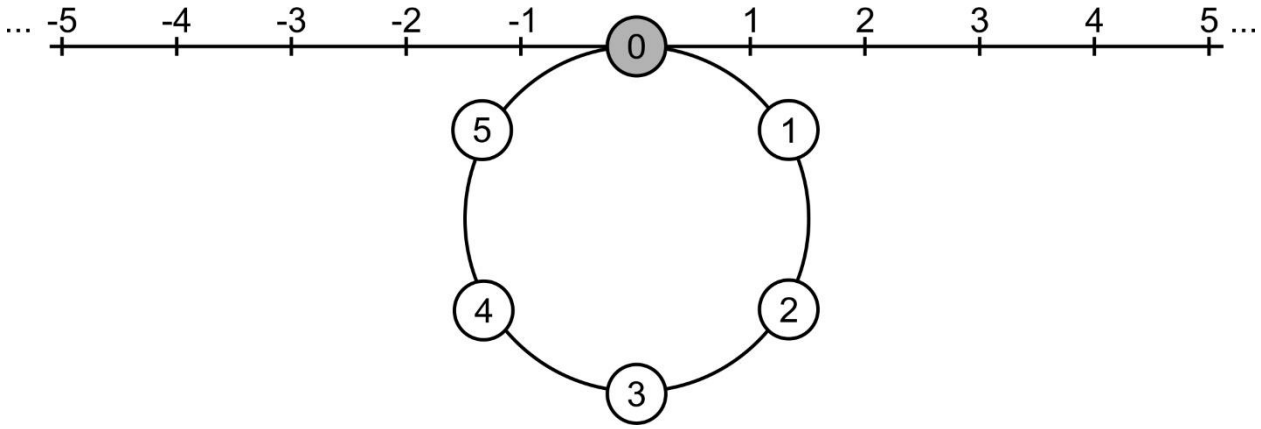

Figure 1.3. The first "wrapping" of the positive semiaxis

We continue the "wrap" the positive semiaxis on the drum. It is obvious in this case that the number 6 will take place in a circle with the number 0; $6_{(6)} = 0$, the number displayed in the circle 7 with the number 1 and so on. Thus we arrive at the figure. 1.4 in which the number of the second scroll are located in a lower half of the dividing line circles.

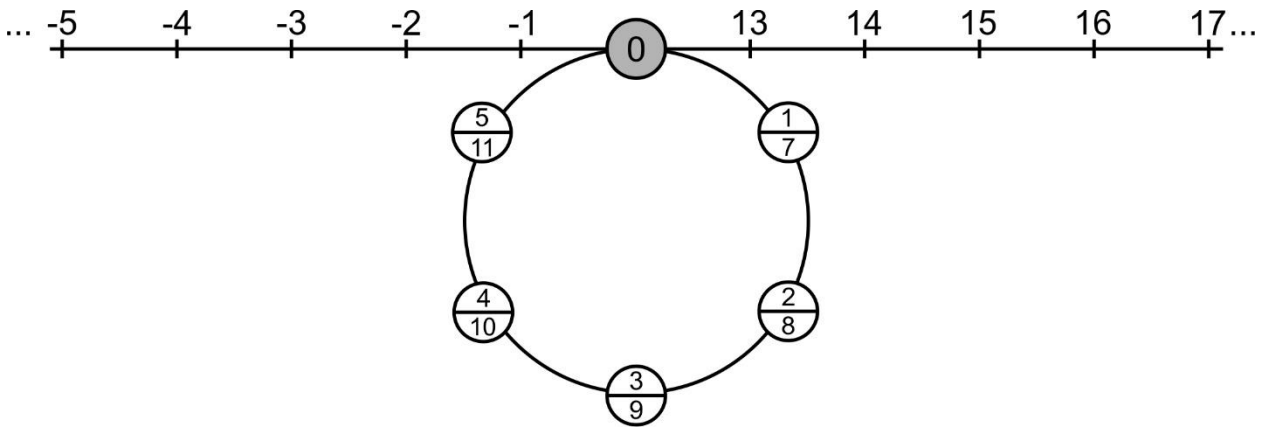

Figure 1.4. The second "wrapping" of the positive semiaxis

According to Fig. 1.3 and 1.4, any non-negative number A modulo m equal to the remainder of division A on m, called *residue*. We introduce for the residue of A modulo m the notation $(A)_m$, then

$$(A)_m = A - \left[A / m\right] \cdot m \qquad (1.4)$$

where $\left[x\right]$ denotes the integer part of the number x.

For instance $(63)_3 = 0,\ (7)_6 = 1$, etc.

Now let us turn to the "negative" coordinate semiaxis. "Wrapping" the semiaxis on the large circle counterclockwise, place the numbers from -1 to -5 in the lower parts of the small circles (Fig. 1.5).

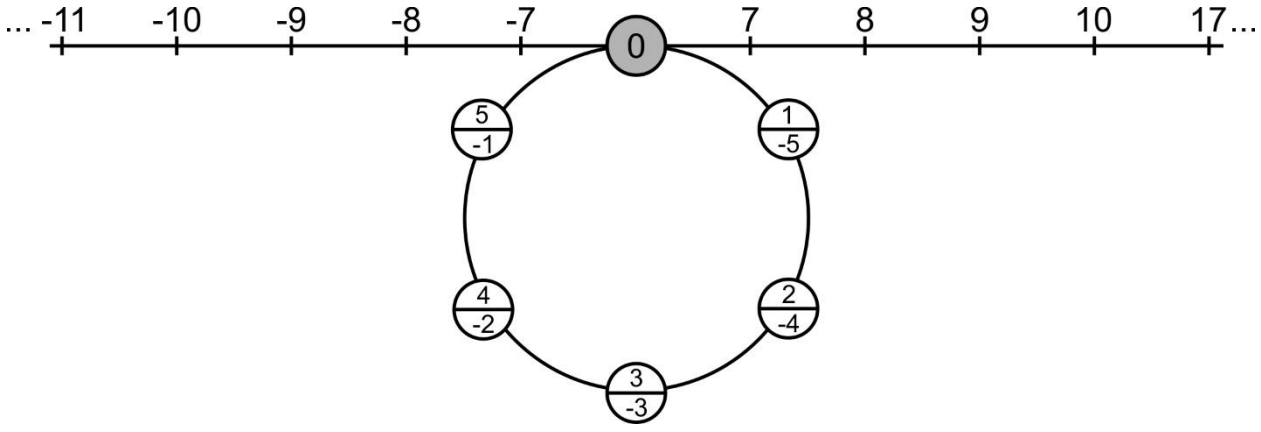

Figure 1.5. "Wrapping" of the negative semiaxis

As it follows from Fig. 1.5, a negative number in the modular arithmetic coincides with one of the positive integers from 0 to $m - 1$ comprising the PNS

modulo m. From the exemplary Fig. 1.5 clearly shows that the deduction of the negative integer is given by

$$(-A)_m = m - (A)_m \tag{1.5}$$

For example,

$$(-47)_8 = 8 - (47)_8 = 8 - 7 = 1.$$

It is important to note that the remainders of negative numbers for some modulo m (residues) are positive numbers.

1.4. Congruences

In some cases two numbers which differ by a multiple of a fixed number m, are equivalent, so that the calculation of these numbers lead to the same result (to the same *remainder* or *residue).*

Rewrite the expression (1.4) as

$$A = \left[A / m\right]m + (A)_m.$$

Number $(A)_m$ called the remainder (*residue*) of the number A modulo m. Usually $(A)_m$ is written in the form: $A \,(\mathrm{mod}\, m)$. If two integers A and B have equal residues modulo m, i.e $(A)_m = (B)_m$, they are called *congruent modulo* m and displayed in the form of the *congruenc*e

$$A \equiv B \,(\mathrm{mod}\, m).$$

The notion of the *congruence* which is introduced by Gauss, expressed in a convenient form that two integers a and b characterized by a multiple of a fixed natural number m. If residues of two integers a and b equal by some module m, then in the case we say that a *congruent* b *modulo* m or, symbolically,

$$a \equiv b \,(\mathrm{mod}\, m). \tag{1.6}$$

This record simply means that $a - b$ divided by m without residue, i.e.

$$(a - b) \,|\, m,$$

or $a = b + mk$, where k is integer.

In fact, let residues r_a and r_b by dividing the a and b on m are r, i.e

$$a = mq_1 + r\,, \tag{1.7}$$

$$b = mq_2 + r\,, \tag{1.8}$$

where $0 \le r < m$ and $q_1, q_2 -$ integers.

Subtracting (1.8) from (1.7) we get $a - b = m \cdot (q_1 - q_2)$, i.e. $(a-b) \mid m$ or $a \equiv b \pmod m$.

Due to the analogy between the congruences (1.6) and equalities (1.7) and (1.8) simplifies the calculations on numbers that differ by a multiple of m. Therefore, the congruence is "equality up to a multiple of m».

Two congruences on the same module m can be added, subtracted or multiplied as well as equalities, that is, if

$$a \equiv \alpha \pmod m \text{ and } b \equiv \beta \pmod m,$$

then

$$a \pm b \equiv (\alpha \pm b) \bmod m,$$
$$ab \equiv \alpha\beta \pmod m.$$

It is easy to confirm both of these congruences by numerical examples.

Congruence can always be multiplied by an integer. So if

$$a \equiv \alpha \pmod m,$$

then

$$ka \equiv k\alpha \pmod m.$$

However, the reduction of a congruence by a factor is not always possible. The reduction by a factor of the congruence becomes valid, if this factor is *coprime to module*, that is,

$$ka \equiv k\alpha \pmod m, \quad \textit{iff} \quad (k, m) = 1. \tag{1.9}$$

Consider numerical examples. Let $a = 17,\ \alpha = 11,\ m = 6$ и $k = 5$. Since the multiplier $k = 5$ prime to module $m = 6$, the congruence of (1.9) is satisfied. If you choose a factor $k = 3$, non-prime to module $m = 6$, it is easy to verify this by congruence (1.9) is violated.

If two numbers a and b under division by the module m form the same residue r, it says something about their that these numbers belong to the same class of *residues* r *modulo* m. Therefore, we can denote the residue classes with the help of these residues. To distinguish classes of residues from residues of residue classes decided to write a dash, for example, $\overline{r}$. *Since when divided by* $0, 1, \ldots, m-1$, the corresponding residue classes denote as $\overline{0}, \overline{1}, \ldots, \overline{m-1}$. The residue class $\overline{0}$ consists of multiples of m, residue class $\overline{1}$ consists of numbers, which under divided by m give residue 1, etc.

The set of residue classes $\overline{0}, \overline{1}, \ldots, \overline{m-1}$ forms a so-called complete *system of residues modulo* m, representatives of which – the numbers 0, 1, ..., m – 1, belong to the set Z_m.

At the conclusion of this section, we note once again that ***the congruence modulo positive integer m*** indicates that the two selected integers when divided by m gives the same remainder (residue).

1.5. Quadratic residues and non-residues

One of the main objects of the elementary number theory are *quadratic residues and non-residues*.

Definition 1.1. If for some number a the congruence

$$x^2 \equiv a \pmod{p},$$

where $p -$ *prime, is solvable, then* a *It called a quadratic residue modulo* p; if this congruence is not solvable, then a *is called a quadratic non-residue modulo* p.

Here is an alternative definition

Definition 1.2. Element a, *belonging to the set of residues modulo a prime* p, It called the quadratic residue, if there is $x \in Z_p$, *such that* $x^2 \equiv a \pmod{p}$. *Element* $a \in Z_p$ *is called the quadratic non-residue, if there is no* $x \in Z_p$ *such that* $x^2 \equiv a \pmod{p}$.

In complete system (multiplicative group) of non-zero residues modulo p, which is denoted as an Z_p^*, half of its elements will be quadratic residues, and the other half - quadratic non-residues.

Example. Let $p=7$, $Z_p^*=\{1,2,3,4,5,6\}$. We have

$$1^2=1\,(\mathrm{mod}\,7),$$

$$2^2=4\,(\mathrm{mod}\,7),$$

$$3^2=2\,(\mathrm{mod}\,7),$$

$$4^2=2\,(\mathrm{mod}\,7),$$

$$5^2=4\,(\mathrm{mod}\,7),$$

$$6^2=1\,(\mathrm{mod}\,7).$$

Numbers 1, 2 and 4 are the quadratic residues and the numbers 3, 5 and 6 - quadratic non-residues. It follows from the above example that the number of quadratic residues coincides with the number of non-residues and for Z_7^* is equal three.

1.6. Modular arithmetic operations

Many arithmetic algorithms are based on calculations by bitwise modulo some integer m, or, as they say, in the *modular* (otherwise called *residues*) bitwise calculations.

A distinctive feature of the bit-wise operations in modular arithmetic is that perform arithmetic operations (as a rule, addition and subtraction) are performed exclusively on one-digit numbers.

This clarification does not mean that we will only deal with one-digit numbers. Multi-digit numbers also will be subject to various transformations. But if, for example, operation performed bitwise modulo m two $n-$ bit numbers $A_{(m)}$ and $B_{(m)}$, then those operation is performed by

$$\overset{m}{\oplus}\begin{array}{cccccccc} a_{n-1} & a_{n-2} & \dots & a_i & \dots & a_1 & a_0 \\ b_{n-1} & b_{n-2} & \dots & b_i & \dots & b_1 & b_0 \end{array},$$

and the result of addition is formed $n-$ digit number

$$C_{(m)}=c_{n-1}\ \ c_{n-2}\ \ \dots\ \ c_i\ \ \dots\ \ c_1\ \ c_0,$$

$i-$digit of which is formed by the rule

$$c_i = a_i \overset{m}{\oplus} b_i,$$

where $\overset{m}{\oplus}$ - addition operator modulo m, a special case of which is the XOR operator - bitwise composition of two *uniform* binary vectors (i.e. vectors of the same length) modulo 2, referred to as the operator $\overset{2}{\oplus}$ or for simplicity $\oplus$.

Table 1.2. gives basic modular operations.

Table 1.2. Operations of modular arithmetic

Notation of the operation	Implemented operation
$\overset{m}{\oplus}$	Addition modulo m
$\overset{m}{\ominus}$	Subtraction modulo m
$\overset{m}{\otimes}$	Multiplication modulo m
$\overset{m}{\oslash}$	Division modulo m

1.6.1. The operation of bitwise modulo addition

A distinctive feature of the *bitwise addition modulo m* is that it is performed for each i- th digit operands excluding transfer units, that is, the transfer unit formed in the usual arithmetic operations of addition is lost. The operation of addition in modular arithmetic is in accordance with *the addition of tables,* called *Cayley tables*. Below is an example of the Cayley table (Table. 1.3) for the bitwise addition of operands x and y modulo 5.

Table 1.3. Operation of addition modulo 5

$\overset{5}{\oplus}$	0	1	2	3	4	$\rightarrow x$
0	0	1	2	3	4	
1	1	2	3	4	0	
2	2	3	4	0	1	
3	3	4	0	1	2	
4	4	0	1	2	3	
$\downarrow y$						

Using Table. 1.3 easy to arrive at the result of bitwise addition of two, for example, six-digit fivefold numbers

$$\begin{array}{r} 304211_{(5)} \\ \overset{5}{\oplus}\ 433042_{(5)} \\ \hline 232203_{(5)} \end{array}.$$

Pay attention to the following property of Table. 1.3. First, the minor diagonal and diagonal parallel auxiliary arranged like numerals. And, secondly, each subsequent row of the table (from top to bottom) of the previous line is formed as a result of its *circular shift* by one bit (step) to the left.

Explain cyclic shifts left and right, also called *circular scrolling*, on the example of a six-digit decimal number $A = 512407$. When the cyclic shift number A one digit to the left Sr. (left) digit moves in the "tail" of the original number A and the number of forms $A^{'} = 124075$. Rotate to the right by one digit of the number of converts A among $A^{''} = 751240$ while the younger, that is the right category A, It moved to its "down".

Explain cyclic shifts left and right, also called *circular scrolling*, on the example of a six-digit decimal number $A = 512407$. When the cyclic shift number A one digit to the left the higher (left) digit moves in the "tail" of the original number A and forming the number $A^{'} = 124075$. Cyclic shift to the right by one digit of the number of converts A to the number $A^{''} = 751240$ while the lower, that is the right digit A, it is moving to its "head".

The above mentioned properties make it much easier to fill the tables of addition for a given module m. In fact, for this purpose enough in the zero line of the table consistently record numbers alphabet Z_m from 0 to $m-1$, and then in each subsequent line numbers preceding line transferred cyclically shifted by one bit to the left.

1.6.2. Operation of bitwise modulo subtraction

The general form of the operation bitwise subtraction modulo m can be represented as

$$\boldsymbol{z} = \boldsymbol{x} \overset{m}{\ominus} \boldsymbol{y},$$

and for $i-$th digit

$$z_i = x_i \overset{m}{\ominus} y_i\,,\ i = \overline{0, n-1}. \tag{1.10}$$

Each digit of $m-$ ary vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ is a digit from the alphabet Z_m and, consequently, does not exceed $m-1$. However, the digit z_i of the difference (1.10) can be negative if $x_i < y_i$. In order to eliminate the negative values of the vector of bits $\boldsymbol{z}$ We use the relation (1.5) for the operand $-y_i$ in formula (1.10). Obtain, provide, $z_i \geq 0$,

$$z_i = (x_i + m - y_i)_m\,.$$

Cayley table for subtracting modulo 5 is represented in Table 1.4. This table allows you to calculate the bitwise difference of two numbers. For example,

$$\begin{array}{rl} \overset{5}{\ominus} & 30421_{(5)} \quad \boldsymbol{x} \\ & 21342_{(5)} \quad \boldsymbol{y} \\ & \overline{14134_{(5)}} \quad \boldsymbol{z}\,. \end{array} \tag{1.11}$$

Table 1.4. Operation of subtraction modulo $m = 5$

$\overset{m}{\ominus}$	0	1	2	3	4	$\rightarrow x$
0	0	1	2	3	4	
1	4	0	1	2	3	
2	3	4	0	1	2	
3	2	3	4	0	1	
4	1	2	3	4	0	
$\downarrow y$						

To check the correctness of the transformation (1.11) is sufficient to perform the bitwise addition of numbers z and y.

$$\begin{array}{rl} \overset{5}{\oplus} & 14134_{(5)} \quad \boldsymbol{z} \\ & 21342_{(5)} \quad \boldsymbol{y} \\ & \overline{30421_{(5)}} \quad . \end{array}$$

The result of the addition restores the number x, which confirms the correctness of calculations (1.11).

Note next properties of subtraction tables (for example, Table 1.4.). At first, the null string of the table. 1.4 coincides with the zero-line table. 1.3, which is natural, because in the general case,

$$(x-0)_m = (x+0)_m .$$

And secondly, all subsequent lines of the Table. 1.4 which are formed from the previous line as a result of cyclic shift of its elements by one digit to the right (in addition tables cyclic shift was carried out to the left).

1.6.3. The operation of modular multiplication

This operation

$$\boldsymbol{z} = \boldsymbol{x} \overset{m}{\otimes} \boldsymbol{y}, \tag{1.12}$$

applies to $m-$ ary codes $\boldsymbol{x}$ and $\boldsymbol{y}$ generally different lengths n_x и n_y and reduced to a set of transformations, the illustrated further numerical examples.

Let $\boldsymbol{x} = 34201_{(5)}$ and $\boldsymbol{y} = 4324_{(5)}$. Operation (12.1) is performed in such a sequence. At first five-digits operands $\boldsymbol{x}$ are $\boldsymbol{y}$ multiplied by the classics "in a column", and then carried out bitwise addition (without transfer) of the results of multiplication modulo $m = 5$. Multiplication $m-$ary operands easier if pre-compiled corresponding Cayley table. For $m = 5$ such a table is shown below.

Table 1.5. The operation of multiplication modulo 5

$\otimes$	0	1	2	3	4	$\rightarrow x$
0	0	0	0	0	0	
1	0	1	2	3	4	
2	0	2	4	1	3	
3	0	3	1	4	2	
4	0	4	3	2	1	
$\downarrow y$						

Here is an example of multiplying two numbers previously selected $\boldsymbol{x} = 34201_{(5)}$ and $\boldsymbol{y} = 4324_{(5)}$. We get

$$
\begin{array}{l}
\quad 34201_{(5)} \\
\overset{5}{\otimes}\ \ 4324_{(5)} \\
\hline
\quad 21304 \\
\overset{5}{\oplus}\ 13402 \\
\quad 42103 \\
\quad 21304 \\
\hline
20114124_{(5)}
\end{array}
$$

According to Table. 1.5 we arrive to the such rule of the formation of matrices of multiplication in an arbitrary $m-$ary radix.

At first the zero row of the matrix is filled with, the elements of which are zeros. Then issued the first line; elements of this line form a sequence of numbers from 0 to $m-1$, those. composed of elements of the alphabet Z_m. Finally, the elements $k-$ multiplying the first row of the matrix are selected from the elements of the first row as a result of its *cyclic decimation* by a factor k, those. It is shown sequentially in each cycle k-th element, starting from zero.

The notion of cyclical thinning can give quite a simple geometric interpretation, referring to their graphic images. Select (Fig. 1.6), for example, the radix $m = 12$.

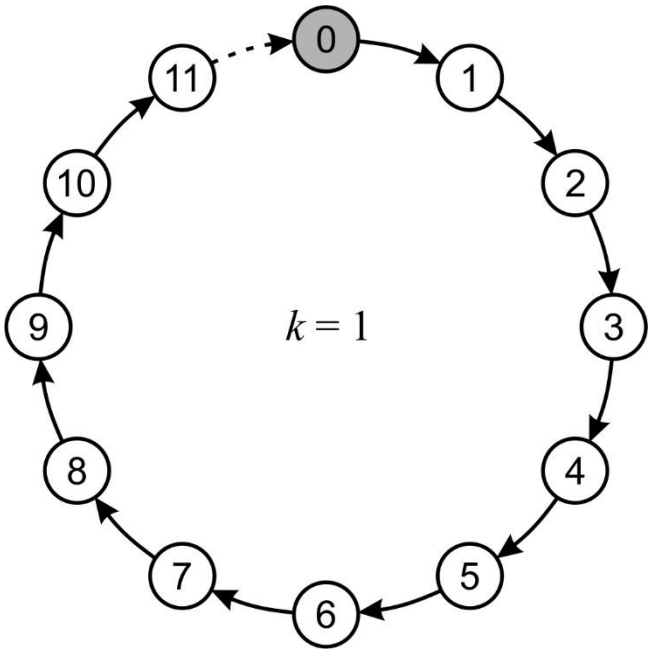

Figure 1.6. Cycle tour of the series $n = \overline{0,11}$.

Go through the alphabet elements Z_{12}, starting with element 0 (highlighted by shading) to 11 corresponds to the coefficient of cyclic thinning $k=1$.

Cyclic bypass graphs of the same sequence with thinning factors $k=2$ and $k=3$ is shown in Fig. 1.7 a) and b), respectively.

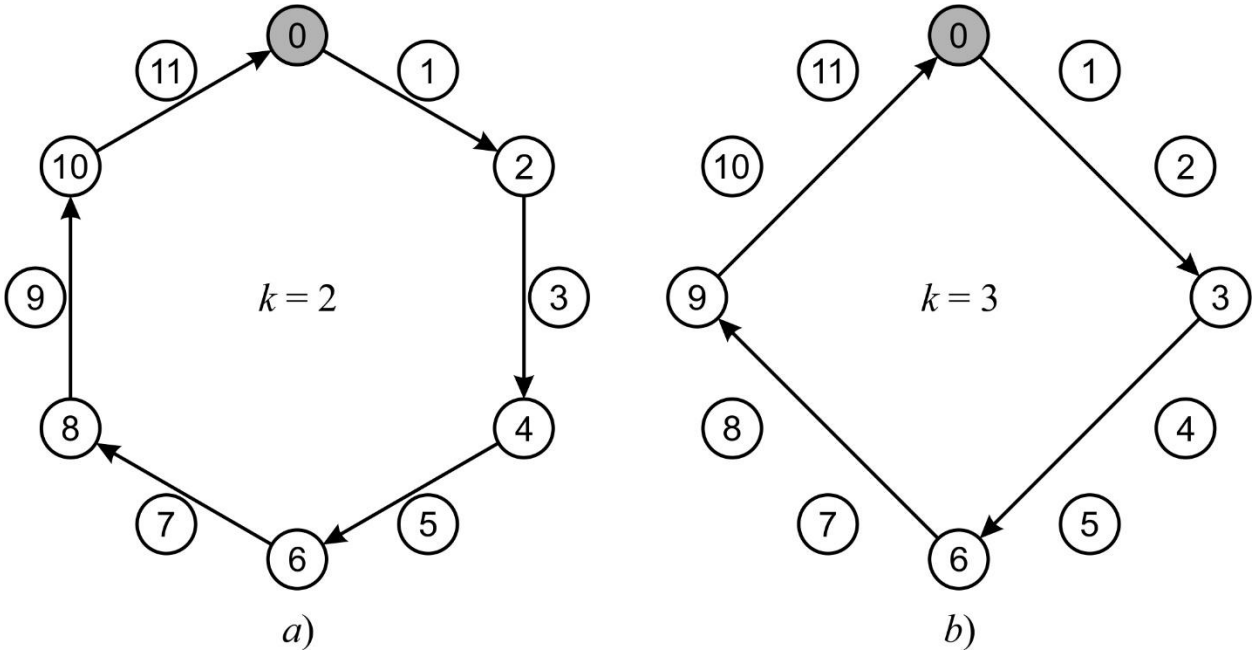

Figure 1.7. Cycle tour of the series $n=\overline{0,11}$ with thinning factors $k=2$ and $k=3$.

In accordance with Fig. 1.7, a, cycle tour of the series $n=\overline{0,11}$ with the thinning factor $k=2$ leads to the formation of the sequence (denoted P_2), including such elements of the alphabet Z_{12}

$$P_2=\{0,2,4,6,8,10\} \tag{1.13}$$

If $k=3$, then (Fig. 1.7, b)

$$P_3=\{0,3,6,9\} \tag{1.14}$$

As follows from (1.13) and (1.14), the sequences P_2 and P_3 consist of a portion of recurrent elements of the alphabet Z_{12}. In the case when the thinning factor k is *coprime* to the base of the number system m, the sequence P_k will consist of all the elements of the alphabet Z_m. This option (coprime numbers m=12 and k =5) shown in Fig. 1.8.

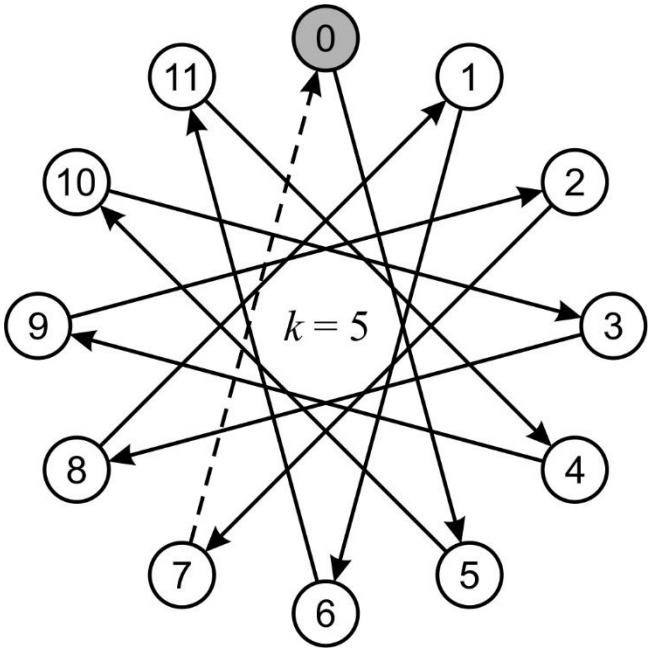

Figure 1.8. Cycle tour of the series $n=\overline{0,11}$ with thinning factor $k=5$

Sequence P_5, corresponding to loop through the analyzed series of numbers with the thinning factor $k=5$, is as follows:

$$P_5=\{0,5,10,3,8,1,6,11,4,9,2,7\}.$$

Present a rigorous mathematical form of the rule for synthesis of Cayley tables of the bitwise modular multiplication. Let $e(k,n)$ be in the Cayley table the $n-$th element of the k-th row, $k,n=\overline{0,m-1}$. And let, in addition, $n\uparrow k$ means $k-$ *thinning* of the series $n=\overline{0,m-1}$, i.e. cyclic selection of each $k-$th element of the alphabet Z_m, starting with the zero element.

The first two rows of multiplication table can be described as a system of equalities.

$$\left.\begin{matrix} e(0,n) \\ e(1,n) \end{matrix}\right\},\ n=\overline{0,m-1}. \tag{1.15}$$

For $k\geq 2$, we have

$$e(k,n)=e(1,\uparrow k), \tag{1.16}$$

i.e. elements of $k-$th row of the table of bitwise multiplication are formed from the elements of the first row in the result of the selection of each of the cyclic $k-$th element, starting from zero, of the alphabet Z_m.

In accordance with the algorithm construct the Cayley table of the bitwise multiplication of 16(hexadecimal) number system (tab. 1.6).

Table 1.6. The operation of multiplication modulo 16

$\overset{16}{\otimes}$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	$\rightarrow x$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
1	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
2	0	2	4	6	8	A	C	E	0	2	4	6	8	A	C	E	
3	0	3	6	9	C	F	2	5	8	B	E	1	4	7	A	D	
4	0	4	8	C	0	4	8	C	0	4	8	C	0	4	8	C	
5	0	5	A	F	4	9	E	3	8	D	2	7	C	1	6	B	
6	0	6	C	2	8	E	4	A	0	6	C	2	8	E	4	A	
7	0	7	E	5	C	3	A	1	8	F	6	D	4	B	2	9	
8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	
9	0	9	2	B	4	D	6	F	8	1	A	3	C	5	E	7	
A	0	A	4	E	8	2	C	6	0	A	4	E	8	2	C	6	
B	0	B	6	1	C	7	2	D	8	3	E	9	4	F	A	5	
C	0	C	8	4	0	C	8	4	0	C	8	4	0	C	8	4	
D	0	D	A	7	4	1	E	B	8	5	2	F	C	9	6	3	
E	0	E	C	A	8	6	4	2	0	E	C	A	8	6	4	2	
F	0	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	

$\downarrow y$

We note that if in Table. 1.6 throw out the null string and the zero column, the remaining table has 15-th order and is *double-symmetric*, ie, symmetric with respect to both the main and auxiliary diagonals.

If the radix m is binary power number (power of two), that is, $m = 2^l$, $l = 1, 2, \ldots$, it is possible to make a recursive form of the relation (1.16):

$$e(2k, n) = e(1, n \uparrow 2), \tag{1.17}$$

for pair and

$$e(2k+1, n) = (e(1, n) + e(2k, n))_m, \tag{1.18}$$

for odd rows of the table of bitwise multiplication.

Initial conditions (1.15) and the system of equations (1.17) and (1.18) make it possible to make a bitwise multiplication tables for all binary power values of m radix. If m is not a power of two, then the Cayley table for the synthesis of modular multiplication is performed by the general rules in accordance with the relations (1.15) and (1.16).

1.6.4. Operation of the modular division

In the subsection we will discuss mainly the calculation of the *inverse values modulo* m. Suppose that y is a number. Then

$$1/y$$

is the inverse value y^{-1} of the number y. In modular arithmetic, the problem of determining inverse values by a given module is solving, when it is necessary to find

$$\left(\frac{1}{y}\right)_m, \tag{1.19}$$

or in a more general formulation, calculate

$$\left(\frac{x}{y}\right)_m, \tag{1.20}$$

where x, y and m – are positive integers.

It turns out that not for all values x, y and m there are solutions of expressions (1.19) and (1.20). For example, number 2 does not have the inverse modulo 4 (in equal measure, as well as on any even modulo m). The general problem of solving expression (1.19) consists of determining a such values of z, that

$$(z \cdot y)_m = 1. \tag{1.21}$$

Equality (1.21) can also be written in the form

$$y^{-1} \equiv z \pmod{m}, \tag{1.22}$$

i.e. the inverse of the y should be congruence z modulo m.

In general, the equation (1.22) has a unique solution if y and m coprime. For example, suppose $y=4$, a $m=7$. Then the inverse of the number 4 modulo 7 can be determined by doing the following chain of transformations:

$$\left(\frac{1}{4}\right)_7 = \left(\frac{1\cdot z}{4\cdot z}\right)_7 = \left(\frac{1\cdot 2}{4\cdot 2}\right)_7 = \frac{2_7}{8_7} = \frac{2}{1} = 2. \qquad (1.23)$$

The solution (1.23) obtained by the method of selection of the multiplier z of the numerator and the denominator on the left side of this equality, whereby the denominator $(4\cdot z)$ is reduced to unity and thus transformed numerator becomes the desired value y^{-1}.

For coprime numbers y and m the general solution of the expression (1.19) has the form

$$z \equiv y^{\varphi(m)-1} \left(\mathrm{mod}\, m\right), \qquad (1.24)$$

where $\varphi(m)$ is the *Euler totient function*, sometimes called the Euler "phi" function.

Euler totient function (**Euler function**) $\varphi(m)$ *is equal to the number of positive integers less than* m *and coprime to* m, for anyone $m \geq 1$. If m is a prime number equal *to* p, then

$$\varphi(p) = p-1 \text{ and } \varphi(p^k) = p^{k-1}\varphi(p).$$

If p and q –prime numbers, then

$$\varphi(p\cdot q) = (p-1)\cdot(q-1).$$

Table. 1.7 shows the values of Euler's function $\varphi(u)$ for u, composed of two decimal numbers s and t, those. $u = s||t$, where $||-$ is the concatenation character (concatenation) of two numbers. We note that if $m \geq 3$, the Euler function $\varphi(m)$ is an even number.

The algorithm (1.24), corresponding to the solution (1.19), can be transferred to a more general problem definition z for the ratio (1.20). Wherein

$$z = (x\cdot y^{\varphi(m)-1}) \bmod m, \qquad (1.25)$$

Table 1.7. Euler function of numbers $u = s \,||\, t$

High Digit	Low digit t										
	0	1	2	3	4	5	6	7	8	9	$\rightarrow t$
0	–	1	1	2	2	4	2	6	4	6	
1	4	10	4	12	6	8	8	16	6	18	
2	8	12	10	22	8	20	12	18	12	28	
3	8	30	16	20	16	24	12	36	18	24	
4	16	40	12	42	20	24	22	46	16	42	
5	20	32	24	52	18	40	24	36	28	58	
6	16	60	30	36	32	48	20	66	32	44	
7	24	70	24	72	36	40	36	60	24	78	
8	32	54	40	82	24	64	42	56	40	88	
9	24	72	44	60	46	72	32	96	42	60	
$\downarrow s$											

The results of calculation z by (1.25) for the modul0 $m = 11$ (prime) are shown in Table. 1.8.

Table 1.8. The solution of the equation (2.19) for the modulo $m = 11$

	1	2	3	4	5	6	7	8	9	10	$\rightarrow x$
1	1	2	3	4	5	6	7	8	9	10	
2	6	1	7	2	8	3	9	4	10	5	
3	4	8	1	5	9	2	6	10	3	7	
4	3	6	9	1	4	7	10	2	5	8	
5	9	7	5	3	1	10	8	6	4	2	
6	2	4	6	8	10	1	3	5	7	9	
7	8	5	2	10	7	4	1	9	6	3	
8	7	3	10	6	2	9	5	1	8	4	
9	5	10	4	9	3	8	2	7	1	6	
10	10	9	8	7	6	5	4	3	2	1	
$\downarrow y$											

Computing z can be performed easily for any modulo, which is a prime number p. Such tables have the property of *double mirror symmetry*, consisting in the fact that

$$z(x, y) = z(p - x, p - y),$$

which can be traced by the table 1.8.

1.7. Foundations of algebra of modular matrices

We will call the matrix $\boldsymbol{A}$ *modular* when all its elements $a_{i,j}$ belong to the set Z_p, i.e $a_{i,j} \in Z_p$, where $p-$ prime number, and in addition, any of the algebraic transformations over matrix elements are completed by reducing them to the modulo p. Such matrices are called also as matrices over a Galois field of characteristic p (see. Section 3) *when* $a_{i,j} \in GF(p)$.

1.7.1. The simplest algebraic transformations

To the algebraic transformations of modular matrices we will refer the operations of addition, subtraction, multiplication and division of matrices, as well as operations of multiplication and division of matrices by an integer.

The operations of addition and subtraction of matrices are very simple. So if $\boldsymbol{R}$ and $\boldsymbol{S}$ are two modular matrices of $n-$ order, then when the matrices are added, a matrix $\boldsymbol{T}$ is formed, elements of which are formed by the rule:

$$t_{ij} = \left(r_{ij} + s_{ij}\right)_{m_t},\ i,\ j = \overline{0, n-1},$$

where m_t is the radix of the number system of the matrix $\boldsymbol{T}$, does not necessarily coincide with the m.

Consider a numerical example. Let $m = 5$ and

$$\boldsymbol{R}_{(5)} = \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix}; \qquad \boldsymbol{S}_{(5)} = \begin{pmatrix} 1 & 4 \\ 3 & 4 \end{pmatrix}.$$

if $m_t = 5$, then

$$\boldsymbol{T}_{(5)} = \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix}.$$

Subtract from the matrices $\boldsymbol{T}_{(5)}$ the matrix $\boldsymbol{R}_{(5)}$. We get

$$\boldsymbol{T}_{(5)} - \boldsymbol{R}_{(5)} = \begin{pmatrix} 1 & -1 \\ 3 & -1 \end{pmatrix}.$$

Taking into account that $(-1)_5 = 4$, we obtain a matrix $\boldsymbol{S}$, as expected.

And now let $m_t = 7$. The sum of matrices $\boldsymbol{R}$ and $\boldsymbol{S}$ (matrix $\boldsymbol{T}$) modulo 7 is equal

$$\boldsymbol{T}_{(7)} = \begin{pmatrix} 3 & 0 \\ 4 & 1 \end{pmatrix}.$$

Again, now we subtract the matrix $\boldsymbol{R}_{(5)}$ from the matrix $\boldsymbol{T}_{(7)}$. We have

$$\boldsymbol{T}_{(7)} - \boldsymbol{R}_{(5)} = \begin{pmatrix} 1 & -3 \\ 3 & -3 \end{pmatrix}.$$

Taking into account that $(-3)_7 = 4$, the last transformation restores the matrix $\boldsymbol{S}$, as one would expect.

If the radix $m_t < m$, then the modular addition operation becomes irreversible and in this case $\boldsymbol{T} - \boldsymbol{S} \neq \boldsymbol{R}$.

Multiplication of the matrix by an integer in modular arithmetic is a fairly trivial operation and reduces to the following. Suppose we are given a square matrix of the order n, whose elements are one-digit numbers with the radix m. When multiplying this matrix by an integer k instead of each element a_{ij} recorded the remainder of dividing the product ka_{ij} on the base m, i.e.

$$a_{ij} \Rightarrow \left(ka_{ij}\right)_m,$$

where the symbol $\Rightarrow$ means the "replacement" of the element a_{ij} by the residue modulo m of the product ka_{ij}.

Consider an example. Let $m = n = 3$, and the matrix $\boldsymbol{A}_{(3)}$ is as follows:

$$\boldsymbol{A}_{(3)} = \begin{pmatrix} 0 & 2 & 2 \\ 1 & 1 & 2 \\ 0 & 1 & 0 \end{pmatrix}.$$

Multiplying this matrix on the integer $k = 2$ we arrive to the matrix

$$\left(k\boldsymbol{A}\right)_{(3)}=\begin{pmatrix}0 & 1 & 1\\ 2 & 2 & 1\\ 0 & 2 & 0\end{pmatrix}.$$

Note that the multiplication of the matrix $\boldsymbol{A}_{(3)}$ by an integer $k=3$ is equivalent to the multiplication by zero, since $\left(3\right)_3=0$. Multiplication of the matrix $\boldsymbol{A}_{(3)}$ by an integer $k=2$ is equivalent to multiplication by unity as $\left(4\right)_3=1$ etc.

The operation of dividing the modular matrix by an integer reduces to the operations of dividing each element of the matrix by this number modulo m, sufficiently detailed in 1.5.4.

We now turn to the operation of modular multiplication of matrices. Let

$$\boldsymbol{A}=\begin{pmatrix}a_{11} & a_{12} & ... & a_{1n}\\ a_{21} & a_{22} & ... & a_{2n}\\ . & . & . & .\\ a_{n1} & a_{n2} & ... & a_{nn}\end{pmatrix};\qquad \boldsymbol{B}=\begin{pmatrix}b_{11} & b_{12} & ... & b_{1n}\\ b_{21} & b_{22} & ... & b_{2n}\\ . & . & . & .\\ b_{n1} & b_{n2} & ... & b_{nn}\end{pmatrix}.$$

be modular square matrix of n order on the radix m.

Definition 1.7. *The product of square modular matrices* $\boldsymbol{A}$ *and* $\boldsymbol{B}$ *of the order* n *is the matrix* $\boldsymbol{C}=\boldsymbol{AB}$*, element* c_{ij} *of which is located in the i-th row and j-th column, equal to the residue modulo* m *of the sum of products of elements of i-th row of the matrix* $\boldsymbol{A}$ *by corresponding elements of j-th column of the matrix* $\boldsymbol{B}$.

So,

$$c_{ij}=\left(\sum_{k=1}^{n}a_{ij}\cdot b_{kj}\right). \qquad (1.26)$$

As an example we calculate the product of two modular matrices

$$\boldsymbol{A}=\begin{pmatrix}4 & 2 & 1\\ 2 & 2 & 4\\ 3 & 1 & 2\end{pmatrix},\quad \boldsymbol{B}=\begin{pmatrix}2 & 4 & 3\\ 1 & 3 & 2\\ 0 & 4 & 1\end{pmatrix}. \qquad (1.27)$$

modulo $m=5$.

Using the formula (1.26), we obtain

$$\boldsymbol{C}=\begin{pmatrix}0 & 1 & 2\\ 1 & 0 & 4\\ 2 & 3 & 3\end{pmatrix}.$$

The product of modular matrices, as well as the usual ones, depends on the order of the factors, that is, *the multiplication of modular matrices in the general case is not commutative*.

To confirm the marked features let us multiply matrices (1.27) in the reverse order, that is, calculate the matrix $\boldsymbol{C'}=\boldsymbol{BA}$ modulo $m=5$. After completing elementary calculations, we find

$$\boldsymbol{C'}=\begin{pmatrix}0 & 0 & 4\\ 1 & 0 & 2\\ 1 & 4 & 3\end{pmatrix}.$$

and we are convinced that $\boldsymbol{C}\neq\boldsymbol{C'}$.

1.7.2. Determinants of modular matrices

When solving the problem associated with calculating the determinants of modular matrices, the entire spectrum of techniques that has been accumulated in the classical theory of matrix calculus can be used, but taking into account the characteristics of performing algebraic operations in modular arithmetic.

We list the main properties of determinants.

Property 1. *When the matrix is transposed, its determinant does not changed.*

Property 2. *If all the elements of a column (row) of the determinant are zero, then the determinant itself is equal to zero*.

Property 3. *When you rearrange any two columns (rows) of the determinant, its sign changes to the opposite.*

Property 4. The determinant does not change if to any of its column (row) is added an arbitrary linear combination of its other columns (rows).

On numerical examples, it is easy to verify that the determinant of a modular matrix is equal to the residue modulo m of the usual determinant of the matrix.

1.7.3. Inverse modular matrices

A modular matrix $\boldsymbol{B}$ *is called the inverse of the matrix* $\boldsymbol{A}$*, if their product modulo* m *is equal to the identity matrix i.e.*

$$(\boldsymbol{AB})_m = (\boldsymbol{BA})_m = \boldsymbol{E}.$$

If the determinant Δ of the matrix $\boldsymbol{A}$ It is not equal to zero, and in addition, Δ and m are coprime, then the matrix $\boldsymbol{A}$ has an inverse $\boldsymbol{A}^{-1}$, which is calculated by the formula

$$\boldsymbol{A}^{-1} = \left(\frac{1}{\Delta}\tilde{\boldsymbol{A}}\right)_m. \qquad (1.28)$$

where $\tilde{\boldsymbol{A}}$ is the adjugate matrix of the matrix $\boldsymbol{A}$.

From the relation (1.28), in particular, it follows that the radix m must be a prime number p, since otherwise $(m \neq p)$ are not guaranteed the existence of the determinant of a modular matrix $\boldsymbol{A}$.

Let $\boldsymbol{A}$ be a matrix of the order n. We represent the adjugate matrix $\tilde{\boldsymbol{A}}$ as

$$\tilde{\boldsymbol{A}} = \begin{pmatrix} \boldsymbol{A}_{11} & \boldsymbol{A}_{21} & \dots & \boldsymbol{A}_{n1} \\ \boldsymbol{A}_{12} & \boldsymbol{A}_{22} & \dots & \boldsymbol{A}_{n2} \\ \dots & \dots & \dots & \dots \\ \boldsymbol{A}_{1n} & \boldsymbol{A}_{2n} & \dots & \boldsymbol{A}_{nn} \end{pmatrix}.$$

This matrix element located in a $i-$ th row and $j-$ th column, is the cofactor $\boldsymbol{A}_{ji}$ of the element a_{ji} of the matrix $\boldsymbol{A}$. The cofactor $\boldsymbol{A}_{ji}$ is given by

$$\boldsymbol{A}_{ji} = (-1)^{j+i}\boldsymbol{M}_{ji},$$

where $\boldsymbol{M}_{ji}$ is the minor of the element a_{ji} of the matrix $\boldsymbol{A}$, equal to the determinant of the matrix which is composed from the matrix $\boldsymbol{A}$ by deleting $j-$th rows and $i-$ th column.

More convenient is the next sequence of calculating of the adjugate matrix. First, we transpose the matrix *A*

$$\boldsymbol{A} \Rightarrow \boldsymbol{A}^T = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{n1} \\ a_{12} & a_{22} & \dots & a_{n2} \\ \dots & \dots & \dots & \dots \\ a_{1n} & a_{2n} & \dots & a_{nn} \end{pmatrix}, \tag{1.29}$$

whereby the adjugate matrix takes the form:

$$\tilde{\boldsymbol{A}} = \begin{pmatrix} \boldsymbol{A}_{11} & \boldsymbol{A}_{12} & \dots & \boldsymbol{A}_{1n} \\ \boldsymbol{A}_{21} & \boldsymbol{A}_{22} & \dots & \boldsymbol{A}_{2n} \\ \dots & \dots & \dots & \dots \\ \boldsymbol{A}_{n1} & \boldsymbol{A}_{n2} & \dots & \boldsymbol{A}_{nn} \end{pmatrix}. \tag{1.30}$$

In the matrix (1.30) the cofactor $\boldsymbol{A}_{ji}$ up to sign, equal $(-1)^{i+j}$, coincides with the determinant of the matrix (1.29), from which the previously removed items of $i-$ th row and $j-$ th column.

Consider the example of calculating the modular inverse matrix of order 3. Let $m = 5$ and

$$\boldsymbol{A} = \begin{pmatrix} 4 & 2 & 1 \\ 2 & 2 & 4 \\ 3 & 1 & 2 \end{pmatrix}. \tag{1.31}$$

According to the property of determinants, an arbitrary linear combination of its other columns can be added to any column of the matrix. Let us add to the first column of the matrix (1.31) third. The summation is carried out modulo $= 5$. We have

$$\Delta = \begin{vmatrix} 0 & 2 & 1 \\ 1 & 2 & 4 \\ 0 & 1 & 2 \end{vmatrix}. \tag{1.32}$$

We expand the matrix (1.32) by the elements of the first column. In view of the sign of the minor of the elements a_{21} of (1.32), we obtain

$$\Delta = \left[- \begin{vmatrix} 2 & 1 \\ 1 & 2 \end{vmatrix} \right] = (-3)_5 = 2.$$

We turn to the second method of calculation of the determinant of the modular matrix. In the classical calculus of the determinant of the matrix is equal to the sum of the products of all the elements of a matrix row (column) by their cofactors. In the modular matrix calculus, this sum must be taken by the given modulo m. In view of the clarification we expand the determinant of the matrix (1.31) by the elements of the first row. Taking into account the signs of cofactors, we obtain

$$\Delta = \left[4\begin{vmatrix} 2 & 4 \\ 1 & 2 \end{vmatrix} - 2\begin{vmatrix} 2 & 4 \\ 3 & 2 \end{vmatrix} + \begin{vmatrix} 2 & 2 \\ 3 & 1 \end{vmatrix} \right]_5 =$$

$$= \left(4(4-4) - 2(4-12) + (2-6)\right)_5 = (26-14)_5 = 2.$$

Both considered variants of calculating the determinant led to the same result, which is natural.

The procedure for calculating the inverse matrix (1.31) involves sequential execution of the following steps. First we write the matrix A^T, transposed to the matrix (1.31),

$$\boldsymbol{A}^T = \begin{pmatrix} 4 & 2 & 3 \\ 2 & 2 & 1 \\ 1 & 4 & 2 \end{pmatrix}. \qquad (1.33)$$

The general form of the matrix of the 3rd order, adjugated to the matrix (1.33), has the form

$$\tilde{\boldsymbol{A}} = \begin{pmatrix} \boldsymbol{A}_{11} & \boldsymbol{A}_{13} & \boldsymbol{A}_{13} \\ \boldsymbol{A}_{21} & \boldsymbol{A}_{22} & \boldsymbol{A}_{23} \\ \boldsymbol{A}_{31} & \boldsymbol{A}_{32} & \boldsymbol{A}_{33} \end{pmatrix},$$

where $\boldsymbol{A}_{ij}$ are cofactors of elements a_{ij} of the matrix (1.33).

Compute cofactors $\boldsymbol{A}_{ij}$ of elements a_{ij} of the matrix (1.33) modulo $m = 5$ with taking into account the sign $(-1)^{i+j}$:

$$\boldsymbol{A}_{11}=\begin{vmatrix}2 & 1\\ 4 & 2\end{vmatrix}=(4-4)_5=0; \qquad \boldsymbol{A}_{12}=-\begin{vmatrix}2 & 1\\ 1 & 2\end{vmatrix}=-(4-1)_5=-3;$$

$$\boldsymbol{A}_{13}=\begin{vmatrix}2 & 2\\ 1 & 4\end{vmatrix}=(8-2)_5=1; \qquad \boldsymbol{A}_{21}=-\begin{vmatrix}2 & 3\\ 4 & 2\end{vmatrix}=-(4-12)_5=-2;$$

$$\boldsymbol{A}_{22}=\begin{vmatrix}4 & 3\\ 1 & 2\end{vmatrix}=(8-3)_5=0; \qquad \boldsymbol{A}_{23}=-\begin{vmatrix}4 & 2\\ 1 & 4\end{vmatrix}=-(16-2)_5=-4;$$

$$\boldsymbol{A}_{31}=\begin{vmatrix}2 & 3\\ 2 & 1\end{vmatrix}=(2-6)_5=1; \qquad \boldsymbol{A}_{32}=-\begin{vmatrix}4 & 3\\ 2 & 1\end{vmatrix}=-(4-6)_5=-3;$$

$$\boldsymbol{A}_{313}=\begin{vmatrix}4 & 2\\ 2 & 2\end{vmatrix}=(8-4)_5=4.$$

We form the adjugate matrix

$$\tilde{\boldsymbol{A}}=\begin{pmatrix}0 & -3 & 1\\ -2 & 0 & -4\\ 1 & -3 & 4\end{pmatrix}. \qquad (1.34)$$

We proceed in the matrix (1.34) from negative elements to their positive values modulo $m=5$:

$$\tilde{\boldsymbol{A}}=\begin{pmatrix}0 & 2 & 1\\ 3 & 0 & 1\\ 1 & 2 & 4\end{pmatrix}.$$

According to (1.28) and taking into account that $\Delta=2$, we can write the expression for the inverse matrix

$$\boldsymbol{A}^{-1}=\left(\frac{1}{2}\begin{pmatrix}0 & 2 & 1\\ 3 & 0 & 1\\ 1 & 2 & 4\end{pmatrix}\right)_5. \qquad (1.35)$$

Let us remove the fractional factor of the matrix (1.35). With this aim, multiplying the numerator and the denominator of the fraction $5\ (1/2)_5$ by 3, we get

$$\left(\frac{1}{2}\right)_5=\left(\frac{1\cdot 3}{2\cdot 3}\right)_5=\left(\frac{3}{6}\right)_5=\frac{3}{1}=3.$$

and hence,

$$\boldsymbol{A}^{-1} = 3\begin{pmatrix} 0 & 2 & 1 \\ 3 & 0 & 1 \\ 1 & 2 & 4 \end{pmatrix}_5 . \qquad (1.36)$$

After completing the operation of multiplication modulo 5 in the right side of the formula (1.36), we arrive to the final expression for the inverse matrix

$$\boldsymbol{A}^{-1} = \begin{pmatrix} 0 & 1 & 3 \\ 3 & 0 & 3 \\ 3 & 1 & 2 \end{pmatrix}_5 . \qquad (1.37)$$

It is easy to verify that the product of the matrices (1.31) and (1.37) modulo 5 equal to the identity matrix of the third order. Therefore, the inverse matrix is calculated correctly.

1.8. Kronecker product of modular matrices

We consider the operation of the *Kronecker product* important in the ordinary and matrix algebra.

Let $\boldsymbol{A}$ and $\boldsymbol{B}$ be square matrices of $k-$th and $n-$th orders, respectively. We write the matrices in the form of

$$\boldsymbol{A} = \left[a_{ij} \right], \quad i, j = \overline{1, k}; \quad \boldsymbol{B} = \left[b_{ij} \right], \quad i, j = \overline{1, n},$$

where i, j are numbers of rows and columns of matrices.

Kronecker product of matrices $\boldsymbol{A}$ and $\boldsymbol{B}$ is the matrix $\boldsymbol{C}$ of the order kn, formed by replacing the elements a_{ij} of the matrix $\boldsymbol{A}$ with the product $a_{ij}\boldsymbol{B}$, i.e.

$$\boldsymbol{C} = \boldsymbol{A} \otimes \boldsymbol{B} = \left[a_{ij} \cdot \boldsymbol{B} \right], \qquad (1.38)$$

where $\times$ - is the sign of the Kronecker (tensor) product.

Let us explain the definition of the Kronecker product on a numerical example, taken from usual (non-modular) algebra. Let

$$\boldsymbol{A} = \begin{pmatrix} 2 & 3 \\ 4 & 1 \end{pmatrix} \text{ and } \boldsymbol{B} = \begin{pmatrix} 0 & 1 & 2 \\ 3 & 2 & 3 \\ 1 & 4 & 2 \end{pmatrix}. \qquad (1.39)$$

Substituting the matrices (1.39) into (1.38), we have

$$\boldsymbol{C} = \begin{pmatrix} 2\boldsymbol{B} & | & 3\boldsymbol{B} \\ -- & | & -- \\ 4\boldsymbol{B} & | & 1\boldsymbol{B} \end{pmatrix}. \qquad (1.40)$$

Replacing in the expression (1.40) the matrix $\boldsymbol{B}$ by its value from (1.39) and performing usual arithmetic multiplication, we obtain a square matrix $\boldsymbol{C}$ of the sixth order

$$\boldsymbol{C} = \begin{pmatrix} 0 & 2 & 4 & 0 & 3 & 6 \\ 6 & 4 & 6 & 9 & 6 & 9 \\ 2 & 8 & 2 & 3 & 12 & 6 \\ 0 & 4 & 8 & 0 & 1 & 2 \\ 12 & 8 & 12 & 3 & 2 & 3 \\ 4 & 16 & 8 & 1 & 4 & 2 \end{pmatrix}. \qquad (1.41)$$

If the Kronecker product involves modular matrix with radix equal to m, then all elements of the matrix (1.41) should be reduce to the residue modulo m. In particular, when $m = 5$, then

$$\boldsymbol{C}_{(5)} = \begin{pmatrix} 0 & 2 & 4 & 0 & 3 & 1 \\ 1 & 4 & 1 & 4 & 1 & 4 \\ 2 & 3 & 2 & 3 & 2 & 1 \\ 0 & 4 & 3 & 0 & 1 & 2 \\ 2 & 3 & 2 & 3 & 2 & 3 \\ 4 & 1 & 3 & 1 & 4 & 2 \end{pmatrix}.$$

If matrices **A** and **B** are of the same order and is equal to the matrix $\boldsymbol{M}$, then the relation (1.38) defines a second Kronecker degree of the matrix $\boldsymbol{M}$ (the exponent is enclosed in square brackets)

$$\boldsymbol{M}^{[2]} = \boldsymbol{M} \otimes \boldsymbol{M}\,.$$

Kronecker degree can be continued. In particular,

$$\boldsymbol{M}^{[3]} = \boldsymbol{M} \otimes \boldsymbol{M} \otimes \boldsymbol{M}; \quad \boldsymbol{M}^{[n]} = \underbrace{\boldsymbol{M} \otimes \boldsymbol{M} \otimes \ldots \otimes \boldsymbol{M}}_{n \ \ times}$$

Summary of the chapter

1. Higher arithmetic or number theory, studies the properties of natural numbers 1, 2, 3, ...

2. The number is an abstract quantitative measure of the set of elements of an arbitrary nature, i.e. a number is a term used to express the quantity. The number consists of digits.

3. A digit is a sign for denoting a number.

4. Signs are notations for writing mathematical concepts (including the concept of number) and calculations.

5. The position of the digit in a number entry is called a digit.

6. Natural number are numbers that are naturally used when counting. The sequence of all natural numbers arranged in ascending order (1, 2, 3, ...) is called the natural series.

7. An extended natural series is a sequence of non-negative integers starting with zero (0, 1, 2, 3 ...).

8. A natural number n is divided by an natural number m, if there is a natural number k, such that $n = m \cdot k$. Divisibility of n by m without residue is denoted as $m \mid n$.

9. The numbers 1 and n are improper divisors of a natural number n

10. Divisors of natural number n, different from unity and the same number n, is called proper divisors of n.

11. An integer number is called a prime number p, if it is divided only by 1 and itself, i.e. has only improper divisors.

12. A composite number is a number n, which in addition to improper dividers has at least one proper divisor.

13. Integer number $\delta \neq 0$ is called a common divisor of integers $a_1, a_2, \ldots, a_n$ if each of these numbers is divided into δ.

14. Two non-negative integers a and b are called coprime if their only common divisor is the unit.

15. Any integer number greater than 1 is a prime number or is decomposed in a product of primes in one and only one way (up to permutation of the factors).

16. Integer number d is called the greatest common divisor (GCD) of integers $a_1, a_2, \ldots, a_n$, if:

- d is a common divisor of these numbers;

- d is divisible by any common divisor of numbers $a_1, a_2, \ldots, a_n$.

17. GCD of the set of integers $a_1, a_2, \ldots, a_n$ is denoted $d = GCD(a_1, a_2, \ldots, a_n)$ or simply $d = (a_1, a_2, \ldots, a_n)$.

18. GCD of coprime numbers a and b is equal 1.

19. Under a number system is commonly understood methods of writing numbers by numeric characters (digits) and rules of operations with the numbers.

20. Number systems can be divided into non-positional and positional system.

21. Non-positional number systems characterized by the fact that each character (from the set of characters, adopted in this system to refer to the numbers) always denotes the same number regardless of the location (position) occupied by this character in the record of the number.

22. In position number systems the same sign can mean different numbers depending on the location (position) occupied by this sign in the record of the number.

23. The number of different digits used in a positional number system (PNS) is called its base.

24. Elementary numbers of arbitrary $m-$ ary positional number system are number from 0 (zero) to $m-1$, where $m-$ is the base of the number system.

25. Each position of a number with the assigned sequence number is called the digit of the number.

26. In any $m-$ ary positional system the radix is written as a combination of 10 digits.

27. The residue of the number n modulo m is the difference r between the number n and the product $k \cdot m$, where k is the integer part of the quotient n/m, i.e. $r = n - [n/m] \cdot m$.

28. To translation integer from one positional system to another it must be consistently divided on the basis m of the system in which it is translated. At the same time the base m is represented as a combination of numbers, which are the

elementary numbers of base of the number system of the initial number. The division is made up, as long as quotient will not less than m. The number in the new system takes the form of division residues, read from the last to the first residue.

29. In the present time, the most widely used are binary-exponential number systems with the base $m = 2^n$, where $n \geq 1 -$ a natural number.

30. The generalization of binary-power number system are $p -$ ary power systems in which the base of number systems is $m = p^n$, where $p -$ prime, and $n \geq 1 -$ natural number.

31. Two integers A and B are called *congruent modulo* m, if they are identical residues modulo m.

32. Residues of positive integers modulo m are formed as a result of clockwise "wrapping" of positive numerical semiaxis on the drum containing m evenly spaced on the drum residues modulo m, those numbers $0, 1, \ldots, m-1$.

33. Residues of negative integers modulo m are formed as a result of counter-clockwise "wrapping" of negative numerical semiaxis on the drum containing m evenly spaced on the drum residues modulo m.

34. If two numbers a and b under divided by module m form the same residue r, then it is say that these numbers belong to the same *class of residues* $\overline{r}$ *modulo* m.

35. Element a, belonging to the set of residues modulo a prime p, is called a quadratic nonresidue modulo p, if there is no $x \in Z_p$, such that $x^2 \equiv a \pmod{p}$.

36. Element a, belonging to the set of residues modulo a prime p, is called a quadratic residue modulo p, if there is $x \in Z_p$, such that $x^2 \equiv a \pmod{p}$.

37. The set of residue classes $\overline{0}, \overline{1}, \ldots, \overline{p-1}$ forms a complete system of residues modulo p, whose members (the number of $0, 1, \ldots, p-1$) belongs to the set Z_p, where $p -$ prime number.

38. In the complete system of non-zero residues modulo p, denoted by Z_p^*, half of them will be quadratic residues, and the other half - quadratic non-residues.

39. A distinctive feature of the bit-wise operations in modular arithmetic is that all arithmetic operations (addition, subtraction, multiplication and division) are performed exclusively on single-digit numbers.

40. Euler totient function $\varphi(m)$ counts the number of positive integers less than m, and coprime to m, for any $m \geq 1$.

41.If $m \geq 3$, then the Euler totient function $\varphi(m)$ is an even number.

42. We will call the matrix $\boldsymbol{A}$ as modular, if all elements a_{ij} belong to the set Z_p, that is $a_{ij} \in Z_p$ and $p-$prime number, and, in besides, any algebraic transformation over matrix elements are completed by reducing them to the residue modulo p. Such matrices are also called matrices over a Galois field of characteristic p, when $a_{i,j} \in GF(p)$.

43. The product of square modular matrices $\boldsymbol{A}$ and $\boldsymbol{B}$ of order n is the matrix $\boldsymbol{C} = \boldsymbol{AB}$, element $c_{i,j}$ of which is located in the i-th row and j-th column, equal to the residue modulo m of the sum of products of elements of i-th row of the matrix $\boldsymbol{A}$ on the corresponding elements of j-th column of the matrix $\boldsymbol{B}$.

44. For the product of modular matrices associative and distributive laws of arithmetic are saved. At the same time, the product of modular matrices, as usual, depends on the order of the factors, i.e., *modular multiplication of matrices is not commutative in general*.

45.Modular matrix $\boldsymbol{B}$ is called the inverse of a matrix $\boldsymbol{A}$, if their product modulo m equal to the identity matrix.

46. If the determinant Δ of the modular matrix $\boldsymbol{A}$ is not equal to zero, and in addition Δ and radix $m-$ coprime, then the matrix $\boldsymbol{A}$ has the inverse $\boldsymbol{A}^{-1}$.

47. Radix m must be a prime number p, since otherwise $(m \neq p)$ are not guaranteed the existence of the determinant of a modular matrix $\boldsymbol{A}$.

48. Kroneker product of matrices $\boldsymbol{A}$ and $\boldsymbol{B}$ is the matrix $\boldsymbol{C}$, formed by the substitution of element a_{ij} of the matrix $\boldsymbol{A}$ by the product $a_{ij}\boldsymbol{B}$.

Questions for self-examination.

1. Give a definition of a number and a digit.

2. What is the difference between the number and the digit?

3. Define the mathematical sign.

4. Give the definition of natural numbers and the notation of the set of natural numbers.

5. What distinguishes of the extended natural number series from the usual natural number series?

6. How to denote the divisibility of natural numbers without a remainder?

7. Which numbers are proper and improper divisors of a natural number n?

8. Give definitions of prime and composite numbers.

9. How common divisors of sets of natural numbers are defined?

10. What numbers are called coprime?

11. The greatest common divisor (GCD) of the set of natural numbers;

definition and properties.

12. What is the GCD of coprime numbers?

13. Give a definition of the number system.

14. What are the main classes of number systems.

15. Define non-positional and a positional number systems.

16. Give examples non-positional and positional notation.

17. What is the radix of a number system?

18. What are elementary numbers of an m −ary positional number system.

19. Give the definition of the digit of the number in positional notation.

20. Which combination of numbers is the basis of the m-ary positioning number system.

21. What is the residue of the number n modulo m?

22. Formulate the algorithm of translation of an integer from one position number system to another.

23. What is the essence of the cyclic shift or circular scrolling of a code?

24. Explain the concept of p −ary power-law number system.

25. What two numbers are called *congruent modulo* m?

26. What is a residue class modulo m?

27. How residues of negative numbers modulo m are formed?

28. Give the definition of a complete system of residues modulo p.

29. How the quadratic residues and quadratic non-residues are defining?

30. What percentage of quadratic residues and non-residues in the complete system of non-zero residues modulo p?

31. What is the feature of the bit-wise operations in modular arithmetic?

32. What is the XOR operator?

33. Give designations of major operators of modular arithmetic.

34. Make a Cayley table for the addition operation for a given modulo.

35. Make a Cayley table for the subtraction of a given modulo.

36. Make a Cayley table for the multiplication of a given modulo.

37. Make a table Cayley for the division operation of a given modulo p.

38. Give the definition of the Euler totient function.

39. What is the feature of a modular matrix?

40. Formulate distribution and associative laws of arithmetic for modular matrices.

41. What are the conditions of existence of inverse modular matrix?

42. What is the Kronecker product of two matrices?

43. What is the feature of Kronecker product of modular matrices?

2. IRREDUCIBLE POLYNOMIALS

Irreducible polynomials play a key role in the theory of modular algebra, and in other relevant sections of discrete mathematics. These include the theory of error-correcting coding and cryptographic protection of information, that is, precisely those sections of mathematics, the presentation of the basic foundations of which are devoted to this manual.

2.1. Basic concepts and definitions

The *polynomial* $f_n(x)$ *of one variable* x is called a finite formal sum of the form

$$f_n(x) = \sum_{i=0}^{n} \alpha_i x^i, \qquad (2.1)$$

where $x-$ *polynomial variable,* α_i- *coefficients of the polynomial* and $n-$ parameter, which is the *degree of the polynomial*.

Exceptionally such polynomials depending only on one variable, will be the subject of further consideration.

We represent the polynomial (2.1) in expanded form (in the form of an *expansion*)

$$f_n(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \ldots + \alpha_k x^k + \ldots + \alpha_1 x^1 + \alpha_0 x^0. \qquad (2.2)$$

According to (2.1) a polynomial is the algebraic sum of *monomials* $\alpha_k x^k$, $k = \overline{0, n}$. In turn, the monomial is the product of the coefficient (a positive integer or element of a field or alphabetic character) α_k and the formal variable x in degree k The expansion (2.2) is the canonical record of the polynomial and it is believed that $\alpha_0 x^0 = \alpha_0$. A polynomial whose leading coefficient α_n is equal one, is called *unital* (normalized, reduced) polynomial.

If the coefficient $\alpha_n \neq 1$, but greater than zero, in order to lead to a unital polynomial form, it sufficed to divide each of its coefficient α_k by α_n. In modular space this normalization of polynomials is feasible if only the coefficients α_k belongs to the set Z_p, i.e. $\alpha_k \in Z_p$, $k = \overline{0, n}$ where p – prime number.

Polynomials are frequently used for representation of numbers in positional notation systems for some base (module) m. The idea of representation $m-$ ary number of the polynomial is as follows. Radix m is replaced by a dummy (artificial, symbolic) variable, e.g. x. Power k of this variable x will correspond to the number of the digit of the number (numbering of digits is done from right to left, starting from the zero digit), and the coefficient α_k — the value of the digit.

Let us write, as an example, an octal number and its decomposition as a sum of powers of the seven:

$$602501_7 = 6 \cdot 7^5 + 0 \cdot 7^4 + 2 \cdot 7^3 + 5 \cdot 7^2 + 0 \cdot 7^1 + 1 \cdot 7^0.$$

Now replace the seven on a dummy variable x, in this case we obtain the expression

$$6 \cdot x^5 + 0 \cdot x^4 + 2 \cdot x^3 + 5 \cdot x^2 + 0 \cdot x^1 + 1 \cdot x^0.$$

Excluding monomials with zero coefficient, we arrive to a *polynomial representation* of the number

$$6 \cdot x^5 + 2 \cdot x^3 + 5 \cdot x^2 + 1 \cdot x^0.$$

The polynomial (2.2) quite unambiguously can be represented by the sequence of its coefficients α_k, including zero values, in this form

$$f_n = \alpha_n \alpha_{n-1} \ldots \alpha_k \ldots \alpha_1 \alpha_0. \qquad (2.3)$$

According to (2.3) the number of bits of the polynomial is one greater than its degree.

Expression (2.2) is a *complete form of the polynomial*, and (2.3) - its *shortened form*. The form (2.2) is often called a *polynomial form*. However, in order to avoid combinations like "oil oil", we will use *the full term of the polynomial form*, sometimes - algebraic polynomial form, thereby eliminating the "clumsy" statement such as – *polynomial form of a polynomial*. Reduction of the polynomial form (2.3) will also be called *vector form of the polynomial*.

The polynomial may be written in the *canonical form*

$$\alpha_n x^n + \alpha_{n-1} x^{n-1} + \ldots + \alpha_k x^k + \ldots + \alpha_1 x^1 + \alpha_0$$

i.e. in descending order, or in order of ascending powers

$$\alpha_0 + \alpha_1 x^1 + \ldots + \alpha_k x^k + \ldots + \alpha_{n-1} x^{n-1} + \alpha_n x^n .$$

Two polynomials are equal if they are made up (in descending order or ascending degrees) of the same monomials, i.e.

$$\alpha_n x^n + \alpha_{n-1} x^{n-1} + \ldots + \alpha_0 = \beta_n x^n + \beta_{n-1} x^{n-1} + \ldots + \beta_0$$

or

$$\alpha_0 + \alpha_1 x^1 + \ldots + \alpha_n x^n = \beta_0 + \beta_1 x^1 + \ldots + \beta_n x^n$$

if and only if $\alpha_k = \beta_k$, $k = \overline{0, n}$.

2.2. Modular arithmetic operations with polynomials

Over two polynomials (number 2 of polynomials is chosen for simplicity), we denote them $P_1(x)$ and $P_2(x)$, can be performed *modular arithmetic operations* of addition, subtraction, multiplication and division. In order to emphasize the distinction between *conventional* and *modular* arithmetic operations, illustrate their parallel by computing with specific examples.

2.2.1. The algebraic sum of polynomials

If there are two polynomials $P_1(x)$ and $P_2(x)$ of arbitrary degrees, their simple algebraic summation (addition or subtraction) is reduced to the corresponding summation of the coefficients of the monomials of the same degree k. The degree of the polynomial sum (difference) is obviously equal to the greater of the degrees, if only the leading coefficients of the respective summation is not reduced, then the actual degree of the sum may be less then the formal (in most of the degrees of polynomials-terms).

Let radix $m = p = 5$ and

$$P_1(x) = 2x^3 + x - 3;\ P_2(x) = 4x^2 + x + 1. \qquad (2.4)$$

We associate with ordinary polynomials $P_1(x)$ and $P_2(x)$ their unital modular equivalents positive monomials. To this end, firstly, transform in the polynomial $P_1(x)$ negative monomial -3 to positive, using the formula $(-k)_m = m-k$, according to which $(-3)_5 = 2$.

$$P_1(x) = 2x^3 + x + 3;\ P_2(x) = 4x^2 + x + 1.$$

And, secondly, to normalize the polynomials dividing modulo 5 numerical coefficients of monomials $P_1(x)$ by 2, and $P_2(x)$ by 4, bearing in mind that $(1/2)_5 = 3$ a $(1/4)_5 = 4.$ We come to such expressions, by expanding the modular notations of polynomials by "caps".

$$\hat{P}_1(x) = x^3 + 3x + 1 \text{ and } \hat{P}_2(x) = x^2 + 4x + 4. \qquad (2.5)$$

In the usual addition of polynomials (2.4)

$$\begin{aligned} P_1(x) + P_2(x) = 2x^3 &+ x - 3 + \\ &+ 4x^2 + x + 1 = \\ &= 2x^3 + 4x^2 + 2x - 2, \end{aligned}$$

whereas subtraction leads to this result

$$\begin{aligned} P_1(x) - P_2(x) = (2x^3 &+ x - 3) - \\ &- (4x^2 + x + 1) = \\ &= 2x^3 - 4x^2 - 4. \end{aligned}$$

By the modulo addition of polynomials (2.5)

$$\begin{aligned} (\hat{P}_1(x) + \hat{P}_2(x))_5 = x^3 &+ 3x + 1 + \\ &+ x^2 + 4x + 4 = \\ &= x^3 + x^2 + 2x, \end{aligned}$$

and by subtracting

$$\begin{aligned} (\hat{P}_1(x) - \hat{P}_2(x))_5 = (x^3 &+ 3x + 1) - \\ &- (x^2 + 4x + 4) = \\ &= x^3 + 4x^2 + 4x + 2. \end{aligned}$$

These examples illustrate the difference in operation is simple and modular summation modulo $m = 5$.

Because in the future we will be dealing primarily with binary polynomials, show performance of the summation operations on such polynomials. Feature of algebraic operations in a binary modular space manifested in the fact that the subtraction operation coincides with is the addition operation, - that is a sign - can be replaced by the sign +, which simplifies the calculations.

So, for $m = p = 2$, let

$$f_3(x) = x^3 + x + 1 \text{ and } f_2(x) = x^2 + x + 1. \qquad (2.6)$$

Then

$$f_3(x) \pm f_2(x) = (x^3 + x + 1) + \\ + (x^2 + x + 1) = x^3 + x^2 + 2x + 2 = x^3 + x^2,$$

as the two younger monomial of the polynomial of sum reset to zero.

2.2.2. Multiplication of polynomials

When multiplying polynomials each term of the polynomial is multiplied by each term of the other, and then (or in the process of multiplication) reduce similar terms (i.e, add up the coefficients of the same degrees of monomials). The degree of the polynomial-product is equal to the sum of the degrees-factors of polynomials.

For these polynomials (2.4) in ordinary multiplication

$$P_1(x) \cdot P_2(x) = (2x^3 + x - 3) \cdot (4x^2 + x + 1) = \\ = 8x^5 + 2x^4 + \underline{2x^3} + \underline{4x^3} + \underline{\underline{x^2}} + \bar{x} - \underline{\underline{12x^2}} - \overline{3x} - 3 = \\ = 8x^5 + 2x^4 + 6x^3 - 11x^2 - 2x - 3,$$

whereas under the modular multiplication of polynomials for the same (2.5)

$$(\hat{P}_1(x) \cdot \hat{P}_2(x))_5 = (x^3 + 3x + 1) \cdot (x^2 + 4x + 4) \\ = x^5 + 4x^4 + \underline{4x^3} + \underline{3x^3} + \underline{\underline{12x^2}} + \overline{12x} + \underline{\underline{x^2}} + \overline{4x} + 4 = \\ = (x^5 + 4x^4 + 7x^3 + 13x^2 + 16x + 4)_5 = \\ = x^5 + 4x^4 + 2x^3 + 3x^2 + x + 4,$$

and binary polynomial (2.6) we have

$$f_3(x)\cdot f_2(x)=(x^3+x+1)\cdot(x^2+x+1)=$$
$$=x^5+x^4+\underline{x^3}+\underline{x^3}+\underline{\underline{x^2}}+\overline{x}+\underline{\underline{x^2}}+\overline{x}+1=$$
$$=x^5+x^4+1.$$

2.2.3. Division of polynomials

The result of the division operation of two polynomials $A(x)$ and $B(x)$ can be written as

$$\frac{A(x)}{B(x)}=C(x)+\frac{D(x)}{B(x)}, \qquad (2.7)$$

where $C(x)-$is the polynomial-quotient, $D(x)-$ polynomial-residual (its degree less than the degree of the polynomial-divider $B(x)$).

If the degree of the polynomial-divisible $A(x)$ less than the degree of the polynomial divider $B(x)$, then the polynomial-quotient $C(x)$ will be absent. In this case $D(x)=A(x)$. Consider the situation where the degree of $A(x)$ greater than or equal the degree of $B(x)$. We introduce the notation Sp for the degree of the polynomial $P(x)$. Let's start with a certain degrees Sc and Sd of polynomials $C(x)$ and $D(x)$ respectively. Degree Sd will be formally equal $Sd=Sb-1$, but it can actually be less down to zero because it is not excluded, for example, the polynomial $A(x)$ divided by $B(x)$ without a reminder. Then $D(x)=0$.

To calculate coefficients of polynomial $C(x)$ and $D(x)$ look at an example. Let $Sa=3$, $Sb=2$. Then, according to (2.7), we can write $Sc=Sa-Sb=1$, $Sd=Sb-1=1$. We have

$$\frac{A(x)}{B(x)}=\frac{a_3x^3+a_2x^2+a_1x+a_0}{b_2x^2+b_1x+b_0}=c_1x+c_0+\frac{d_1x+d_0}{b_2x^2+b_1x+b_0}. \qquad (2.8)$$

Multiplying equation (2.8) by a polynomial $b_2x^2+b_1x+b_0$, we get

$$(c_1x+c_0)\cdot(b_2x^2+b_1x+b_0)+(d_1x+d_0)=$$
$$=a_3x^3+a_2x^2+a_1x+a_0. \qquad (2.9)$$

We open the brackets, we reduce these and equating the coefficients of equal degrees of the left and right sides of the equality (2.9)

$$
\begin{aligned}
x^3: &\quad c_1 b_2 = a_3, \\
x^2: &\quad c_1 b_1 + c_0 b_2 = a_2, \\
x^1: &\quad c_1 b_0 + c_0 b_1 + d_1 = a_1, \\
x^0: &\quad c_0 b_0 + d_0 = a_0.
\end{aligned}
\tag{2.10}
$$

The system of relations (2.10) can be regarded as a system of equations for the unknown coefficients of polynomials $C(x)$ and $D(x)$. Pay attention to the following facts. At first, the system splits into two independent systems, namely: equations

$$
\begin{aligned}
x^3: &\quad c_1 b_2 = a_3, \\
x^2: &\quad c_1 b_1 + c_0 b_2 = a_2,
\end{aligned}
\tag{2.11}
$$

contain as unknown variables the coefficients c_0 and c_1 of the polynomial $C(x)$, and the following two equations

$$
\begin{aligned}
x^1: &\quad c_1 b_0 + c_0 b_1 + d_1 = a_1, \\
x^0: &\quad c_0 b_0 + d_0 = a_0,
\end{aligned}
\tag{2.12}
$$

besides c_0 and c_1 contain unknown coefficients d_0 and d_1 of the polynomial $D(x)$.

And, secondly, it is natural that we should first solve the subsystem (2.11), that is, to determine c_0 and c_1, and then having the coefficients $C(x)$, of the subsystem (2.12) to find the coefficients d_0 and d_1 of the polynomial $D(x)$.

Concretize coefficients of polynomial $A(x)$ and $B(x)$ of this example in respect with modular division operations (2.7) by setting the radix (modulo) equal to five, and the coefficients

$$
\begin{aligned}
&a_0 = 3; \quad a_1 = 2; \quad a_2 = 1; \quad a_3 = 4; \\
&b_0 = 2; \quad b_1 = 1; \quad b_2 = 3.
\end{aligned}
\tag{2.13}
$$

Solving the system of equations (2.11) with respect to the unknown coefficients c_0 and c_1 taking into account the relations (2.13), we obtain

$$c_1 = \left(\frac{a_3}{b_2}\right)_5 = \left(\frac{4}{3}\right)_5 = (4\cdot 2)_5 = 3;$$
$$c_0 = \left(\frac{a_2 - c_1 b_1}{b_2}\right)_5 = \left(\frac{1-3}{3}\right)_5 = \left(\frac{-2}{3}\right)_5 = 1. \qquad (2.14)$$

Substituting value (2.14) in the system of equations (2.12) and taking into account values (2.13), we find the remaining coefficients

$$d_0 = \left(a_0 - c_0 b_0\right)_5 = (3-2)_5 = 1;$$
$$d_1 = \left(a_1 - (c_1 b_0 + c_0 b_1)_5\right)_5 = \left(2 - \left(3\cdot 2 + 1\right)_5\right)_5 = (2-2)_5 = 0. \qquad (2.15)$$

Calculated in (2.14) and (2.15) coefficients of $C(x)$ and $D(x)$ make it possible to present the result of the division operation (2.8) of two polynomials $A(x)$ and $B(x)$ as such

$$\frac{A(x)}{B(x)} = 3x + 1 + \frac{1}{3x^2 + x + 2}. \qquad (2.16)$$

By the expression (2.16) can be obtained, and other known method: polynomial division "into a column" or "corner". Recall the essence of this method. First recorded divisible polynomial of degree greater or equal than the polynomial divider, step back from him enough space and through the traditional "corner", as in long division, the polynomial divisor is written. The site will be recorded under the dash particular, the terms of the result of the private written in the form of monomials equal monomial the extent to which you need to multiply the monomial senior divider to get senior monomial of the dividend. In another recorded monomial private multiplied each term of the polynomial divider; the result is recorded a polynomial dividend and between them there is subtraction, with the remainder of the division already has a degree less than the original polynomial is divisible. To the resulting polynomial is applied the same operation, by adding to a polynomial-private monomial of another, as long as the new degree polynomial divider is less than the degree of the divisor polynomial. After successful completion of the algorithm result of the division of two polynomials is the sum of the polynomial obtained in the algorithm in a private cell, and fractions of the polynomial, the remainder divided by the initial divider.

To illustrate the modular division algorithm of the polynomials by a "corner" referring to the example (2.8), keeping for it previously selected parameters (2.13) and $m=5$. So, we have

$$\begin{array}{l|l} 4x^3+x^2+2x+3 & \underline{3x^2+x+2} \\ \underline{4x^3+3x^2+x} & 3x+1 \leftarrow \cdots \textit{quotient C(x)} \\ \quad 3x^2+x+3 & \\ \quad \underline{3x^2+x+2} & \\ \qquad\qquad 1 \leftarrow \cdots \textit{residue D(x)} & \end{array}$$

Under the dash in the scheme of dividing by a "corner" (2.17) recorded differences of the two upstream dashes polynomials. We note that the difference of monomials x^2 and $3x^2$ (2.17) is equal to $3x^2$, because the

$$(x^2-3x^2)_5=(1-3)_5\cdot x^2=(-2)_5\cdot x^2=3x^2.$$

As you can see, the results of the modular division (2.16) and (2.17) agree that confirms the correctness of calculations.

2.3. Irreducible and primitive polynomials

The set of polynomials in one variable over the given field form two disjoint subsets: *reducible* (or decomposable into prime factors, which are prime polynomials) and *irreducible* (indecomposable on prime factors) polynomials.

The polynomial of degree $n>1$ over the given field is called ***reducible*** if it can be represented as a product of two polynomials of lesser degrees $m>0$ and $l>0$ respectively.

Irreducible or ***prime*** are those unital polynomials that are not constants and which can not be represented as a product of two polynomials of lesser degrees $m>0$ and $l>0$ respectively.

It is possible to formulate a notion of the irreducible polynomial over the given field a little differently. Namely, *irreducible is called a polynomial, which has no other divisors other than trivial*. By the trivial divisors of the polynomial it is understand the polynomial himself and units of the field. Thus, we can say that the irreducible polynomials (IP) play a role similar to prime numbers. At the same time, *reducible is a polynomial which has at least one non-trivial divisor*.

Irreducible polynomials f determined by a number of basic numerical parameters, such as *the characteristic, degree* and *order* of polynomials, denoted by p, *deg* and *ord* respectively.

Coefficients α_i of the irreducible polynomial f_n degree n such that $\alpha_i \in Z_p$, $i = \overline{0, n}$, i.e. belong to the set of residues modulo a prime number p. Numbers of the set $Z_p = \{0, 1, \ldots, p-1\}$ form (see. Section 3) a prime Galois field $GF(p)$, referred to as F_p. Consequently, for coefficients α_i of the of the polynomial next relations hold:

$$\alpha_i \in GF(p) = F_p = Z_p,\ i = \overline{0, n}. \qquad (2.18)$$

Concerning IP it is accepted to speak that it is an irreducible polynomial over F_p. In this case it means that the coefficients α_i of the polynomial satisfy the condition (2.18).

Parameter *p* of the IP similar to the same parameter of the Galois field will be called where it would be appropriate, *characteristics* of the irreducible polynomial. The proposed parameter of the IP is not one universally accepted and introduced us to simplify the wording of certain definitions.

Characteristic p of an IP must be a prime number in view of the following reasons. Let $f_n(x)$ be an irreducible polynomial with coefficients $\alpha_i \in Z_m$, $i = \overline{0, n}$, and the leading coefficient $\alpha_n \geq 1$. Let m – be the parameter, which is a modulus. Normalization of the polynomial, which is carried out by dividing all coefficients α_i on α_n, may be carried out only if the modulus is a prime number.

The degree** (deg) **of the irreducible polynomial is the maximum degree of the polynomial monomials with nonzero coefficients.

The order of the polynomial (*ord*), sometimes also referred to its *index*, *period* or *exponent* is the smallest positive integer e, under which the given polynomial $f_n(x)$ divides (without reminder) the binomial $x^e - 1$.

In the set of irreducible polynomials there exists a subset of so-called *primitive polynomials*, which play an important role in coding theory and in cryptography. We discuss below some of the features of the concept of "primitive polynomial" (PP) and give it the treatment somewhat different from the generally accepted.

In the literature on the theory of error-correcting coding, given next definition of a PP. Irreducible over $GF(p)$ polynomial f_n of degree n is called primitive if its *root* (the definition of the "root" of the polynomial is given below in the text) is a *primitive element* of the extended field $GF(p^n)$ characteristics p. In turn, "primitive" is an element c of the field, which generates the multiplicative group $\langle c \rangle$ of maximum order (period). This means that the sequence of powers of a primitive element c, starting at first degree, in the ring of residues modulo f_n includes all non-zero elements of the Galois extension of the field (see. Sections 3 and 4).

And, finally, briefly explain the term "a root of the polynomial ".

The root of

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

over the field F_p – this an element $c \in F_p$ (or an element of the extension $GF(p^n)$), such that the following two equivalent conditions are satisfied:

1) the polynomial $f_n(x)$ is divided by the binomial $x - c$;

2) the substitution of the element c instead x reduces the polynomial $f_n(x)$ to the identity, that is,

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

In a number of cryptographic source the concept of PP is introduced as follows. An irreducible polynomial $f_n(x)$ with coefficients $\alpha_n = 1$, $\alpha_i \in GF(p)$, $i = \overline{0, n-1}$, is primitive if it divides without reminder the binomial $x^e - 1$, provided that the minimum positive e is given by the expression

$$\min e = p^n - 1.$$

In the classical theory of finite fields the notion of the primitive polynomial is defined by the following manner: the polynomial $f_n(x)$ of degree n is a primitive polynomial over $GF(p)$ if it is the irreducible polynomial such that $f_n \neq 0$ and $ord\ f_n = p^n - 1$.

There is no contradiction between these definitions of PP. In fact, they are one and the same, that will explain further clarifying the physical meaning of the term "primitive polynomial".

Give here (see Table 2.1.) the complete list of binary irreducible polynomials f_8 of eight degree. Let $\theta_{\min}$ – be the minimal generating primitive element, the sequence of powers of which modulo IP f_8 consists a full set of nonzero vectors of the eighth order, which we call the *multiplicative group* (or sequence) of the *maximum order* (MPGMO) and is denoted by $GF^*(p^n)$, where p – characteristic of the field.

Table 2.1. The irreducible binary polynomials of eight degree

№	Value of the polynomial	$\theta_{\min}$	№	Value of the polynomial	$\theta_{\min}$	№	Value of the polynomial	$\theta_{\min}$
1	100011011	11	11	101101001	10	21	110110001	110
2	100011101	10	12	101110001	10	22	110111101	111
3	100101011	10	13	101110111	11	23	111000011	10
4	100101101	10	14	101111011	1001	24	111001111	10
5	100111001	11	15	110000111	10	25	111010111	111
6	100111111	11	16	110001011	110	26	111011101	111
7	101001101	10	17	110001101	10	27	111100111	10
8	101011111	10	18	110011111	11	28	111110011	110
9	101100011	10	19	110100011	101	29	111110101	10
10	101100101	10	20	110101001	10	30	111111001	11

Shading in Table. 2.1 primitive polynomials are distinguished. f_8. Bold type minimum primitive elements $\theta_{\min}$ are distinguished. The $\theta_{\min}$ are forming MPGMO that meet a couple ($f_8, \theta_{\min}$).

Definition 2.1. *Sequence* a_k, $k = 0, 1, 2, \ldots$, of *degrees of forming element* α *(i.e. the sequence* $a_k = \alpha^k$*, starting with zero degree) shown to the residue modulo the irreducible polynomial* f_n of *characteristics* p, *we will call multiplicative sequence generated by the element* α *over IP* f_n of *degrees* n.

Thus, the multiplicative sequence (MS) is nothing more than a

$$a_k = \alpha^k \pmod{f_n},\ k = 0, 1, 2, \ldots$$

The number of different elements of the multiplicative sequence called the *order of the sequence*, for which we introduce the designation *L*. The maximal order of the multiplicative sequence is achieved if

$$L = p^n - 1, \qquad (2.19)$$

where $p-$ characteristic of irreducible polynomial f_n, and $n-$ his degree.

In table. 2.2 MS which formed by generating element (GE) $\alpha = 10$ over binary irreducible polynomial fourth degree $f_4^{(1)} = 10011$, $f_4^{(2)} = 11001$ and $f_4^{(3)} = 11111$ are given. The first two polynomials $f_4^{(1)}$ and $f_4^{(2)}$ are primitive polynomials then the third $f_4^{(3)}$ - only irreducible but not primitive.

Consider irreducible polynomials of characteristic $p = 3$. Table. 2.3 shows, for example, the unital IP of fourth degree over F_3 and corresponding minimum primitive elements $\theta_{\min}$, generating MPGMO $GF^*(3^4)$. Shading and bolding in the table. 2.3 are made by the same rules as in the Table. 2.1.

Table 2.2. Multiplicative sequences formed by GE $\alpha = 10$ NP over the polynomial of fourth degree

k	$f_4^{(1)} = 10011$					$f_4^{(2)} = 11001$					$f_4^{(3)} = 11111$			
	3	2	1	0		3	2	1	0		3	2	1	0
0	0	0	0	1		0	0	0	1		0	0	0	1
1	0	0	1	0		0	0	1	0		0	0	1	0
2	0	1	0	0		0	1	0	0		0	1	0	0
3	1	0	0	0		1	0	0	0		1	0	0	0
4	0	0	1	1		1	0	0	1		1	1	1	1
5	0	1	1	0		1	0	1	1		0	0	0	1
6	1	1	0	0		1	1	1	1					
7	1	0	1	1		0	1	1	1					
8	0	1	0	1		1	1	1	0					
9	1	0	1	0		0	1	0	1					
10	0	1	1	1		1	0	1	0					
11	1	1	1	0		1	1	0	1					
12	1	1	1	1		0	0	1	1					
13	1	1	0	1		0	1	1	0					
14	1	0	0	1		1	1	0	0					
15	0	0	0	1		0	0	0	1					

Table 2.3. Irreducible polynomials of fourth degree over F_3

№	Value polynomial	θ_{min}	№	Value polynomial	θ_{min}	№	Value polynomial	θ_{min}
1	10012	10	7	11002	10	13	12002	10
2	10022	10	8	11021	11	14	12011	11
3	10102	110	9	11101	101	15	12101	101
4	10111	11	10	11111	12	16	12112	10
5	10121	12	11	11122	10	17	12121	11
6	10202	11	12	11222	10	18	12212	10

We draw attention to the fact that the primitive polynomials shown in Tab. 2.1 and 2.3, meet the minimum primitive elements $\theta_{min}=10$, generating MPGMO. Section 1 shows (see Table. 1.1) that in any number system the radix m is recorded as a combination of numbers 10. As a consequence, the characteristic p, which is the basis of the number system for the coefficients α_k of the IP f, is also equal to 10.

Let ω be the generating element (GE) of a multiplicative group (MPG), formed by the irreducible polynomial f of degrees n and characteristics p. Then $(k+1)-$ th degree of GE ω, as a component of MPG can be represented by the relation $\omega^{k+1}=\omega^k\cdot\omega$. If $\omega=p=10$, then each subsequent component ω^{k+1} of MPG is created by shifting the previous components ω^k by one bit to the left (as the result of multiplication on $p-$ ary number 10). If it turns out that the highest non-zero digit of the number ω^{k+1} is shifted in $(n+1)-$ digit (the first digit - the extreme right), the number of ω^{k+1} is the residue modulo f_n.

Based on the foregoing, we introduce such an empirically validated by data of Table. 2.1 and 2.3, the definition of a PP.

Primitive polynomial is irreducible over F_p polynomial f of degree n, forming the multiplicative group of maximum order p^n-1, minimum generating element of which coincides with the characteristic of IP p, i.e. $\theta_{min}=p=10$.

There is another version of the definition PP.

By a ***primitive*** *polynomial* we call irreducible over F_p polynomial f of degrees n, generating an extended Galois field $GF(p^n)$, the minimum primitive element θ_{min} of which coincides with the characteristic of the field p.

Both of these definitions of PP are identical in meaning and directly disclose the *physical meaning* of the term "primitive polynomial".

And in the conclusion of the section, we note that any primitive polynomial is irreducible, while not every irreducible polynomial is primitive.

Primitive polynomials have the following main characteristics:

- if $f_n(x)$ is a primitive polynomial of degree n, then the polynomial $x^n f_n(1/x)$ is primitive polynomial;
- if $x^A + x^B + 1$ is the primitive polynomial, then the polynomial $x^A + x^{A-B} + 1$ the primitive polynomial;
- if $x^A + x^B + x^C + x^D + 1$ is the primitive polynomial, then the polynomial $x^A + x^{A-D} + x^{A-C} + x^{A-B} + 1$ is the primitive polynomial etc.

These relations make it possible, knowing a polynomial $f_n^{(1)}(x)$ of degrees n, calculate the other polynomial $f_n^{(2)}(x)$ the same degree simply.

Consider an example. Let $f_8 = 101100101$ be a primitive binary polynomial of degree eight, whose algebraic presentation has the form

$$f_8^{(1)}(x) = x^8 + x^6 + x^5 + x^2 + 1.$$

Using the third property of primitive polynomials, we obtain

$$f_8^{(2)}(x) = x^8 + x^6 + x^3 + x^2 + 1.$$

Both of these PP are part of the irreducible polynomials of degree eight, summarized in Table 2.1.

2.4. Main characteristics of irreducible polynomials

Recall that the *irreducible* is a polynomial f_n of degree n, which cannot be represented as the product of two polynomials of lower degree. In turn, if the polynomial f_n is *reducible*, then there is an expansion for it

$$f_n = f_k \cdot f_{n-k},\ 1 \le k < n. \qquad (2.20)$$

In solving the problem of synthesis of irreducible binary polynomials we will use their abbreviated (vector) forms as a sequences of coefficients α_k of their monomials, i.e.

$$f_n = \alpha_n \alpha_{n-1} \ldots \alpha_k \ldots \alpha_1 \alpha_0, \qquad (2.21)$$

where

$$\alpha_k \in F_2 = GF(2) = Z_2 = \{0,1\}.$$

To date, precise algorithms for the synthesis of PPs of higher degrees, which would not have expected some sorting and which are acceptable for practical application, have not yet been developed. A method of production of irreducible polynomials close to the procedure of generating of prime numbers and is as follows. It is generated $(n+1)-$ bit odd unital number that serves the equivalent of the reduced form of the irreducible polynomial $n-$ th degree (2.21), and a sequence of tests is performed on it, each of which confirms or refutes the hypothesis that the tested polynomial is an irreducible. But even for polynomials that have passed all tests, there is, albeit small, a probability that they can be factored (2.20) and, therefore, are not irreducible.

The complexity of the generation of irreducible polynomials increases exponentially with increasing degree of polynomials. Therefore, in Sec. 2.5 synthesis algorithm of binary irreducible polynomials in "manual mode" is proposed, and it is acceptable for the generation of polynomials of small degree.

We first formulate a series of simple propositions, useful for solving the problem of guaranteed construction of IP.

We introduce axiomatically irreducible polynomials of the first degree f_1, excluded from further consideration trivial degenerate polynomial of degree zero f_0, equal to one. There are two IP f_1, namely:

$$\begin{aligned} f_1^{(ч)} &= 10_2 = 2_{10} - \text{even polynomial,} \\ f_1^{(н)} &= 11_2 = 3_{10} - \text{odd polynomial.} \end{aligned} \qquad (2.22)$$

We show that any binary irreducible polynomial f_n of degree n satisfies the following theorem.

Theorem 2.1. *A binary polynomial f_n of degree n if and only if is the irreducible polynomial if it is an odd unital with odd weight (**necessary conditions**) which does not allow an expansion in the product of two or more polynomials of smaller degrees of (**sufficient condition**).*

Proof of Theorem 2.1 will begin by confirming of the *necessary conditions* for irreducibility of polynomials. The requirement that the *candidate polynomial be odd* (and this becomes a polynomial ending with unity) is in fact an axiomatic since if the polynomial is even, that is, it ends with zero, then it means that it is divisible by at least an even polynomial $f_1^{(ч)} = 10$ of the first degree. In this case f_n – decomposable polynomial and, thus, becomes reducible. Condition of *the polynomial unitality*, suggesting that its leading coefficient $\alpha_n = 1$, inherent in the polynomial by definition.

Finally, in order to confirm that the *weight of an irreducible polynomial must be odd* (by weight ν_f is understood the number of ones contained in the polynomial f_n) introduce and prove such an auxiliary Assertion.

Assertion 2.1. *If the weight* ν_f *of polynomial* f_n *is an even number, then such a polynomial is divisible without a remainder, at least on an odd polynomial of the first degree* $f_1^{(н)} = 11$.

Proof. Consider first as a polynomial $f_n^{(2)}$ *the binomial* $f_n(x) = x^n + 1$, whose reduced form has the form

$$f_n^{(2)} = 1\underbrace{00\ldots0}_{(n-1)\,times}1. \qquad (2.23)$$

The weight ν_f of the polynomial (2.23) is even, equal to two. Having completed the first step of "corner" dividing of a given polynomial by a polynomial $f_1^{(н)} = 11$, we get

$$\begin{array}{llllll|l} \mathbf{1} & \mathbf{0} & 0 & \ldots & 0 & & 1\ \ 1 \\ \underline{1\ \ 1} & \downarrow & & & & & \\ \mathbf{1} & \mathbf{0} & & & & & 1 \end{array} \qquad (2.24)$$

As follows from the dividing stage (2.24) to each zero in the relation (2.23) corresponds (after the demolition of another zero) partial dividend 10 allocated in (2.24) in bold type. Continuing the procedure for dividing the polynomial $f_n^{(2)}$ by the scheme (2.24), we arrive at the residual division, in which the last zero of the polynomial (2.23) is involved

$$\begin{array}{cccc|c} \mathbf{1} & \mathbf{0} & 1 & & 1\ \ 1 \\ \hline 1 & 1 & \downarrow & & 1\cdots 1 \\ \hline & \mathbf{1} & \mathbf{1} & & \end{array}$$

Thus, it becomes clear that an odd polynomial of the first degree $f_1^{(н)} = 11$ with even weight $\nu_f = 2$ divides the polynomial (2.23) without a remainder.

Complete quotient q, generated by the scheme (2.24), is

$$q = \underbrace{11\ldots1}_{(n-1)\ times} = 1^{[n-1]},$$

where $\lambda^{[k]}$ means $k-$ multiple digits λ.

And now we turn to the odd polynomial of degree n with weight ν_f, equal to four, denoting it through $f_n^{(4)}$. Polynomial $f_n^{(4)}$ can be represented in the form of a bitwise sum modulo 2 of an exterior odd polynomial $f_n^{(2)}$, which is given by the relation (2.23) and the inner even polynomial $f_m^{(2)}$, whose abbreviated form is as follows:

$$f_m^{(2)} = 1\overbrace{\underbrace{00\ldots0}_{k\ bits}\underbrace{10\ldots0}_{l\ bits}}^{m\ bits}, \qquad (2.25)$$

with $1 \le m \le (n-2)$, $l \ge 0$.

The polynomial (2.25) can be written in this form

$$f_m^{(2)} = f_k^{(2)} \cdot 0^{[l]}. \qquad (2.26)$$

The polynomial $f_k^{(2)}$, as follows from a comparison of the expressions (2.25) and (2.26), repeats the form of the polynomial $f_n^{(2)}$ *i.e.*

$$f_k^{(2)} = 1\underbrace{00\ldots0}_{(k-1)\ times}1. \qquad (2.27)$$

Consequently, the polynomial $f_1^{(н)} = 11$ divides both the polynomial (2.27) and the polynomials (2.25) and (2.26). Similarly, it can be shown that the polynomial $f_1^{(н)} = 11$ divides an odd polynomial $f_n^{(2k)}$ with even weight $\nu_f = 2k$,

$1 \le k \le \lfloor (n-1)/2 \rfloor$, where $\lfloor x \rfloor -$ the integer part of x. This completes the proof of both Proposition 2.1 and the conditions for the oddness of the weight of an IP in Theorem 2.1.

Prohibition of decomposition of the irreducible polynomial as a product of two or more polynomials of smaller degrees is a sufficient condition of an IP by definition.

Thus, we confirmed all the necessary and sufficient conditions Theorem 2.1, that is, the theorem is proved in its entierly.

We introduce the concept of the *dual irreducible polynomial*, called as *reciprocive* (*rarely* - conjugate) polynomial.

The dual irreducible polynomial of $n-$ th degree is called a polynomial $f_n^*(x)$, in which the order of the coefficients α_k of monomials is inverse with respect to the order of the coefficients of the original polynomial $f_n(x)$.

For example, if the original (primary) polynomial

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

indices k of coefficients α_k of monomials increase in the right-to-left direction, then in the dual polynomial

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

the indices of the monomial coefficients increase from left to right.

Primary and dual irreducible (primitive) polynomials are mutually reversible, that can display by the relation

$$f_n(x) \leftrightarrow f_n^*(x)$$

They are related by the following lemma.

Lemma 2.1. *The polynomial that is dual to the irreducible polynomial is irreducible, and a dual to primitive is primitive*.

Proof the lemma by the method of proof by contradiction on the example of a decomposable polynomial which is represented by the concatenation of two irreducible polynomials, such that

$$f_{n+1}(x) = f_k(x) \,||\, f_{n-k}(x). \qquad (2.28)$$

Let $n = 8;\ k = 4;\ f_k(x) = f_4(x) = 11111$ — be an irreducible polynomial of degree four and $f_{n-k}(x) = f_4(x) = 10011$ — be the primitive polynomial of degree four, so that

$$\overset{f_k \quad f_{n-k}}{f_{n+1} = 1111110011} \qquad (2.29)$$

becomes a *reducible polynomial* of the ninth degree.

Invert the bits of the polynomial (2.29), we arrive at the conjugate polynomial

$$\overset{f^*_{n-k} \quad f^*_k}{f^*_{n+1} = 1100111111} \qquad (2.30)$$

that gives the proof of Lemma 2.1, since f^*_k remains simply irreducible, and f^*_{n-k} – primitive polynomial.

From the comparison of polynomials (2.28) – (2.33) we obtain

$$f^*_{n+1}(x) = f^*_{n-k}(x) \,||\, f^*_k(x).$$

In a more general case, for the reduced form of a reducible polynomial if

$$f_{n+m-1} = f_{n_1} \,||\, f_{n_2} \,||\ldots||\, f_{n_m}$$

then

$$f^*_{n+m-1} = f^*_{n_m} \,||\, f^*_{n_{m-1}} \,||\ldots||\, f^*_{n_1},$$

where $n = \sum_{i=1}^{m} n_i$ and f_{n_k} – is the irreducible polynomial of degree n_k.

2.5. Synthesis of binary irreducible polynomials

By the formulae (2.22) two irreducible binary polynomials of the first degrees are introduced

$$f_1^{(1)} = 10 - \text{the even polynomial;}$$

$$f_1^{(2)} = 11 - \text{the odd polynomial,}$$

which are primitive polynomials.

Short form of a binary IP of $n-$th degree can be displayed in this form

$$f_n = 1\alpha_{n-1}\alpha_{n-2}\ldots\alpha_1 1. \qquad (2.31)$$

in which digits α_k, $k = \overline{1, n-1}$, must satisfy the conditions of Theorem 2.1 and Assertion 2.1, the most important of which (are due to the *conditions*) are that, first, the weight of the set of coefficients α_k *must be* an odd number and, secondly, the polynomial (2.31) *should not have* any other divisors, except trivial (that is, unit and the polynomial itself).

The last condition means that no one irreducible polynomial f_m of degree m such that $1 \le m \le \lfloor n/2 \rfloor$ can not be a divisor of the polynomial (2.31).

Carry out further synthesis procedure of irreducible polynomials of degree $n \ge 2$.

Irreducible polynomial of the second degree f_2 can be obtained on the basis of a particular variant of the abbreviated form (2.31), namely

$$f_2 = 1\,\alpha_1\,1. \qquad (2.32)$$

According to (2.32) as a coefficient α_1 only value 1 can be selected, since if $\alpha_1 = 0$, then the polynomial (2.32) becomes even in weight and, therefore, is divisible by a polynomial $f_1 = 11$. In this way,

$$f_2 = 111 \qquad (2.33)$$

is a unique irreducible polynomial of the second degree.

The multiplicative sequence of non-zero binary vectors the length of the two generator polynomials (2.33) over the forming element $\omega = 10$, is shown in Table. 2.4.

Table 2.4. The multiplicative sequence generated by the irreducible polynomial (2.33)

k	$f_2 = 111$	
	1	0
0	0	1
1	1	0
2	1	0
3	0	1

The length of the multiplicative sequence satisfies condition (2.19), and this means that the polynomial $f_2 = 111$ primitive.

Irreducible polynomials of the third degree f_3 meets the reduced form

$$f_3 = 1\,\alpha_2\,\alpha_1 1. \tag{2.34}$$

Taking into account the constraints on the coefficients $\alpha_2\,\alpha_1$ in (2.34), we obtain two polynomials

$$\begin{aligned} f_3^{(1)} &= 1011; \\ f_3^{(2)} &= 1101, \end{aligned} \tag{2.35}$$

and the multiplicative sequences formed by them over the generating element $\omega = 10$ are summarized in Table. 2.5.

Table 2.5. Multiplicative sequence generated by the MA $\alpha = 10$ over the third degree NP

k	$f_3^{(1)} = 1011$			$f_3^{(2)} = 1101$		
	2	2	1	0	1	0
0	0	0	1	0	0	1
1	0	1	0	0	1	0
2	1	0	0	1	0	0
3	0	1	1	1	0	1
4	1	1	0	1	1	1
5	1	1	1	0	1	1
6	1	0	1	1	1	0
7	0	0	1	0	0	1

As shown in Table. 2.5, the polynomials (2.35) are dual primitive polynomials.

Irreducible polynomials of degree four f_4 are calculated on the basis of their general reduced form

$$f_4 = 1\alpha_3\,\alpha_2\,\alpha_1 1. \tag{2.36}$$

The applicants of the inner polynomial in (2.36) include only such polynomials $f = \alpha_3\,\alpha_2\,\alpha_1$, whose weight ν_f is an odd number.

Table 2.6. The composition of polynomials f of odd-weighted

№	α_3	α_2	α_1		№	α_3	α_2	α_1
1	0	0	1		3	1	0	0
2	0	1	0		4	1	1	1

Only those fourth-degree polynomials (2.36) generated by internal polynomials $f_2^{(i)}$, $i=\overline{1,4}$, from Table. 2.6, become irreducible, which do not divide into a single irreducible polynomial of the second degree $f_2=111$.

Let us pay attention to the fact that the polynomials $f_2^{(1)}=001$ and $f_2^{(3)}=100$ are dual, therefore, the polynomial divisibility test f_2 only those polynomials f_4, for which the polynomials in Table 1 are internal. 2.6 under numbers 1 (or 3), 2 and 4. Using the division of binary polynomials by a "corner", we arrive at such results.

For a polynomial $f_4^{(1)}=10011$ we have

$$\begin{array}{lll} \textit{dividend} \longrightarrow & 1\ 0\ 0\ 1\ \mathbf{1} & \left|\begin{array}{l}\underline{1\ 1\ 1} \longleftarrow \textit{divisor}\\ 1\ 1\ 0 \longleftarrow \textit{quotient}\end{array}\right. \\ & \underline{1\ 1\ 1}\ \downarrow & \\ & \quad 1\ 1\ 1 & \\ & \quad \underline{1\ 1\ 1} & \\ & \qquad\quad \mathbf{1} \longleftarrow \textit{remainder} & \end{array} \qquad (2.37)$$

Recall that under the dash in the scheme of dividing the "area" (2.37) recorded the difference between the two upstream dashes polynomials. The bold identity in the divisible (2.37) is the remainder of the polynomial division $f_4^{(1)}$ on a polynomial $f_2=111$. Consequently, a polynomial of degree four $f_4^{(1)}=10011$ and together with it the dual polynomial $f_4^{(3)}=11001$ are irreducible polynomials.

In a similar way, the irreducibility of the polynomial $f_4^{(4)}=11111$, the remainder of dividing by a polynomial $f_2=111$ is equal to. It remains to test the divisibility of a polynomial $f_4^{(2)}=10101$. According to the "corner" scheme, we arrive at this result

$$
\begin{array}{lll}
\textit{dividend} \longrightarrow 1\ 0\ 1\ 0\ 1 & \big| & 1\ 1\ 1 \longleftarrow \textit{divisor} \\
\underline{1\ 1\ 1}\ \downarrow & & \underline{1\ 1\ 1} \longleftarrow \textit{quotient} \\
1\ 0\ 0 & & \\
\underline{1\ 1\ 1} & & \\
1\ 1\ 1 & & \\
\underline{1\ 1\ 1} & & \\
0\ 0\ 0 \longleftarrow \textit{remainder} & &
\end{array}
\qquad (2.38)
$$

According to (2.38), the polynomial $f_4^{(2)} = 10101$ is divisible by a polynomial $f_2 = 111$. Therefore $f_4^{(2)}$— reducible polynomial, and polynomials of the fourth degree turn out to be irreducible (we change the superscripts in them)

$$f_4^{(1)} = 10011;$$

$$f_4^{(3)} = 11111,$$

and also the polynomial $f_4^{(2)} = 11001$, which is a dual polynomial $f_4^{(1)}$.

Having made multiplicative sequence of irreducible fourth-degree polynomial for the forming element $\omega = 10$, we establish that the polynomials $f_4^{(1)}$ and $f_4^{(2)}$ are primitive (their order is 15), while the irreducible polynomial $f_4^{(3)}$ it is not primitive and its order is five.

A theoretical analysis of the algorithm can be used in solving the problem of synthesis of irreducible polynomials of any degree n. However, the limiting factor of this version of the synthesis of non-linear systems is the fact that as the degree of polynomials n exponentially increases the amount of necessary calculations.

Summary of the chapter

1. A polynomial (polynomial) is the algebraic sum of monomials (monomials).

2. Monomial - is the product of the coefficient and the degree of formal variable.

3. Complete the form of a polynomial is a sum of monomials.

4. The shortened form of a polynomial is formed by a sequence of decomposition coefficients of a polynomial, including their zero values.

5. Reduce of the polynomial form is a polynomial expansion coefficients sequence, including zero values.

6. The number of bits per unit of the polynomial degree is greater than he.

7. The degree of the irreducible polynomial - is included in the maximum degree of monomial polynomial with a non-zero coefficient.

8. The order of a polynomial is the smallest natural number e, under which the given polynomial $f_n(x)$ divide the remainder of the binomial $x^e - 1$.

9. The feature of algebraic operations in binary modular space is manifested in the fact that in it the subtraction operation coincides with the operation of addition, i.e. sign $-$ can be replaced by $+$.

10. reducibility of such polynomials are called, which can be represented as a product of at least two polynomials of lesser degree.

11. Irreducible or simply called such unitary polynomials, is not a constant, which can not be represented as a product of two polynomials of lesser degree.

12. Irreducible is a polynomial, which has no other divisors other than trivial.

13. Trivial divisors of a polynomial are unit and itself polynomial.

14. An irreducible polynomial over a prime Galois field is said to be primitive if its root α is a primitive element of the extended field $GF(p^n)$ characteristics p.

15. Primitive is such an element α the Galois field, which generates a multiplicative group of maximal order (period).

16. A sequence of degrees, starting with a zero degree, of a primitive element α in the residue ring modulo an irreducible polynomial f_n contains all nonzero elements of the field of the extended Galois field $GF(p^n)$.

17. The primitive polynomial is an irreducible polynomial F_p polynomial f degree n characteristics p (necessary conditions) generating the extended Galois field $GF(p^n)$, whose minimal primitive element $\theta_{\min}$ Coincides with the characteristic of the field p (sufficient conditions).

18. The primitive polynomial is an irreducible polynomial F_p polynomial f degree n characteristics p (necessary conditions) generating the extended Galois field $GF(p^n)$, whose minimal primitive element $\theta_{\min}$ Coincides with the characteristic of the field p (sufficient conditions).

19. Any primitive polynomial is an irreducible, while not every irreducible polynomial is primitive.

20. The binary polynomial of degree n if and only if the polynomial is irreducible if it is - an odd unitary polynomial with an odd weight (necessary conditions), does not allow expansion of the product of two or more polynomials of smaller degrees of (sufficient condition).

21. The dual (or conjugate) is called irreducible polynomial polynomial, which the order of the coefficients of the monomials is inverse of the initial order of sequence of coefficients polynomial.

22. The polynomial dual to irreducible is also irreducible, and dual to primitive is primitive.

23. Binary polynomials of the first degree are degenerate primitive polynomials.

24. The sequence of powers of the generator element α, starting with the zero power reduced to the remainder modulo an irreducible polynomial f_n characteristics p, is called the multiplicative sequence formed by the element α over the NP f_n degree n.

25. The number of different elements of the multiplicative sequence is the order of the sequence.

Questions for self-examination

1. Give the definition of the polynomial.

2. What is a monomial of the polynomial?

3. Write an example of a polynomial in the full and in the abbreviated forms.

4. What are called unitary polynomials?

5. Which condition must meet the coefficients in the modular space?

6. Explain the scheme of the reducing of the polynomial to the unitary form.

7. What is the feature of the operations of summation in the binary modular space?

8. Give the definition of reducible and irreducible polynomials.

9. What divisors of polynomials are trivial?

10. Explain the concept of "root of the polynomial" and what conditions must meet?

11. Explain the term "characteristic polynomial".

12. Which element of the Galois field is called primitive?

13. Give the definition of the "degree" and of the "order" of irreducible polynomials.

14. What does the term "primitive polynomial"?

15. What is the physical meaning of the primitive polynomial?

16. Formulate the necessary and sufficient conditions to be satisfied by irreducible binary polynomial.

17. What is the order of the multiplicative sequence?

18. Give a definition and examples of dual irreducible polynomial.

19. Is dual polynomial irreducible (primitive) if the original polynomial is irreducible (primitive)?

3. GROUPS, RINGS AND GALOIS FIELDS

Algebraic structures (systems) listed in the title are fundamental in the mathematical theory of error-correcting coding and cryptographic protection of information.

3.1. Basic concepts and definitions

Definition 3.1. *In mathematics, and more specifically in abstract algebra, an algebraic structure on a set A (called carrier set or underlying set) is a collection of finitary operations on A. Each operation has an arity. The set S of these operations is called the signature of the algebraic structure.*

The set A with this structure is also called an algebra of the signature S. Usually operations of the signature satisfy a certain system of axioms.

As sets of elements in algebraic structures serve numbers, characters, vectors, matrices and other objects. Over these objects n- ary operations are defined.

Definition 3.2. *Let A be an arbitrary non-empty set and $n-$ be a natural number. Any mapping $\tau: A^n \to A$ is called the n- ary operation on the set A.*

The mapping $\tau: A^n \to A$ should be understood as follows: a certain set of objects, consisting of n elements $a_1, a_2, \ldots, a_n$, belonging to the set A, which is written in the form $(a_1, \ldots, a_n) \in A^n, a_i \in A$ generates an element b of the same set A, i.e. $b \in A$.

Thus, according to the definition given above, n- ary operation correspond to each n-tuple – an unchangeable ordered sequence of elements $(a_1, a_2, \ldots, a_n) \in A^n$, uniquely matches element $b \in A$. Components $a_1, a_2, \ldots, a_n$ of the n-tuple $(a_1, \ldots, a_n)$ are called arguments of the operation τ, and b — the result of applying the operation to the arguments $a_1, a_2, \ldots, a_n$.

In other words, the *arity* of operations or functions in mathematics is the number of arguments, or operands. The word formed from the names of the small-

ary operations (unary - one argument, binary – two, ternary - three, etc.). Historically, the first appeared binary operations ($n=2$) and unary operations ($n=1$).

Informally speaking, *predicate* is the statement, in which you can substitute arguments. If the argument is one then the predicate expresses a property, if more arguments then the relation among the arguments.

For n-ary operation use the notation

$$b=\tau(a_1, a_2, \ldots, a_n) \text{ or } b=a_1, a_2, \ldots, a_n\tau$$

Usually, if $n=2$, then write $a_1 \tau\, a_2$. When $n=1$ and $n=2$ speak respectively about unary operation and about binary operation. Specifically, the notion of a nullary operation is defined (that is, for $n=0$). By a nullary operation on the set A understand an arbitrary fixed element of this set. An example of an unary (one-placed) operation is the operation of calculation of the inverse element (if exists) $\bar{a} \in A$ for the element a of the same set A.

The most important in algebra and, therefore, the most studied are binary operations. Examples of such operations might be the addition and multiplication of numbers, addition and multiplication of matrices, etc.

A brief definition of a binary algebraic operation can be formulated on the basis of the particular case $(n=2)$ of the Definition 3.2 for n-ary operation. Namely

Definition 3.3. *The binary algebraic operation (BAO), acting on the set A is called a mapping*

$$\tau: A^2 \to A.$$

Let us give further more detailed definition of the BAO.

Definition 3.4. *A binary algebraic operation on the set A is called a such mathematical operation «τ », which for any pair of elements a and b from A uniquely associates an element $c=a\tau b$, belonging to the same set, and called the composition or product of the elements a and b.*

Often, instead τ use another special character: $\circ, *, \cdot, \oplus, \otimes, +, -$ and so on. On the set A it is possible to specify many different operations. Wishing to single out one of them, parentheses are used $(A, \circ)$ and say that the operation $\circ$ defines the algebraic structure on A or $(A, \circ)$ is the algebraic structure (algebraic system).

A binary algebraic operation can have such important properties as associativity, commutativity and transitivity.

Definition 3.5. *Algebraic operation* $\circ$*, given on the set* A*, is said to be associative if for any elements* a_1, a_2 *and* a_3 *from* A *the equality is satisfied.*

$$(a_1 \circ a_2) \circ a_3 = a_1 \circ (a_2 \circ a_3).$$

If the operation $\circ$ has the associativity property, then we can omit the brackets and write $a_1 \circ a_2 \circ a_3$ instead $(a_1 \circ a_2) \circ a_3$ and $a_1 \circ (a_2 \circ a_3)$. For example, associative addition of natural numbers: for any natural numbers a_1, a_2 and a_3 the equality $(a_1 + a_2) + a_3 = a_1 + (a_2 + a_3)$ is satisfied.

There are algebraic operations which non-associative. For instance, subtraction is not associative for integers. For example, $(12-7)-3 \neq 12-(7-3)$.

Associativity of the algebraic operation allows record without parentheses all expressions containing only the operation, but permute elements which are included in the expression, generally speaking, impossible. Permutation is possible only in the case where the operation $\circ$ is commutative.

Definition 3.6. *Binary algebraic operation* $\circ$*, given on the set* A*, is said to be commutative if for any elements* a_1 *and* a_2 *from* A *the equality is satisfied.*

$$a_1 \circ a_2 = a_2 \circ a_1.$$

Examples of commutative operations give addition and multiplication of natural numbers, since for any natural numbers a_1 and a_2 equalities $a_1 + a_2 = a_2 + a_1$, $a_1 \cdot a_2 = a_2 \cdot a_1$ are satisfied. These equalities are valid not only for natural numbers, but for any real numbers, therefore, addition and multiplication are also commutative on the set of real numbers.

There are non-commutative algebraic operations,. Thus, subtraction is not commutative for integers. For example $12-7 \neq 7-12$.

Transitivity in mathematics (or *transitive relation*) is a relation in which if one element in any way corresponds with the second, and the second in exactly the same way corresponds to the third, the first and the third element corresponds to the same manner. More precisely the concept of transitive relation is formulated as follows.

Definition 3.7. *Binary relation* R *on the set* A *is said to be transitive if for any three elements* a, b, c *of the set* A *relations* aRb *and* bRc *implies fulfillment of the relation* aRc.

For example, if $a = b$ and $b = c$, then $a = c$. Further, if $a \| b$ and $b \| c$, then $a \| c$, and so on.

Here, believing that by doing so will be given an additional interpretation of the term "binary relation", an abbreviated table of mathematical symbols (Table. 3.1) is used to refer to elements of binary relations a, b, c an arbitrary set A.

Table 3.1. Basic mathematical symbols of binary relations

Symbol	*Name* Pronunciation	Value
$\Rightarrow$ $\rightarrow$	*Implication, consecution* «implicate» or «if ..., then»	$A \Rightarrow B$ or $A \rightarrow B$ means «if A true, then B also true»
$\Leftrightarrow$	*Equivalence* « if and only if »	$A \Leftrightarrow B$ means «A true if and only if, when B true»
$\forall$	*Quantifier universality* «for all», «for of all», «for any»	$\forall x, P(x)$ means «$P(x)$ is valid for all x»

Often in the set, on which an algebraic operation is considered, special elements which are called *algebraically neutral* or *absorbing*, are highlighted .

Definition 3.8. *Element* e *of the set* A *is said to be neutral with respect to an algebraic operation* $\circ$, *if for any element* a *from the set* A *the equalities* $a \circ e = e \circ a = a$ *take place.*

It is proved that if the neutral element with respect to an algebraic operation exists, it is unique.

Definition 3.9. *Element* p *from the set* A *is called absorbing with respect to an algebraic operation* $\circ$, *if for any element* a *from the set* A *the equalities* $a \circ p = p \circ a = p$.

Thus, in the set Z_0 of non-negative integers, zero is a neutral element with respect to addition, since for any a from A the equalities $a + \mathbf{0} = \mathbf{0} + a = a$ take

place. The same number zero is an absorbing element with respect to multiplication: for any a from the set Z_0 the equalities $a \cdot \mathbf{0} = \mathbf{0} \cdot a = \mathbf{0}$ take place.

At the same time, in the set Z_0 of non-negative integers, one is a neutral element with respect to multiplication, since for any a of A the equalities $a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$ take place. The same element $\mathbf{1}$, being a component of a set of propositions A, is an absorbing element with respect to the algebraic operation of disjunction over propositions: for any statement a from the set A equalities $a \vee \mathbf{1} = \mathbf{1} \vee a = \mathbf{1}$ take place.

An important role in algebraic structures play a so-called *invertible* and *symmetrical* elements.

Definition 3.10. Let $(X, \circ)$ *be an algebraic structure with a neutral element* e *. Element* $a \in X$ *is said to be* ***invertible*** *if there is an element* $b \in X$ *, for which*

$$a \circ b = b \circ a = e. \tag{3.1}$$

Element b *is called* ***symmetric*** *to* a.

If b is symmetric element to a, then a is symmetric element to b.

3.2. Groups

The concept of a group $(G, \circ)$ is the central concept in the theory of algebraic structures and finds wide application not only in mathematics, but also in various applied fields of science and technology.

3.2.1. General characteristics of groups

Definition 3.11. *A non-empty set of elements* G *of an arbitrary nature with a binary operation defined on it* $\circ$ *is called a group if*

1) operation $\circ$ *is associative;*

2) there is a neutral element e *such that* $ae = ea = a, a \in G;$

3) every element a *of* G *has a symmetric (inverse) element* $b \in G.$

The conditions 1), 2) and 3) listed above are called axioms of the group. Suppose that in the group G, in addition to the three axioms indicated, the following condition is also satisfied:

$$a \circ b = b \circ a,$$

The condition is called *commutativity.*

In this case, the group G is called a ***commutative*** or ***abelian*** group. If the number of elements of the group is finite, then the group is ***finite***, otherwise it is called ***infinite***. The number of elements of a finite group determines its ***order***, otherwise called the ***cardinality*** of the group, and is denoted by $|G|$ or by $\#G$.

Group operation $\circ$ most often introduced by two characters:

1) by a ***point***; sometimes instead of $a \cdot b$ write simply ab and talk about multiplying the elements of the group; Group is called multiplicative and with the full method of recording (when you want to explicitly specify a group operation) denote this $(G,\cdot)$ or so $(G,\times)$; a neutral element is entered by the symbol $\mathbf{1}$ or by e and is called a unit, and an element symmetric to a, is the inverse of a and denoted as a^{-1}, wherein

$$a \cdot a^{-1} = a^{-1} \cdot a = \mathbf{1}, \text{ or } aa^{-1} = a^{-1}a = \mathbf{1}.$$

2) ***the symbol of addition*** $+$; then talk about the addition of elements of the group; Group is called ***additive*** and denote $(G,+)$; a neutral element is entered by the symbol $\mathbf{0}$ and call it zero, and an element symmetric to a, is the opposite to a and denote $-a$. In this way

$$a + (-a) = \mathbf{0}.$$

As an example of the additive group, we can give the set of integers connected by the operation of addition. At the same time, the set of rational numbers, not including 0, serves as an example of the multiplicative group. These two groups just laid the foundation of the general group theory.

Recall that the set of rational numbers, denoted by Q (from English quotient), is formed by the ratio of two integers m and n. If $a = m/n$ is some rational number, then the inverse of it in multiplication is an element $a^{-1} = n/m$.

At least two should specify the reasons for which zero is not included in the multiplicative group of the set of rational numbers. This is firstly because there is no element in the group that inverse to zero, and as a consequence, secondly, division by zero is a prohibited operation.

Definition 3.12. *A subset H of the multiplicative group G, that is itself a group with respect to an operation $\circ$, defining G, is called a subgroup of G.*

A subset H of the group G is a subgroup of it if and only if:

1. H contains a unit element of G;

2. Contains the product of any two elements from H;

3. Contains with every element h the inverse h^{-1} of the element.

Definition 3.13. *A subset of a group G, consisting of one-element 1(or e), is called the unit subgroup of the group G.*

Definition 3.14. The group itself G and the unit subgroup 1*(or e)* are called improper subgroups of the group G, all the rest are proper.

Finite groups conveniently to define in the form of Cayley tables, which are one of the ways for presentation of group operations.

Definition 3.15. *The Cayley table is a table that describes the structure of finite algebraic systems by arranging the results of an operation in a table reminiscent of the multiplication table*.

Examples of Cayley's tables of addition $(a+b)$ modulo a composite number $m=6$ (for the additive group) and of multiplication $(a\cdot b)$ modulo a prime number $m=p=7$ (for the multiplicative group) are given in Table. 3.2 and 3.3 respectively. The operators of addition and multiplication in modulo are usually denoted in the form $\overset{m}{\oplus}$, $\overset{m}{\otimes}$ or $\oplus_m, \otimes_m$ respectively.

Table 3.2. Additive residue group modulo 6

$\oplus_6$	0	1	2	3	4	5	$\rightarrow b$
0	0	1	2	3	4	5	
1	1	2	3	4	5	0	
2	2	3	4	5	0	1	
3	3	4	5	0	1	2	
4	4	5	0	1	2	3	
5	5	0	1	2	3	4	
$\downarrow a$							

Table 3.3. Multiplicative residue group modulo 7

$\otimes_7$	1	2	3	4	5	6	$\rightarrow b$
1	1	2	3	4	5	6	
2	2	4	6	1	3	5	
3	3	6	2	5	1	4	
4	4	1	5	2	6	3	
5	5	3	1	6	4	2	
6	6	5	4	3	2	1	
$\downarrow a$							

We note that the tables corresponding to both additive and multiplicative groups of residues are symmetric.

3.2.2. Finite multiplicative group of residues

Definition 3.16. *The multiplicative group of invertible elements of the set of residues modulo* m *is called the finite multiplicative group* $(G,\cdot)$ *residue modulo* m.

Further, it is assumed that the group operation in $(G,\cdot)$ is denoted as multiplication; the number n of elements g of the finite group $(G,\cdot)$ determines its order; A neutral element is denoted by the symbol **1***(*or *e)* and is called a *unity*.

Since the element 0 of the set of residues is not invertible, it is thereby excluded from the set of elements of the multiplicative group (MPG) of residues and, as a consequence, the order n the MPG is one less than the number m of elements $\{0,1,\dots m-1\}$, which form a set of residues modulo m, i.e $n=m-1$.

We give the most important characteristics of finite multiplicative groups and their classification. Let g be the element of the finite MPG.

Definition 3.17. *The order* ord *of the element* g *of the finite group* $(G,\cdot)$ of the *order* n *is defined as the minimal natural number* k *such that* $g^k(\mathrm{mod}\, n)=(g^k)_n=\mathbf{1}$.

According *to* ***Lagrange's theorem****:*

1) *the order of any element* g *of the group* $(G,\cdot)$ *is a divisor of the order of the group, that is* $ord(g)\,|\,ord((G,\cdot))$;

2) *any element* g *of the finite group* $(G,\cdot)$ *of the order* n *satisfies the relation* $(g^n)_n=1$.

Let's consider an example. Let $\{1,2,\dots,12\}$ be elements of MPG of the 12th order $(n=12)$, formed by nonzero elements of the set of residues modulo a prime number $m=p=13$. Let's collect in the tab. 3.4 residues of powers of all elements g of the MPG and orders ord of these elements.

Table 3.4. Residues of degrees of elements of the MPG modulo 13

$\downarrow g$	Power of the element g in k-th degree													$ord(g)$
	0	1	2	3	4	5	6	7	8	9	10	11	12	
2	1	2	4	8	3	6	12	11	9	5	10	7	1	12
3	1	3	9	1										3
4	1	4	3	12	9	10	1							6
5	1	5	12	8	1									4
6	1	6	10	8	9	2	12	7	3	5	4	11	1	12
7	1	7	10	5	9	11	12	6	3	8	4	2	1	12
8	1	8	12	5	1									4
9	1	9	3	1										3
10	1	10	9	12	3	4	1							6
11	1	11	4	5	3	7	12	2	9	8	10	6	1	12

Elements $g=1$ and $g=12$ of the MPG are not included in Table. 3.4, since their orders are a priori known. In fact, in the first place, it is obvious that $ord\,(1)=1$, and, secondly, for an arbitrary value of the module m, which is a prime or a composite number, the order of the largest residue $g=m-1$ of the group (namely, this is an element $g=12$ in this example) is 2.

Indeed, according to the definition, the order of the element g of MPG module m is equal to that minimal natural number $k\geq 1$, which maps $g^k \pmod p$ in the unit. We form the second degree of the residue $m-1$. We have

$$(m-1)_m^2=\left(m^2-2m+1\right)_m=1 \qquad (3.2)$$

as m^2 and $2m$ modulo m are equal to zero.

This establishes that the order of the element $g=p-1$ of the MPG module p is equal to two. Consequently, the orders ord elements g of the MPG modulo $m=p=13$ form a sequence of numbers $\{1,2,3,4,6,12\}$, which constitute the complete set of divisors of the MPG of the order $n=12$. Thus, the main points of the Lagrange theorem are confirmed by the considered numerical examples.

Referring to Table. 3.4, we note that the degrees of its four elements 2, 6, 7 and 12 modulo 13 form multiplicative groups of maximal order (MPGMO).

Definition 3.18. *Element g, whose degrees compose a certain group $(G,\cdot)$, is called the generating element (generator) of this group.*

If g is a generator of the group $(G,\cdot)$, then the inverse to g element g^{-1} is also a generator of the same group $(G,\cdot)$, which is clearly illustrated by the graph shown in Fig. 3.1.

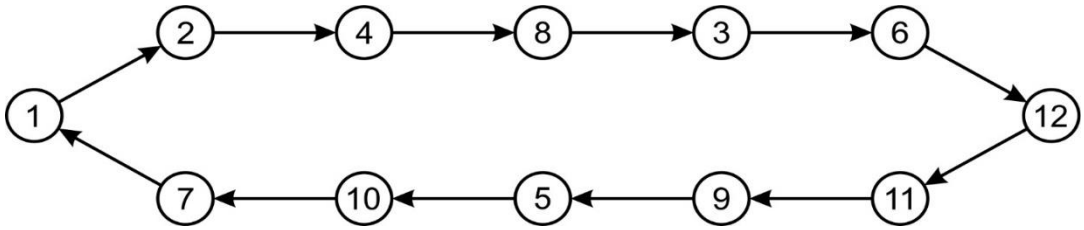

Figure 3.1. Graph of the MPGMO residues modulo 13 formed by the element $g = 2$.

The generating element of the group is the element $g = 2$ (by traversing the contour of the graph clockwise) or inverse to $g = 2$ element $g = 7$, if you bypass the contour of the graph counterclockwise. Elements $g = 2$ and $g = 7$ of the MPGMO are mutually inverse, since $(2 \cdot 7)_{13} = 14_{13} = 1$. The second pair of mutually inverse elements forming multiplicative groups of maximal order, are located below each other in Fig. 3.1 elements $g = 6$ and $g = 11$ such that $6_{13}^{-1} = 11$ and $11_{13}^{-1} = 6$.

Definition 3.19. Group $(G,\cdot)$, *formed by the powers of one primitive element* g, *is called a* ***cyclic group***.

Usually such mathematical notation of a cyclic group is used: $< g >$; less often $< g >_n$, which means "cyclic group of the order n, generated by the element g».

The graph of the MPGMO, shown in Fig. 3.1, and Table. 3.4 confirms the fact that there are groups $(G,\cdot)$, which are generated not by one but by several elements. Thus, the notion of "a system of generating elements" comes to replace the concept of one generating element.

Definition 3.19. *Some set* S *elements of a group* $(G,\cdot)$ $(G,\cdot)$ *is called a system of generators of this group if every element* g *of the groups* $(G,\cdot)$ *is the product of a finite number of factors, each of which is either an element* s *of the set* S, *or is the inverse of some element* s *of the set* S.

For example, according to Table. 3.4 the set S_{12}, the degrees of elements of which generate the MPGMO, represented by the graph in Fig. 3.1, constitute the elements of the set $S_{12} = \{2, 6, 7, 11\}$; subscript 12 with S means order (ord) of the cyclic group formed by the elements of the set S.

We give the *main properties* of cyclic groups:

1. All cyclic groups are abelian.

2. Every subgroup of a cyclic group is cyclic.

3. A cyclic group of order n has exactly $\varphi(n)$ generating elements, where φ is the Euler function.

According to the third property for the cyclic group of order 12 there are exactly four generating element, since $\varphi(12) = 4$, as is confirmed by the data in Table. 3.4.

With the help of the graph shown in Fig. 3.1, you can set a number of other properties of the group $(G, \cdot)$. In particular, the GMO of residues modulo 13 contains two cyclic subgroups for each order $n = 6, 4$ and 3, the forming elements of which are pairs of mutually inverse elements of the group (4, 10), (8, 5) and (3, 9), respectively, and so on.

3.2.3. Inverse elements of the multiplicative groups

Below, we will consider the basic "engineering" techniques for computing the inverse elements of multiplicative groups of residues modulo natural numbers m.

The multiplicative group of residues modulo m is denoted Z_m^*. The top index "asterisk" emphasizes that the element 0 and another noninvertible elements are excluded from the residue set $Z_m = \{0, 1, \ldots, m-1\}$ and from the group Z_m^*.

We recall that in the multiplicative group Z_m^* the element b is the inverse of a, if the condition Z_m^* is satisfied

$$(a \cdot b)_m = 1 \qquad (3.3)$$

Usually the element inverse to an element a, is denoted as a^{-1}.

Let us show further on numerical examples that the inverse element a^{-1} exists only if a and module m are coprime numbers.

The most elementary way to calculate the inverse of multiplication is to select the value of a number $b \in Z_m^*$ which would satisfy equation (3.3). Naturally, in this case, the number 1 should be excluded from the search, if $a \neq 1$.

Let us choose as a module the composite number $m = 9$. Let's reduce to the tab. 3.5 residues of products $a \cdot b$ for $a = 3$ and $a = 6$, which are not coprime with the module $m = 9$.

Table 3.5. Residues of products $a \cdot b$ modulo $m = 9$

a	b						
	2	3	4	5	6	7	8
3	6	0	3	6	0	3	6
6	3	0	6	3	0	6	3

The data of Table. 3.5 confirm that if $(a, m) \neq 1$, then there are no such values $b = a^{-1}$, which would preserve the equality (3.3); that is, the numbers a, which are not coprime with the base m, have no inverse values.

Under the computation by the method of sequential search, the multiplicative inverse values of the elements $a \in Z_9^*$, coprime with the module $m = 9$, and those are the numbers 1, 2, 4, 5, 7 and 8, we take into account that $1^{-1} = 1$ (axiomatic equality) and $8^{-1} = 8$, as a consequence of (3.2). The remaining elements form mutually inverse pairs (2, 5) and (4, 7).

At first glance it may seem strange, for example, such an equality, taken from the previous paragraph: $2^{-1} = 5$, which in the usual sense is treated as: $(2^{-1} = 1/2 = 0.5) = 5$. That is, it would seem that the fractional number 0.5 is equal to the whole number 5. But this is not so. No fractions are discussed here, since other objects are considered - the residues modulo $m = 9$. In fact, we will perform such a simple transformation of "fraction" $1/2$. Multiplying the numerator and denominator of the relation $2^{-1} = 1/2$ by 5, we have

$$(2^{-1})_9 = \left(\frac{1}{2}\right)_9 = \left(\frac{1 \cdot 5}{2 \cdot 5}\right)_9 = \frac{(5)_9}{(10)_9} = \frac{5}{1} = 5.$$

Thus we arrive at the result: $(2^{-1})_9 = 5$. Equally, like $(5^{-1})_9 = 2$.

These examples lead us to the following conclusion:

1. All elements z of the set Z_p^* modulo a prime number p have multiplicatively inverse values, and besides $1^{-1}=1$ and $(p-1)^{-1}=(p-1)$.

2. The multiplicative group of residues Z_m^* can be formed besides modulo a prime number $m=p$, also for any natural m.

In addition to the method of sequential search in calculating inverse values a^{-1} modulo m, which can be cumbersome if $m>>1$, there are algebraic methods for determining a^{-1} for arbitrary values a^{-1} and m, among which (methods) one of the most popular is the method based on the so-called Fermat's small theorem (SFT). The essence of the SFT is as follows:

If p is a prime number and a is an integer not divisible by p, then $a^{p-1}-1$ divided by p, i.e a^{p-1} is congruent with the identity modulo p, which is mathematically written in the form

$$a^{p-1}\equiv 1 \pmod{p}. \qquad (3.4)$$

For example, if $a=2;\ p=7$, then $2^6=64$ there is a number congruent with 1 modulo 7, because $64-1=63=7\cdot 9$.

For an alternate version of the SFT come by dividing the left and right sides (3.4) by a, that is directly (not strictly mathematically, but true for the final result) leads to an estimate of the multiplicative inverse of the value a^{-1} modulo p, namely

$$(a^{-1})_p=(a^{p-2})_p. \qquad (3.5)$$

Let's consider an example. Let $a=3$ and $p=13$. According to (3.5), we have

$$(3^{-1})_{13}=(3^{11})_{13}=(177'147)_{13}=9,$$

which coincides with the data of the graph shown in Fig. 3.1.

Of course, it would seem that a simple formula (3.5) for computing the inverse of multiplication may not be acceptable when a and p become sufficiently large numbers. You can work around this problem by using one of the fast modular exponentiation algorithms widely used in various cryptosystems to speed up computing operations with large numbers. Below is a description of the algorithm, referred to as the *method of repeated squaring and multiplication*.

Let it be required to calculate $a^s \bmod p$. Let's represent the degree s in the form of a binary vector

$$s = s_{j-1}2^{j-1} + s_{j-2}2^{j-2} + \ldots + s_2 2^2 + s_1 2^1 + s_0,$$

where $s_j = (0,1)$.

Then

$$a^s \bmod p = a^{s_{j-1}2^{j-1}+s_{j-2}2^{j-2}+\ldots+s_2 2^2+s_1 2^1+s_0} \bmod p =$$
$$= (a^2)^{s_{j-1}2^{j-2}+s_{j-2}2^{j-3}+\ldots+s_2 2^1+s_1 2^0} a^{s_0} \bmod p =$$
$$= ((a^2)^2)^{s_{j-1}2^{j-3}+s_{j-2}2^{j-4}+\ldots+s_2 2^0} (a^2)^{s_1} a^{s_0} \bmod p =$$
$$= (\ldots((a^2)^2\ldots)^2)^{s_{j-1}} \ldots (a^8)^{s_3} (a^4)^{s_2} (a^2)^{s_1} a^{s_0} \bmod p =$$

Next, the value of expression $a^2 \bmod p$ is calculated and a replacement is performed in the transformed expression. This operation is carried out until the final result is found.

Structural-logical scheme of the algorithm of fast exponentiation is shown in Fig. 3.2.

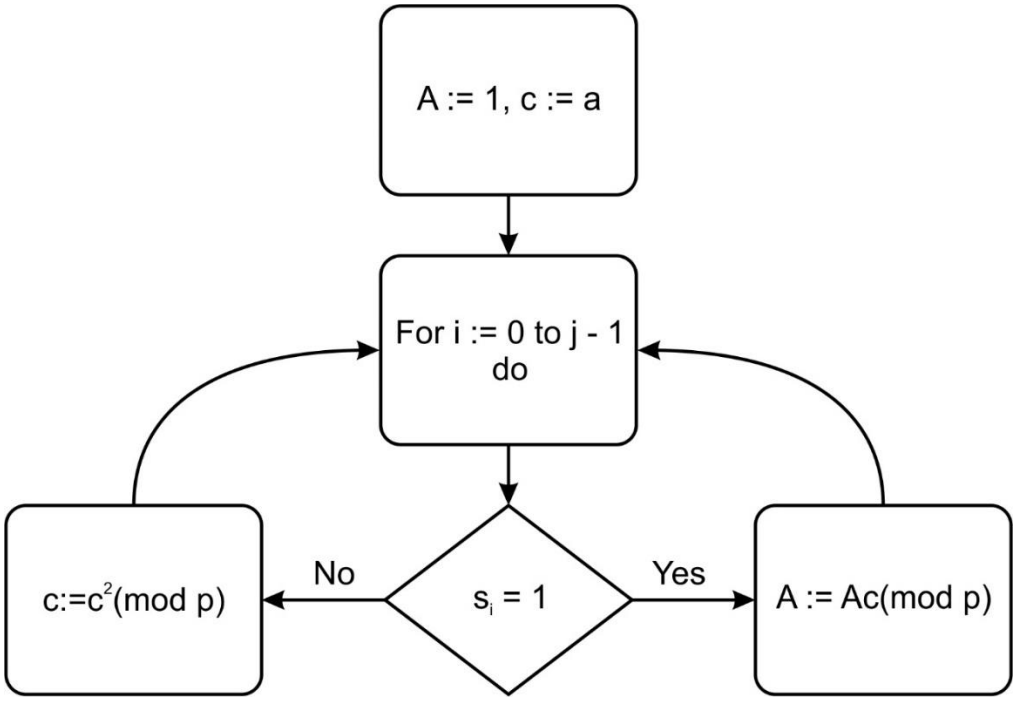

Figure 3.2. A block diagram of the method repeated squaring and multiplication

Let's illustrate the algorithm with next example. Let it be required to calculate $\mathbf{249}^{321} \bmod \mathbf{499}$. We represent the degree in the form $321 = 256 + 64 + 1 = 2^8 + 2^6 + 2^0$. We have

$$\mathbf{249}^{321} \bmod \mathbf{499} = \mathbf{249}^{2^8+2^6+2^0} \bmod \mathbf{499} =$$
$$= (((((((\mathbf{249}^2)^2)^2)^2)^2)^2)^2)^2((((((\mathbf{249}^2)^2)^2)^2)^2)^2\mathbf{249} \bmod \mathbf{499} = \left[\mathbf{249}^2 \equiv \mathbf{125} \left(\bmod \mathbf{499}\right)\right] =$$
$$= ((((((\mathbf{125}^2)^2)^2)^2)^2)^2)^2((((\mathbf{125}^2)^2)^2)^2)^2\mathbf{249} \bmod \mathbf{499} = \left[\mathbf{125}^2 \equiv \mathbf{156} \left(\bmod \mathbf{499}\right)\right] =$$
$$= (((((\mathbf{156}^2)^2)^2)^2)^2)^2(((\mathbf{156}^2)^2)^2)^2\mathbf{249} \bmod \mathbf{499} = \left[\mathbf{156}^2 \equiv \mathbf{384} \left(\bmod \mathbf{499}\right)\right] =$$
$$= ((((\mathbf{384}^2)^2)^2)^2)^2((\mathbf{384}^2)^2)^2\mathbf{249} \bmod \mathbf{499} = \left[\mathbf{384}^2 \equiv \mathbf{251} \left(\bmod \mathbf{499}\right)\right] =$$
$$= (((\mathbf{251}^2)^2)^2)^2(\mathbf{251}^2)^2\mathbf{249} \bmod \mathbf{499} = \left[\mathbf{251}^2 \equiv \mathbf{127} \left(\bmod \mathbf{499}\right)\right] =$$
$$= ((\mathbf{127}^2)^2)^2\mathbf{127}^2\mathbf{249} \bmod \mathbf{499} = \left[\mathbf{127}^2 \equiv \mathbf{161} \left(\bmod \mathbf{499}\right)\right] =$$
$$= (\mathbf{161}^2)^2\mathbf{161} \cdot \mathbf{249} \bmod \mathbf{499} = \left[\mathbf{161}^2 \equiv \mathbf{472} \left(\bmod \mathbf{499}\right)\right] =$$
$$= \mathbf{472}^2\mathbf{161} \cdot \mathbf{249} \bmod \mathbf{499} = \left[\mathbf{472}^2 \equiv \mathbf{230} \left(\bmod \mathbf{499}\right)\right] =$$
$$= \mathbf{230} \cdot \mathbf{161} \cdot \mathbf{249} \bmod \mathbf{499} = \mathbf{447}$$

Thus, we arrive at the final result

$$\mathbf{249}^{321} \bmod \mathbf{499} = \mathbf{447}.$$

3.3. Rings

The **ring** (also an *associative ring*) in general algebra $(R, +, \times)$ is a natural generalization of integers, which is an algebraic structure in which two operations are defined: (1) an *invertible addition operation* and (2) *multiplication*, similar in properties to corresponding operations on numbers.

Invertibility of the operation is understood in the sense that the operation of addition responsible inverse operation - the subtraction (and vice versa). The operation of division in general case is not defines over elements of the ring.

Definition 3.20. *A ring is an arbitrary set R, on which binary operations of* ***invertible addition*** *are given (that is, operations $+$, $-$) and multiplication $\times$, with the following properties, observed for any $a, b, c \in R$:*

1. $a + b = b + a$ — ***commutativity*** *of addition;*

2. $a + (b + c) = (b + a) + c$ — ***associativity*** *of addition;*

3. $\exists\, \mathbf{0} \in R \quad (a + \mathbf{0} = \mathbf{0} + a)$ — *the existence of a neutral element with respect to addition;*

The above mathematical notation reads: in the ring R there is such an element $\mathbf{0}$, called a neutral element, which any element a, belonging to R, ensures equality $a + \mathbf{0} = \mathbf{0} + a$;

4. $\forall a \in R, \quad \exists\, b \in R \quad (a + b = b + a = \mathbf{0})$ — *the existence of an* ***inverse*** *(or opposite) element with respect to addition;*

5. $(a \times b) \times c = a \times (b \times c)$ — ***associativity*** *of multiplication;*

6. $\begin{cases} a \times (b + c) = (a \times b) + (a \times c) \\ (b + c) \times a = (b \times a) + (c \times a) \end{cases}$ — *diztributivity*

Usually under the ring understand associative ring with unity, for which: $\forall e \in R, \quad \exists\, a \in R \quad (a \times e = e \times a)$. The neutral element e is usually referred to as **1**.

Ring whose elements are numbers and operations are *addition* and *multiplication* of numbers is called a ***number ring***.

Examples of numeric rings:

- Z — integers (with the usual addition and multiplication).

- Z_n — residue ring modulo a natural number n.

3.4. The Galois Fields

The ***field*** is the most abstract concept in mathematics and makes up algebra F, for whose elements all four arithmetic operations are defined (*addition, subtraction, multiplication* and *division*, apart from division by zero), and the properties of these operations are close to the properties of ordinary numerical operations.

Although the names of field operations are taken from arithmetic, it should be borne in mind that field elements are not necessarily numbers, and the definitions of operations may be far from arithmetic. For example, field elements can be represented by vectors, spatial matrices and other objects.

We give a more complete definition of the field.

Definition 3.20. ***A field*** *is a nonempty set F, on which are given invertible algebraic operations, called addition $+$ and multiplication $\times$, satisfying the following axioms:*

1. For any a, b and c, belonging to F, $(a+b)+c=a+(b+c)$. This is the *associativity of addition*;

2. For any a, b and c, belonging to F, $(a+b)+c=a+(b+c)$. This is the *commutativity of addition*;

3. There is a zero element $\mathbf{0}$, belonging F, such that for any element a, belonging to F, the equality holds: $\mathbf{0}+a=a+\mathbf{0}=a$. This is the *existence of a zero element*;

4. For any element a exist $-a$, such that the equality holds: $a+(-a)=(-a)+a=\mathbf{0}$. This is the existence of the *opposite element* $-a$ for each a;

5. For any a, b and c, belonging to F, $(a+b)\times c=a\times c+b\times c$. This is the *distributivity of multiplication with addition*;

6. For any a, b and c, belonging to F, $(a\times b)\times c=a\times(b\times c)$. This is the *associativity of multiplication*;

7. For any a, b and c, belonging to F, $a\times b=b\times a$. This is the *commutativity of multiplication*;

8. There is a single element $\mathbf{1}$, belonging F, such that for any element a, belonging to F, the equality holds: $\mathbf{1}\times a=a\times\mathbf{1}=a$. This is the existence of a *unit element*;

9. For any element a, not equal to zero, there is an inverse element $1/a=a^{-1}$ such that the equality holds: $a\times a^{-1}=a^{-1}\times a=\mathbf{1}$. This is the existence of an *inverse element* for each nonzero a.

The term "invertible operation" in the definition of a field means, in particular, that, along with the *addition* operation for field exists inverse operation of *subtraction* as well as *multiplication* is followed by inverse operation of *division* (excluding division by zero).

Thus, the field is nothing else than a commutative ring R with a unit in which all four algebraic operations are defined: addition, subtraction, multiplication and division (except division by zero), with each nonzero element a of the field F meets the inverse element a^{-1}, belonging to the same field.

Examples of fields: Z_p — residue field modulo p, where p is a prime number; F_q — finite field from $q = p^n$ elements, where p — prime number, n is a natural number, and so on.

At the same time, the set of integers Z does not form a field. Indeed. Is the field a ring?

Yes it is. Multiplication and addition are present. All the axioms are satisfied.

Does Z is a commutative ring?

Yes, it is also. For example $5 \times 3 = 3 \times 5 = 15$.

Is Z a ring with unity?

Yes it is.

But Z it is not a field, because there is no inverse for each element of Z, since these are integers. And the inverse element is a unit divided by this same element. For example, suppose $a = 3$, then $a^{-1} = 1/a = 1/3$. But 1/3 – this is not an integer.

But the set of rational (Q) and real numbers (R) will be fields.

We are interested only in *finite fields*, called *Galois field*, which contain a finite number q elements and are denoted by $GF(q)$ or F_q. The theory of finite fields is the central mathematical theory underlying the noise-immune coding and cryptology.

Field parameter q is either a prime number p, or the power of a prime number p^n, where n is a natural number. If $q = p$, then the field is called a *prime Galois field* and is denoted by $GF(p)$ or F_p. If $q = p^n$, $n > 1$, then the field is called the *extended Galois field* and is denoted by $GF(p^n)$ or F_{p^n}.

An example of a prime Galois field $GF(p)$ can be the residue field Z_p modulo a prime number p, i.e $GF(p) = \{0, 1, 2, \ldots, p-1\}$. Elements of a prime field in this case are nonnegative integers not exceeding $p-1$.

At the same time, the elements of the extended field $GF(p^n)$, as a partial case, can be either $n-$dimensional code combinations, each digit r_i of which belongs to a prime field $GF(p)$, i.e. $r_i \in GF(p)$, $i = \overline{1,n}$, or a polynomial of degree not exceeding $n-1$, both ways of representing the same polynomial consisting of

n monomials; or (1) by the sequence of its $p-$ary coefficients (we call it the vector form), or (2) in the form of $p-$ary polynomial of $(n-1)-$th power of one variable (polynomial form).

As an example of an extended field, we give the field $GF(2^3)$. The elements of this field are three-bit codes, starting with the code 000 to 111.

Argument p of the field $GF(p)$, as well as $GF(p^n)$, is one of the most important parameters of the Galois field and is called the *field characteristic*. Since any field $GF(q)$ along with non-zero elements a must contain their inverse values a^{-1}, then the characteristic of the field p must be *just a prime number*.

Non-zero elements of the field F_q form a group with respect to the operation of multiplication, which is called the *multiplicative group of the field* and is denoted by F_q^*. This group is cyclic, that is, there is a generating element in it, and all other elements are obtained by raising to the power of the generator element, also called the *generator*. In this case, the powers of the generating element in the formation of the multiplicative group of the prime Galois field are reduced to the residue modulo a prime number p, and in the formation of MPG of the extended field $GF(p^n)$ residue modulo of the IP $n-$th degree polynomial $f_n(x)$ (generating $GF(p^n)$) with coefficients over the field $GF(p)$.

It is quite obvious that the field F_q can be formed by a union, we denote this operation by the sign $\vee$, elements of the multiplicative group F_q^* and the zero element $\mathbf{0}$ of the field, that is $F_q = F_q^* \vee \mathbf{0}$. For the fields considered above, the zero element $\mathbf{0}$ of the prime field $GF(p)$ is a numerical zero, and for an extended field $GF(p^n)$ is the $n-$dimensional zero vector.

The generating element of the multiplicative group F_q^*, denote it α, is also called the primitive element of the field F_q. Field F_q contains $k = \varphi(q-1)$ primitive elements α_i, $i = \overline{1, k}$, where φ is Euler totient function.

To determine the primitive elements of a field $GF(p)$ it is enough to find one of them, for example, α_1, and then use

$$\alpha_i = \alpha_1^{s_i} (\text{mod } p), \quad i = \overline{1, k}, \tag{3.6}$$

where s_i — exponents that are relatively prime to the number p.

We will illustrate the scheme for calculating primitive elements (3.6) of a simple Galois field of characteristic $p=11$. Mutually simple with a number $p-1=10$ are the numbers s_i, equal to 1, 3, 7 and 9. As α_1 for $GF(11)$ we choose the minimal primitive element $\alpha_1=2$ of the field. Using formula (3.6), we find $\alpha_2=8$, $\alpha_3=7$ and $\alpha_4=6$.

In order to confirm the correctness of expression (3.6) in Table. 3.6 residues of powers modulo $p=11$ ranged primitive elements $\alpha=\{2, 6, 7, 8\}$ are given.

Table 3.6. Residues of sequences of degrees of primitive elements α of the prime finite field $GF(11)$

α	Degrees of primitive elements										
	0	1	2	3	4	5	6	7	8	9	10
2	1	2	4	8	5	10	9	7	3	6	1
6	1	6	3	7	9	10	5	8	4	2	1
7	1	7	5	2	3	10	4	6	9	8	1
8	1	8	9	6	4	10	3	2	5	7	1

From Table. 3.6 it follows that the elements 6, 7 and 8 calculated by formula (3.6) are indeed primitive elements of the field $GF(11)$, forming, like the element $\alpha_1=2$, multiplicative groups of maximal order (Figures 3.3 and 3.4).

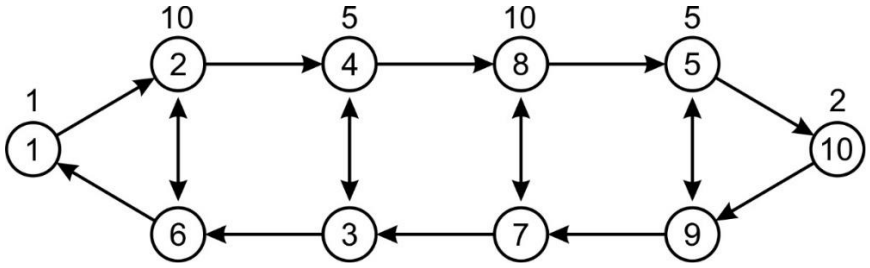

Figure 3.3. Graph of the MPGMO residues modulo 11, formed by the element $g=2$

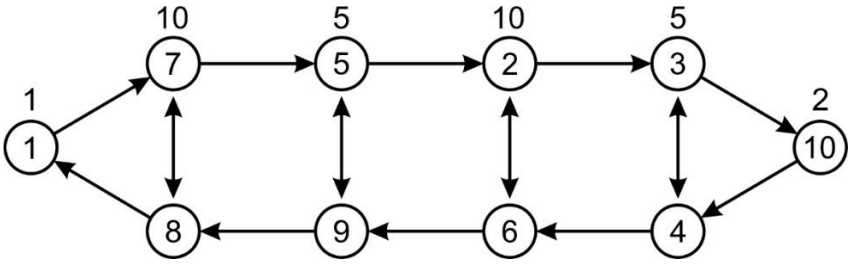

Figure 3.4. Graph of the MPGMO residues modulo 11, formed by the element $g=7$

Inside the circles in Fig. 3.3 and 3.4 indicate the values of elements of the groups, and over them - orders *ord* of these elements. Double-headed arrow combined mutually inverse elements of the group.

And in the conclusion of the section pay attention to the following two circumstances. Firstly, the fact that the orders of the elements of the multiplicative group defined easily enough directly from the graph of the counter of the group. In fact, consider, for example, the graph of the multiplicative group of the field $GF(11)$, presented in Fig. 3.4, and set the goal to calculate the order of the element 3 of the group generated by the primitive element 7. To do this, we traverse the contour of the graph clockwise, starting from vertex 1, thinning out three elements, until we return to the beginning of the bypass, that is, the vertex 1 (Figure 3.5).

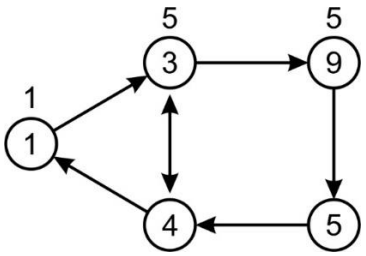

Figure 3.5. Subgraph MPG of residues modulo 11, defined by the element $g = 3$

We see that such circumvention of the graph is done in five phases and hence, ord (3) = 5. Exactly the same order has the element 3 in MPGMO which is presented in Fig. 3.3. And this is natural, because the element 3 is part of the field, the order of which (element) should not depend on which group (or subgroup) can be included the element in question.

And, finally, in the second place, the orders of various nonzero elements of the field $GF(11)$, which equal to 1, 2, 5 and 10 (as it follows from Figures 3.3-3.5) are, as it should be, divisors of the order of the multiplicative group $GF^*(11)$.

Summary section

An algebraic system (or algebraic structure) in the general case is understood to mean the set A of elements of an arbitrary nature (carrier) with a set of operations (signatures) defined on it that satisfies a certain system of axioms.

2. Tuple is an ordered sequence of elements $A^n = \{a_1, a_2, \ldots, a_n\}$.

3. The arity of an operation or function in mathematics is the number n of their arguments, or operands.

4. Under nullary algebraic operations on the set A understand an arbitrary fixed element of this set.

5. An example of a unary (single) operation can be the operation of computing an element $\bar{a} \in A$ inverse to the element a of the same set A.

6. A binary algebraic operation on a set A is a mathematical operation «τ», which to an arbitrary pair of elements a and b of the set A uniquely associates an element $c = a\tau b$, belonging to the same set, and called the composition or product of the elements a and b.

7. The binary algebraic operation can have such important properties like *associativity*, *commutativity* and *transitivity*.

8. An algebraic operation $\circ$, defined of a set A is called *associative,* if for any elements a_1, a_2 and a_3 from A the equality $(a_1 \circ a_2) \circ a_3 = a_1 \circ (a_2 \circ a_3)$ holds.

9. A binary algebraic operation $\circ$, defined on a set A, is called *commutative*, if for any elements a_1 and a_2 from A the equality $a_1 \circ a_2 = a_2 \circ a_1$ holds.

10. *Transitivity* in mathematics (or *transitive relation*) is a relation in which if one element in some way relates to the second, and the second in exactly the same way corresponds to the third, then the first element correlates with the third corresponds in the same manner.

11. A binary relation R on a set A is said to be *transitive* if for any three elements a, b, c of the set the fulfillment of relations aRb and bRc implies that the relation aRc is satisfied.

12. Often in the set on which the algebraic operation is considered, special items that are called *neutral* and *absorbent* are highlighted.

13. An element e of the set A is said to be *neutral* with respect to an algebraic operation $\circ$, if for any element a of the set A the equalities $a \circ e = e \circ a = a$ hold.

14. An element p of the set A is called *absorbing* with respect to an algebraic operation $\circ$, if for any element a of the set A the equalities $a \circ p = p \circ a = p$ hold.

15. In the set Z_0 of integer nonnegative numbers zero is the *neutral* with respect to addition, since for any a from Z_0 the equalities $a + \mathbf{0} = \mathbf{0} + a = a$ hold. The same number zero is an absorbing element with respect to multiplication: for any a from the set Z_0 equalities $a \cdot \mathbf{0} = \mathbf{0} \cdot a = \mathbf{0}$ hold.

16. In the set Z_0 of integer nonnegative numbers unit is the *neutral* with respect to multiplication, since for any a from Z_0 the equalities $a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$ hold. The same element 1, being a component of the set of propositions A, is an absorbing element with respect to the algebraic operation of disjunction over propositions: for any proposition a from the set A the equalities $a \vee \mathbf{1} = \mathbf{1} \vee a = \mathbf{1}$ hold.

17. An important role in algebraic structures plays a so-called *invertible* and *symmetrical* elements.

18. Let $(X, \circ)$ be an algebraic structure with *a neural element* e. Element $a \in X$ is called *invertible*, if there is an element $b \in X$, such that $a \circ b = b \circ a = e$. The element b is called to be *invertible (or symmetric)* to a. If b *is invertible* element to a, then a *is invertible* element to b.

19. A nonempty set of elements of an arbitrary nature G with a binary operation $\circ$ defined on it is called a *group* if: (a) *the operation* $\circ$ *is assosiative*; (b) t*here is a neural element* e; (c) *any element* a *from* G *has symmetrical invertible element* $b \in G$. The conditions (a), (b), and (c) are called *axioms of the group*.

20. Suppose that in the group G, besides the three axioms indicated, the condition: $a \circ b = b \circ a$, called *commutativity*, is also satisfied. In this case, the group is called a *commutative* or *abelian* group.

21. If the number of elements of a group is finite, the group is *finite*, otherwise it is called *infinite*.

22. The number of elements of a finite group determines its *order* and is denoted by $|G|$.

23. Group operation $\circ$ is most commonly introduced using two characters:

(1) the sign of multiplication $\cdot$ or $\times$; then the group is called *multiplicative* and is denoted by $(G,\cdot)$ or $(G,\times)$; *the neural element* is introduced by the symbol **1** and is called a *unit*, and an element, *symmetrical to* a, is *invertible* to a and is denoted a^{-1}, wherein $a \cdot a^{-1} = \mathbf{1}$ or $aa^{-1} = \mathbf{1}$;

(2) the sign of *addition* $+$; then speak about the addition of elements of the group; the group are called *additive* and denote $(G,+)$; a neural element is introduced by the symbol **0** and is called *zero*, and element invertible to a, is the opposite to a, and is denoted $-a$.

24. A subset H of a group G, that is itself a group with respect to an operation $\circ$, defining G, is called a subgroup and is such if and only if: (1) H contains a unit element of G; (2) contains the product of any two elements of H; (3) with every element h contains an inverse element h^{-1}, that is one of the ways of representing group operations.

25. It is convenient to define finite groups in the form of *Cayley tables*, which are one of the ways to represent group operations.

26. *Cayley table* is the table, that describes the structure of finite algebraic systems by positioning operation results in the table, the table-like multiplying.

27. A finite multiplicative group $(G,\cdot)$ of residues modulo m is called the multiplicative group of invertible elements of the set of residues modulo m.

28. A group operation in a multiplicative group $(G,\cdot)$ is denoted as multiplication; the number n of elements g of a finite group $(G,\cdot)$ determines its *order*; a neutral element is entered by the symbol **1** and is called *unit*.

29. The order *ord* of an element g of a finite group $(G,\cdot)$ of the order n is defined as the minimal natural number k such that $g^k (\mathrm{mod}\, n) = (g^k)_n = 1$.

30. The order of any element g of the group $(G,\cdot)$ is a divisor of the order of the group, that is $ord(g) \mid ord(G,\cdot)$.

31. Any element g of a finite group $(G,\cdot)$ of order n satisfies relation $(g^n)_n = 1$.

32. An element g, of whose degrees a certain group $(G,\cdot)$ is composed, is called the *generator (generating, primitive*) element of this group.

33. A group $(G,\cdot)$, formed by the powers of one primitive element g, is called a *cyclic group* and is denoted by $< g >$.

34. There are groups $(G,\cdot)$, that are generated not by one, but by several elements. Thus, the notion of a "system of generative elements" comes to replace the concept of one generating element.

35. A certain set S of elements of a group $(G,\cdot)$ is called a *system of generators* of this group if every element g of the group $(G,\cdot)$ is the product of a finite number of factors, each of which either is an element s of the set S, or is inverse to some element s of the set S.

36. For a cyclic group of the order n there are exactly $\varphi(n)$ generating elements, where φ is the Euler function.

37. All elements z of a set Z_p^* modulo a prime p have multiplicative inverse values, and $1^{-1}=1$ and $(p-1)^{-1}=(p-1)$.

38. The multiplicative group of residues Z_m^* can be *formed only modulo a prime number* $m=p$, since if it turns out m to be a composite number, then in the set Z_m^* there is at least one element z, that is not coprime to m, and as a consequence, this element will not have an inverse value, which contradicts the third axiom of the group: any element z from Z_m^* has an inverse element $z^{-1} \in Z_m^*$.

39. A *ring* is an arbitrary set R, where binary operation of *invertible addition* (i.e. the operations +, -), and *multiplication* are given.

40. The ring whose elements are numbers and operations are *addition, subtraction* and *multiplication* of numbers is called a *number ring*.

41. The field is the most abstract concept in mathematics and compose an algebra F, for which elements all four arithmetic operations are defined (*addition, subtraction, multiplication* and *division*, except the division by zero), and the properties of these operations similar to those of conventional numeric operations.

42. Finite fields, called *Galois fields*, contain a finite number q of elements and are denoted $GF(q)$. If $q=p$, where p is a prime number, then the field is called a *simple Galois field* and is denoted as $GF(p)$ or F_p. If $q=p^n$, $n>1$, then the field is called the *extended Galois field* and is denoted as $GF(p^n)$ or F_{p^n}.

43. Elements of the extended field $GF(p^n)$, as a particular variant, can be either $n-$dimensional code combinations, each digit r_i of which belongs to a simple field $GF(p)$, that is $r_i \in GF(p)$, $i=\overline{1,n}$, or a polynomial of degree not exceeding $n-1$.

44. The argument p of the field $GF(p)$, like $GF(p^n)$, is one of the most important parameters of the Galois field and is called the *characteristic* of the field. Since any field $GF(q)$ along with nonzero elements a must contain their inverse values a^{-1}, then the characteristic p must be just a prime number.

45. The generating element of the multiplicative group F_q^*, we denote it α, is also called the *primitive element* of the field F_q. The field F_q contains $k=\varphi(q-1)$ primitive elements a_i, $i=\overline{1,k}$, where φ is the Euler function.

46. To determine the primitive elements of a field $GF(p)$ it is sufficient to find one of them, for example, a_1, and then use the relation $a_i = a_1^{s_i} \pmod p$, $i=\overline{1,k}$, where s_i are exponents that are coprime to the number p.

Questions for self-examination

1.Give a definition of the algebraic structure.

2. What is a tuple?

3. Give the definition of the arity of an algebraic operation.

4. How to understood the nullary algebraic operation?

5. Give an example of a nullary algebraic operation.

6. Define a binary algebraic operation.

7. What are the main characteristics that may have algebraic operations.

8. Give generalized forms that reflect the associativity, commutativity and transitivity of algebraic operations..

9. What elements are neutral with respect to addition and multiplication-operations?

10. Give a definition of the inverse element.

11. By what characters (signs) introduce the basic algebraic operations?

12. Give the definition of a group.

13. What are the basic axioms of groups.

14. What is the property of Abelian groups?

15. What is the order of the group and how it is designated?

16. Give a definition of subgroups.

17. What are the Cayley table?

18. Give the definition of the multiplicative group by a modulo.

19. Define the order of the element of the group.

20. In what ratio are the orders of the group and its elements?

21. How to understand the term "generating element a group"?

22. Which group is called cyclic?

23. What is a "system of generators" of the group?

24. For what reason the multiplicative group can be formed modulo a prime number?

25. Give the definition of the ring as the algebraic structure.

26. What kind of ring is called a numeric?

27. What is the algebraic structure of the "field".

28. What operations are used in the fields?

29. What is the Galois field?

30. Explain the concept of "the characteristic".

31. What elements of the Galois field are called primitive?

32. How to calculate the primitive elements of a Galois field?

4. MATRICES AND GENERATORS OF PSEUDO-RANDOM GALOIS SEQUENCE

The final section of the training manual sets out the questions of construction of linear shift register with linear feedbacks, these are the simplest form of pseudo-random number generators (PRNG) or sequences (PRS), based on generalized Galois and Fibonacci matrices over the field F_p.

4.1. Preliminaries

The term Galois matrix as objectively related with their Fibonacci matrix, borrowed from the theory of cryptography, where are widely used generators of pseudo-random binary sequence in the Galois and Fibonacci configurations built on linear shift registers (LSR) with linear feedbacks (LFB). Shift register of the length n bits can appears in one of $2^n - 1$ inner states S_k, $k = \overline{0, 2^n - 2}$. Only SR with exceptionally selected feedback functions can trace across all $2^n - 1$ inner states . These are so called *registers (generators) of maximal period*.

We draw attention to the fact that when it comes to the classic SR, then this implies that the register bits (triggers) may be in one of two states: 0 or 1. These registers are binary SR, and they acquire a property register (generators PRN) the maximum period, if only feedbacks formed primitive polynomials with coefficients over a Galois field of characteristic 2.

For simplicity, we sometimes called generic SR and the corresponding generalized Galois and Fibonacci matrices as *Galois and Fibonacci registers* and *matrices of characteristic p*.

The main problem considered below is to develop algorithms for constructing generalized primitive Galois matrices (as well as Fibonacci matrices) of the $n-$th order over field $GF(p)$, $p \geq 2$. The matrices have to define unique the structure of the corresponding generalized $n-$bits linear shift registers of the maximum period,

as well as formed on their basis generators of pseudo-random Galois sequences of maximal length ($m-$sequence) equal to p^n-1.

Let us explain the term "primitive matrix". Let $\boldsymbol{A}=(a_{i,j})$ be the nondegenerate matrix of the order $n>1$ over prime finite field such that $a_{i,j}\in GF(p)$ for all $i,j=\overline{1,n}$ and $\boldsymbol{E}=(\delta_{i,j})$, where $\delta_{i,j}$ – the Kronecker symbol, be the unit matrix of the same order that $\boldsymbol{A}$. The matrix $\boldsymbol{A}$ is said to be nondegenerate over a field $GF(p)$ if its determinant $\det \boldsymbol{A}$ is not equal zero modulo p, i.e. $\det \boldsymbol{A} \pmod p \in \overline{1,\ p-1}$, where p prime. The operation of raising a matrix $\boldsymbol{A}$ to some power d is carried out in the residue field modulo p, and each element of the matrix $\boldsymbol{A}^d$ is reduced to a nonnegative remainder modulo p. The sequence of degrees of the matrix $\boldsymbol{A}$, starting with the zero degree, for which $\boldsymbol{A}^0=\boldsymbol{E}$, forms a cyclic group $<\boldsymbol{A}>$ of order d. The matrix $\boldsymbol{A}$ will be called *primitive* if the smallest natural number e, for which $\boldsymbol{A}^e=\boldsymbol{E}$, satisfies the relation $e=p^n-1$. The essence of the term "primitive" matrix is similar, to a certain extent, the essence of the term "primitive element" of the field $GF(p^n)$.

Introduce some notations. Let $L_{n,p}=p^n-1$ be a total number of $n-$bit vectors with elements over $GF(p)$, with the exception of the zero vector; $L_{n,p}^{(\theta)}$ – the number of primitive generators θ, which is determined by the Euler function φ of the argument $L_{n,p}$, that is $L_{n,p}^{(\theta)}=\varphi(L_{n,p})$,

In Table. 4.1 as an example shows the complete set of primitive generators of field elements $GF(3^4)$ over an irreducible polynomial $f_4=12101$.

Table 4.1. Primitive elements of the fields $GF(3^4)$ over the IP $f_4=12101$

j	i							
	1	2	3	4	5	6	7	8
0	101	102	120	122	201	202	210	211
8	1010	1012	1021	1022	1102	1111	1112	1122
16	1200	1211	1220	1222	2011	2012	2020	2021
24	2100	2110	2111	2122	2201	2211	2221	2222

The number of the generative (GE) element is determined by the sum of the column number i and the row value j of Table. 4.1, i.e. $k = i + j$. The sequence of the maximum length, equal to 80, formed by the primitive element $\theta = 1102$ and highlighted by shading in Table. 4.1, is summarized in Table. 4.2.

Table 4.2. Multiplicative group of $GF(3^4)$ over IP $f_4 = 12101$ and generating element $\theta = 1102$

j	i									
	1	2	3	4	5	6	7	8	9	10
0	0001	1102	1001	2211	1221	2001	0020	1111	2121	2122
10	0221	1222	0100	1021	0022	0012	1120	0211	2000	2221
20	0110	0210	1201	1220	1202	2022	2200	1200	0121	0201
30	0111	1012	2202	0101	2120	1020	2220	2011	2212	2020
40	0002	2201	2002	1122	2112	1002	0010	2222	1212	1211
50	0112	2111	0200	2012	0011	0021	2210	0122	1000	1112
60	0220	0120	2102	2110	2101	1011	1100	2100	0212	0102
70	0222	2021	1101	0202	1210	2010	1110	1022	1121	1010

4.2. Classic Galois matrices and generators

It is known, as it was mentioned earlier, that in order for the SR is the generator of pseudo-random sequence of maximal period corresponding feedback polynomial must be a primitive polynomial (PP). Example eighth order Galois generator forming PRSs of maximum period as shown in Fig. 4.1.

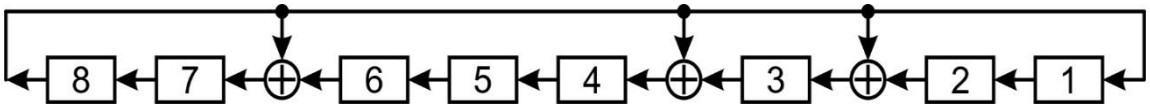

Figure 4.1. Structural scheme of the PRS generator by the Galois scheme over primitive polynomial $f_8 = 101001101$

The classical Galois generator, shown in Fig. 4.1, associates with each non-zero element of the field $GF(2^8)$ the corresponding power of the primitive element $\theta = 10$ modulo PP $f_8 = 101001101$. As the elements of the memory of linear shift registers, as a rule, $D-$triggers are used, the level of the signal at the output of which (0 or 1) after the synchronization pulse repeats the level of the signal fed to the input of the trigger.

As follows from the block diagram of the generator (Fig. 4.1), the feedbacks in the classical Galois generators (registers) of the maximum period are uniquely determined by the selected PP f_n of degree n and are formed in this way: the responses of each digit ($D-$trigger) SR are applied to the inputs of the subsequent digits, being for them excitation functions. In addition, the response of the upper register bit is fed (according to the XOR scheme) to the inputs of those and only those digits whose numbers coincide with the numbers of non-zero monomials of the PP. In this case, the lowest monomial, located on the right of the polynomial f_n, as well as the low order of the register, corresponds the number 1. Binary PPs f_n generate extended fields $GF(2^8)$ whose minimal primitive element θ is equal to 10. The sequence of powers of any primitive element θ of the Galois field modulo PP f_n, that is $\theta^k (\text{mod } f_n)$, $k = 0, 1, \ldots$, form a sequence of maximum length $L = 2^n - 1$ ($m-$sequence). A fragment of such a sequence for PP $f_8 = 101001101$ is presented in Table. 4.3.

Table 4.3. Fragment of a sequence of degrees element $\theta = 10$ modulo $f_8 = 101001101$

Degree	Register bits							
k	8	7	6	5	4	3	2	1
0	0	0	0	0	0	0	0	1
1	0	0	0	0	0	0	1	0
2	0	0	0	0	0	1	0	0
3	0	0	0	0	1	0	0	0
4	0	0	0	1	0	0	0	0
5	0	0	1	0	0	0	0	0
6	0	1	0	0	0	0	0	0
7	1	0	0	0	0	0	0	0
8	0	1	0	0	1	1	0	1
9	1	0	0	1	1	0	1	0
10	0	1	1	1	1	0	0	1
…	…	…	…	…	…	…	…	…
254	1	0	1	0	0	1	1	0
255	0	0	0	0	0	0	0	1

By direct verification it is easy to verify that the SR (Fig. 4.1) with feedbacks formed by the PP f_8 generates a sequence of register states that coincides with the $m-$sequence (Table 4.3).

Each linear SRLF generator of PRS of maximal period can be represented by an equivalent primitive Galois matrix $\boldsymbol{G}$ that forms the same $m-$sequence as the generator of PRS. We denote by $\boldsymbol{G}_f^{(n)}$ a two-dimensional Galois matrix of $n-$th order over an irreducible polynomial f_n that is not necessarily PP. With the help of the $\boldsymbol{G}_f^{(n)}$ we introduction the recursive calculation of states $S(t)$ of the register at discrete moments of time t:

$$S(t)=S(t-1)\cdot\boldsymbol{G}_f^{(n)},\quad t=1,2,\ldots,\quad S(0)=00000001. \tag{4.1}$$

The vector $S(0)$ in (4.1) the lower line is highlighted (we assign to it the number 1) of the matrix $\boldsymbol{G}_f^{(8)}$. Therefore, in the bottom row of the matrix $\boldsymbol{G}_f^{(8)}$, it is necessary to write down (according to Table 4.3) a value $S(1)=10$ that coincides with the minimum generating element (GE) $\theta=10$ of the field $GF(2^8)$ over the PP $f_8=101001101$.

Relation $S(2)=S(1)\cdot\boldsymbol{G}_f^{(n)}$ the second (bottom) row of the matrix is determined $\boldsymbol{G}_f^{(n)}$, which, according to Table. 1, regardless of the PP, or simply the NP, should be equal to 100. Continuing the calculations, we arrive at the matrix

$$\boldsymbol{G}_f^{(8)}=\begin{pmatrix}0&1&0&0&1&1&0&1\\1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&1&0\end{pmatrix}\begin{matrix}8\\7\\6\\5\\4\\3\\2\\1\end{matrix}\quad\begin{matrix}\\\\\\\\\cdot\\\\\\\\\end{matrix}\tag{4.2}$$

$$\begin{matrix}8&7&6&5&4&3&2&1\end{matrix}$$

In accordance with expression (4.2), the synthesis algorithm for classical Galois matrices can be formulated as follows. Let f_n- be a vector form of a PP of degree $n-$ such that

$$f_n=\{1,\alpha_{n-1},\alpha_{n-2},\ldots,\alpha_2,\alpha_1,1\},\quad \alpha_i\in\{0,1\},\quad i=\overline{1,n-1}, \tag{4.3}$$

and $\theta=10-$ minimal GE field of the $GF(2^n)$ over the PP f_n. We put GE 10 on the right in the bottom line of the Galois matrix and fill the elements of the matrix,

adhering to a simple rule. We put the units in the elements of the diagonal located below the main diagonal of the matrix, and in the remaining elements of the matrix $\boldsymbol{G}_f^{(n)}$, except the top line, we write zeros. The upper line of the matrix should be expected to appear $(n+1)-$ bit vector is 100 ... 0. But this is inadmissible, since the order of the matrix is n. Reducing such a vector to the remainder modulo f_n, we arrive at the fact that in the upper row of the matrix $\boldsymbol{G}_f^{(n)}$ should place PP f_n, represented in (4.3), excluding its highest unit, that is, $n-$bit vector $\alpha_{n-1}, \alpha_{n-2}, \ldots, \alpha_2, \alpha_1, 1$.

On the basis of the proposed method, we call it the *method of diagonal filling*, we obtain the general form of the classical Galois matrix of $n-$ th order

$$\boldsymbol{G}_f^{(n)} = \begin{pmatrix} \alpha_{n-1} & \alpha_{n-2} & \cdots & \alpha_2 & \alpha_1 & 1 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix}. \qquad (4.4)$$

Matrices $\boldsymbol{G}_f^{(n)}$ over the PP f_n are one-to-one connected with Fibonacci matrices $\boldsymbol{F}_f^{(n)}$ by the operator $\perp$ of the *right-sided transpose*

$$\boldsymbol{G} \overset{\perp}{\longleftrightarrow} \boldsymbol{F}, \qquad (4.5)$$

i.e. transposition with respect to the auxiliary diagonal.

$$\boldsymbol{F}_f^{(n)} = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 & \alpha_1 \\ 0 & 1 & \cdots & 0 & 0 & \alpha_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & \alpha_{n-2} \\ 0 & 0 & \cdots & 0 & 1 & \alpha_{n-1} \end{pmatrix}. \qquad (4.6)$$

A particular variant of the Fibonacci matrix over a primitive polynomial of the eighth order $f_8 = 101001101$ is determined by the relation

$$\boldsymbol{F}_f^{(8)} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} 8 \\ 7 \\ 6 \\ 5 \\ 4 \\ 3 \\ 2 \\ 1 \end{matrix}. \qquad (4.7)$$

$$8 \quad 7 \quad 6 \quad 5 \quad 4 \quad 3 \quad 2 \quad 1$$

An example of a classical Fibonacci generator of the eighth order forming the PRS of the maximum period is shown in Fig. 4.2.

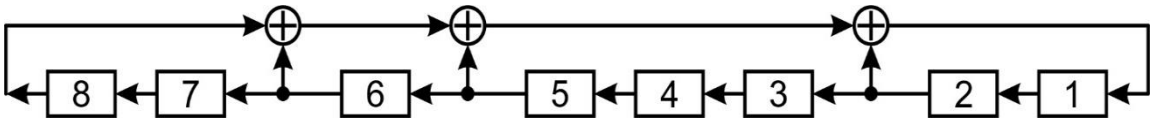

Figure 4.2. Structural scheme of PRS generator by the Fibonacci scheme over primitive polynomial $f_8 = 101001101$

Matrix (4.4) and (4.6) are special cases of Frobenius canonical matrix

$$\boldsymbol{\Phi} = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & 0 & -a_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & -a_{n-2} \\ 0 & 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}.$$

Such a matrix is also called an *accompanying one for the polynomial*.

$$f(x) = x^n - \alpha_{n-1}x^{n-1} - \alpha_{n-2}x^{n-2} - \ldots - \alpha_1 .$$

If $f(x) = f_n(x)$ is the primitive binary polynomial of the $n-$degree, then

$$f_n(x) = x^n + \alpha_{n-1}x^{n-1} + \alpha_{n-2}x^{n-2} + \cdots + \alpha_0, \quad \alpha_i \in \{0,1\}. \qquad (4.8)$$

Frobenius matrix corresponding to the PP (4.8), there is nothing more than a Fibonacci matrix

$$\boldsymbol{F}_f^{(n)} = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & a_0 \\ 1 & 0 & \cdots & 0 & 0 & a_1 \\ 0 & 1 & \cdots & 0 & 0 & a_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & a_{n-2} \\ 0 & 0 & \cdots & 0 & 1 & a_{n-1} \end{pmatrix}. \qquad (4.9)$$

Transposing the matrix (4.9) with respect to the auxiliary diagonal we come to the Galois matrix

$$\boldsymbol{G}_f^{(n)} = \begin{pmatrix} a_{n-1} & a_{n-2} & \cdots & a_2 & a_1 & a_0 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix}. \qquad (4.10)$$

The matrices (4.4) and (4.6), whose first-born matrices are the matrices (4.10) and (4.9), respectively, are used to construct the SRLFB according to the Galois and Fibonacci schemes over primitive polynomials. It is precisely such matrices $\boldsymbol{G}$ and $\boldsymbol{F}$ we will call the classical Galois and Fibonacci matrices.

The PRS generator in the Fibonacci configuration generates a binary $m-$ sequence of PRNs having the same statistical properties as the sequence of numbers generated by the Galois generator. To confirm the above thesis, let us consider, as an example, classical fourth-order Galois and Fibonacci PRNs generators (Figures 4.3 and 4.4), the feedback links to which are formed by a primitive polynomial of the fourth degree $f_4 = 10011$.

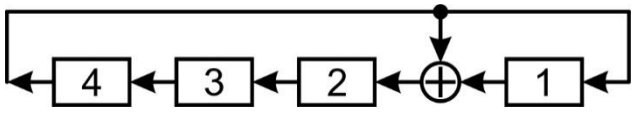

Figure 4.3. Block diagram of the generator of PRNs by the Galois scheme over PP $f_4 = 10011$

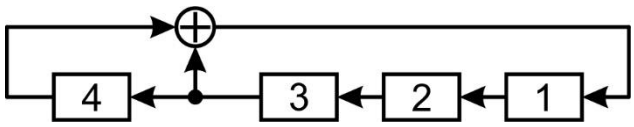

Figure 4.4. Block diagram of the generator of PRNs by the Fibonacci scheme over PP $f_4 = 10011$

Galois and Fibonacci matrices of the forth order over PrP $f_4 = 10011$ have the form:

$$\boldsymbol{G}_f^{(4)} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad (4.11); \qquad \boldsymbol{F}_f^{(4)} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \qquad (4.12)$$

Non-zero sequences of binary semi-bytes (call their Galois $\boldsymbol{G}_f$ and Fibonacci $\boldsymbol{F}_f$ sequences) over the primitive polynomial $f_4 = 10011$ are summarized in Table. 4.4 and are constructed either directly from the structural circuits of the generators (Figures 4.3 and 4.4), or based on the recurrence relations (4.1) with respect to the matrices (4.11) and (4.12).

Table 4.4. Sequences of non-zero binary semi-bytes Galois and Fibonacci over PrP $f_4 = 10011$

t	$\boldsymbol{G}_f$				$\boldsymbol{F}_f$			
	4	3	2	1	4	3	2	1
0	0	0	0	1↓	0	0	0	1
1	0	0	1	0	0	0	1	0
2	0	1	0	0	0	1	0	0
3	1	0	0	0	1	0	0	1
4	0	0	1	1	0	0	1	1
5	0	1	1	0	0	1	1	0
6	1	1	0	0	1	1	0	1
7	1	0	1	1	1	0	1	0
8	0	1	0	1	0	1	0	1
9	1	0	1	0	1	0	1	1
10	0	1	1	1	0	1	1	1
11	1	1	1	0	1	1	1	1↓
12	1	1	1	1	1	1	1	0
13	1	1	0	1	1	1	0	0
14	1	0	0	1	1	0	0	0
15	0	0	0	1	0	0	0	1

Let's pay attention to such features of the data presented in tab. 4.4. First, if under the discrete time in the left column of Table. 4.4. to understand the degree k of the primitive generative element $\theta = 10$ modulo PrP $f_4 = 10011$, then the collection of columns 1-4, united by a symbol $\boldsymbol{G}_f$, is the multiplicative group of the Galois field $GF(2^4)$ over the primitive polynomial $f_4 = 10011$. And, secondly, assuming that the output bits of the PRS generators are removed (Figures 4.3 and 4.4) from the output of their extreme right-hand bits (triggers), we see that the bit sequence formed by the Fibonacci generator coincides with the Galois generator sequence, but cyclically shifted by 11 counts down the column.

The lower shaded row of Table. 4.4 ($t = 15$) repeats its upper line ($t = 0$) and is excluded from the cyclic shift. The coincidence of sequences formed by Galois and Fibonacci generators can be easily traced by the starting elements (shaded and marked with the symbol $\downarrow$).

4.3. Related matrix and generators of Galois

Relation (4.5), in which the right-transposition (i.e., rotation of the matrix with respect to the auxiliary diagonal) matrix Galois converted into Fibonacci matrix leads to the following reflection. There are no objective reasons for which the classical (left-hand) matrix transposition Galois (or Fibonacci) to bring the properties of the transformed matrix, different from those that are generated by right-transposition. This means, in particular, that if, for example, $\boldsymbol{G}_f$ - a primitive matrix, then not only $\boldsymbol{G}_f^{T}$, but also $\boldsymbol{G}_f^{T\perp}$ - also primitive matrices.

Denote by ${}^{*}\boldsymbol{G}_f$ (${}^{*}\boldsymbol{F}_f$) - the matrices formed by the combination of the classical (left-sided) and right-sided transpositions of the Galois (Fibonacci) matrices of $n-$order over the PP f_n, that is,

$$\begin{aligned} {}^{*}\boldsymbol{G}_f &= \boldsymbol{G}_f^{T\perp} = \boldsymbol{G}_f^{\perp T}; \\ {}^{*}\boldsymbol{F}_f &= \boldsymbol{F}_f^{T\perp} = \boldsymbol{F}_f^{T\perp}. \end{aligned} \tag{4.13}$$

Relations (4.13) emphasize the fact that operations of left- and right-hand transposition are commutative and, as a consequence,

$$\begin{aligned} T \perp T &= \perp; \\ \perp T \perp &= T. \end{aligned} \tag{4.14}$$

Thus, pairs of Galois matrices ($\boldsymbol{G}$ and ${}^{*}\boldsymbol{G}$), like Fibonacci ($\boldsymbol{F}$ and ${}^{*}\boldsymbol{F}$), are connected by a one-to-one (bijective) relation

$$\begin{aligned} \boldsymbol{G} &\xleftrightarrow{T\perp} {}^{*}\boldsymbol{G}; \\ \boldsymbol{F} &\xleftrightarrow{T\perp} {}^{*}\boldsymbol{F}. \end{aligned} \tag{4.15}$$

The introduced Galois ${}^{*}\boldsymbol{G}$ and Fibonacci ${}^{*}\boldsymbol{F}$ matrices are said to be conjugate to the base matrices $\boldsymbol{G}$ and $\boldsymbol{F}$, respectively.

Let us pay attention to the fact that in algebra (in the section of group theory) the term "conjugate element" is connected by such a definition.

Definition 4.1. *An element x^{*} of a certain group X is a conjugate to the element x of the same group if there exists an element $z \in X$ such that*

$${}^{*}x = z^{-1} \cdot x \cdot z. \tag{4.16}$$

The transformation (4.16) is called the conjugation, and the elements x and ${}^{*}x$, which can be matrices, are conjugate (or dual) elements (matrices).

A comparison of expressions (4.13), (4.15) and (4.16) it is clear that the proposed definition of "conjugate matrix," differs from the definition adopted in algebra.

The general forms of classical conjugate matrices of the $n-$order, in accordance with (4.4), (4.6) and (4.13) or (4.15), are given by the relations:

$${}^{*}\boldsymbol{G}_{f}^{(n)} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & \alpha_1 & \alpha_2 & \cdots & \alpha_{n-2} & \alpha_{n-1} \end{pmatrix}; \tag{4.17}$$

and

$$ {}^{*}\boldsymbol{F}_{f}^{(n)} = \begin{pmatrix} \alpha_{n-1} & 1 & 0 & \cdots & 0 & 0 \\ \alpha_{n-2} & 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \alpha_{2} & 0 & 0 & \cdots & 1 & 0 \\ \alpha_{1} & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}. \qquad (4.18) $$

In particular, the conjugate Galois matrix of the eighth order over the primitive polynomial $f_8 = 101001101$ has the form:

$$ {}^{*}\boldsymbol{G}_{f}^{(8)} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} 8 \\ 7 \\ 6 \\ 5 \\ 4 \\ 3 \\ 2 \\ 1 \end{matrix} \cdot \qquad (4.19) $$

$$ \begin{matrix} 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{matrix} $$

Structurally-logic circuit of the Galois conjugate generator that meets the matrix (4.19) is shown in Fig. 4.5.

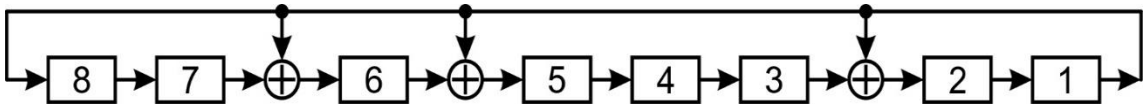

Figure 4.5. The block diagram of the dual generator PRS by Galois scheme over primitive polynomial

The conjugate Fibonacci matrix of the eighth order over the PP $f_8 = 101001101$ is determined by the expression

$$
{}^{*}\boldsymbol{F}_{f}^{(8)} = \begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix} \begin{matrix} 8 \\ 7 \\ 6 \\ 5 \\ 4 \\ 3 \\ 2 \\ 1 \end{matrix}
$$
$$
8 \quad 7 \quad 6 \quad 5 \quad 4 \quad 3 \quad 2 \quad 1 \qquad (4.20)
$$

and the circuit of the PRS generator corresponding to the matrix (4.20) is shown in Fig. 4.6.

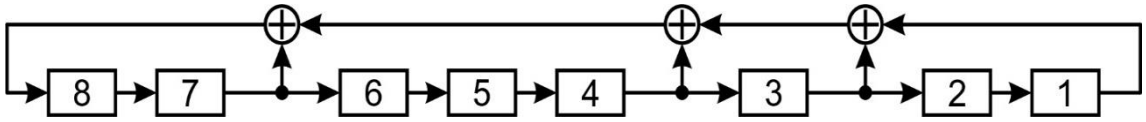

Figure 4.6. The block diagram of the dual oscillator CAP Fibonacci chart above primitive polynomial

The collection of basic and associated Galois and Fibonacci matrices can conditionally displayed graphically as shown in Fig. 4.7.

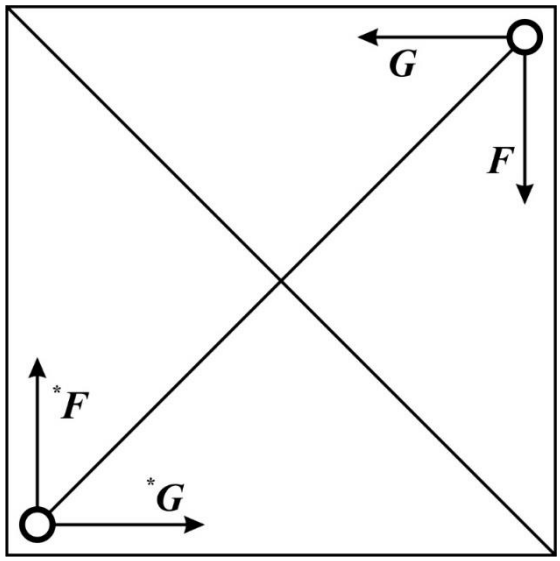

Figure 4.7. Related graphic display of Galois and Fibonacci matrices

The arrows in Fig. 4.7 indicate the directions in the rows or columns of the matrices over which the coefficients α_k, $k = \overline{0, n}$ of the primitive polynomials f_n are arranged, starting with the lower coefficient α_0 in the direction of the higher one α_{n-1}.

A circle indicates the angular elements of the matrices in which the coefficients α_0 equal to one are placed. For example, a vector marked with a symbol $\boldsymbol{G}_f$ symbolizes the fact that the coefficients of the polynomial f_n generating the Galois matrix are written to the upper row of the matrix from right to left, with a coefficient α_0 equal to 1 placed in the upper right corner of the matrix.

Consider another vector, for example, one that is marked with a symbol ${}^*\boldsymbol{G}_f$. The interpretation of this vector is as follows. In the conjugate Galois matrix, the generating polynomial f_n is located in the left column of the matrix, and the lowest coefficient α_0 of the polynomial must be inscribed in the lower-left corner of the matrix.

Symbolic display of Galois and Fibonacci matrices presented on Fig. 4.7 makes it possible to establish the relationship (Table. 4.5) of the four matrices included in the group under consideration.

Table 4.5. Interrelation of Galois and Fibonacci matrices

	$\boldsymbol{G}$	$\boldsymbol{F}$	${}^*\boldsymbol{G}$	${}^*\boldsymbol{F}$
$\boldsymbol{G}$	–	⊥	⊥ T	T
$\boldsymbol{F}$	⊥	–	T	⊥ T
${}^*\boldsymbol{G}$	⊥ T	T	–	⊥
${}^*\boldsymbol{F}$	T	⊥ T	⊥	–

Referring to Fig. 4.7, it seems that the square is half-empty and, as a consequence, there is a desire to supplement the main vectors of the axis, similar to those found on the secondary diagonal of the square. This expansion of the number of vectors (matrices) based on the hypothetical assumption that the newly formed matrix primitiveness retain properties that have the matrix of the initial set of reference and associated matrices Galois and Fibonacci. Designated addition may be accomplished, for example, the operation of the inverse column permutation matrices $\boldsymbol{M} \in \left\{\boldsymbol{G}, {}^*\boldsymbol{G}, \boldsymbol{F}, {}^*\boldsymbol{F}\right\}$, as indicated on Fig. 4.8.

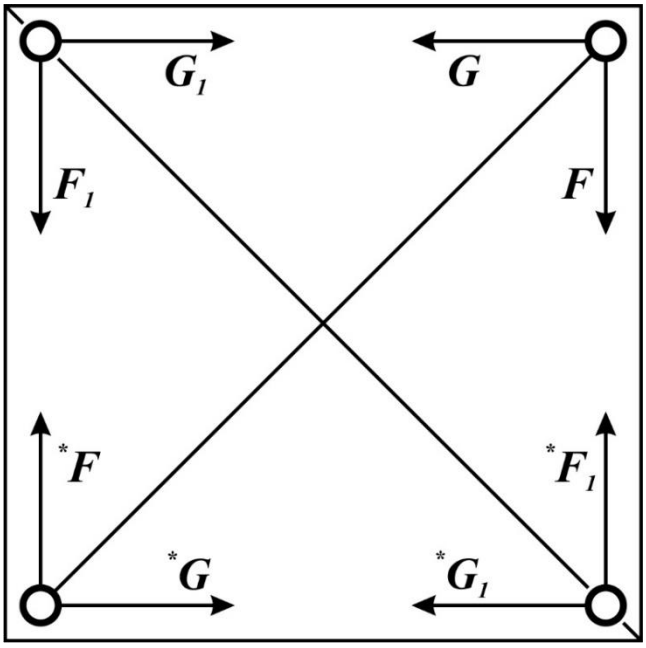

Figure 4.8. Extension (1) of the conditional-graphic Display of Galois and Fibonacci matrices

Mathematically, the operation of inverse column permutation of any square matrix $\boldsymbol{M}$ can be realized by transformation

$$\boldsymbol{M}1 = \boldsymbol{M} \cdot \mathbf{1}, \tag{4.21}$$

where $\mathbf{1}$ is the matrix (operator) of the inverse permutation (MIP), which, for example, of the fourth order, has the form

$$\mathbf{1} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}. \tag{4.22}$$

We show further that the inverse permutation of the columns of a primitive Galois matrix leads to loss of the primitiveness of the newly formed matrix. In fact, let

$$\boldsymbol{G}1 = \boldsymbol{G} \cdot \mathbf{1}, \tag{4.23}$$

where $\boldsymbol{G}$ is the Galois matrix of the fourth order over PP $f_4 = 10011$

$$\boldsymbol{G} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \qquad (4.24)$$

On the basis of relations (4.22) - (4.24) we obtain

$$\boldsymbol{G}1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}. \qquad (4.25)$$

The sequence of powers of the matrix (4.25) composes series

$$\boldsymbol{G}1^1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}; \ \boldsymbol{G}1^2 = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}; \ \boldsymbol{G}1^3 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \qquad (4.26)$$

in which the elements are omitted

$$\boldsymbol{G}1^0 = \boldsymbol{E} \ \text{ and } \boldsymbol{G}1^4 = \boldsymbol{E}. \qquad (4.27)$$

The set of matrices (4.26) and (4.27) form a fourth-order group.

Exactly to the same results come by inverse column permutation of Fibonacci matrices. That is, as a consequence of the conversion That is, as a consequence of the transformation

$$\boldsymbol{F}1 = \boldsymbol{F} \cdot \mathbf{1},$$

for example, a matrix of the fourth order $\boldsymbol{F}$, which is the generator of the multiplicative group of the 15th order, we arrive to a matrix $\boldsymbol{F}1$ generating, like the matrix $\boldsymbol{G}1$, a multiplicative group of the fourth order.

Extensions of the number of Galois and Fibonacci matrices (both basic and conjugate) can be achieved not only by inverse permutation of their columns, but also by an inverse permutation of the rows of these matrices (we denote the original matrices by $\boldsymbol{M}$), which is realized by the transformation,

$$\boldsymbol{M}2 = \mathbf{1} \cdot \boldsymbol{M},$$

shown in Fig. 4.9.

It is easy to see that matrices $\boldsymbol{M}2$ have the same singularities as matrices $\boldsymbol{M}1$. In particular, if $\boldsymbol{G}$ there is a fourth-order Galois matrix, then, constructed on the basis of the matrix $\boldsymbol{G}$ matrices $\boldsymbol{G}1$, ${}^{*}\boldsymbol{G}1$, $\boldsymbol{F}1$ and ${}^{*}\boldsymbol{F}1$, as well as the matrices $\boldsymbol{G}2$, ${}^{*}\boldsymbol{G}2$, $\boldsymbol{F}2$ and ${}^{*}\boldsymbol{F}2$, will be the generating matrices of the multiplicative groups of the fourth order.

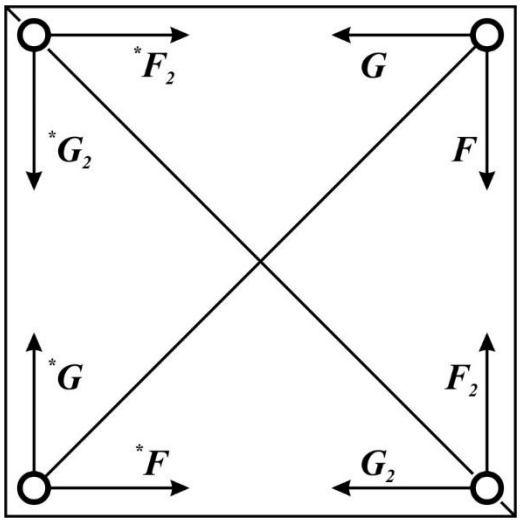

Figure 4.9. Extension (2) of the conditional-graphic display of Galois and Fibonacci matrices

Thus, the multiplication of the square matrix $\boldsymbol{M}$ by the MIB on the left is equivalent to the inversion of the rows of the matrix $\boldsymbol{M}$, and to the right - the inversion of the columns of this matrix. Consequently, the conjugate matrix $\boldsymbol{M}^{*}$ can be obtained from the matrix $\boldsymbol{M}$ by a joint inversion of its rows and columns performed in any sequence or otherwise

$$\begin{aligned} {}^{*}\boldsymbol{G}_f &= \mathbf{1}\cdot\boldsymbol{G}_f\cdot\mathbf{1}; \quad \boldsymbol{G}_f = \mathbf{1}\cdot{}^{*}\boldsymbol{G}_f\cdot\mathbf{1}; \\ {}^{*}\boldsymbol{F}_f &= \mathbf{1}\cdot\boldsymbol{F}_f\cdot\mathbf{1}; \quad \boldsymbol{F}_f = \mathbf{1}\cdot{}^{*}\boldsymbol{F}_f\cdot\mathbf{1}. \end{aligned} \tag{4.28}$$

According to the one-to-one correspondence (4.28), any of the matrices considered (basic $\boldsymbol{M}$ or conjugate $\boldsymbol{M}^{*}$) can be obtained as a result of a similarity transformation of another matrix, that is,

$$\boldsymbol{G} \xleftrightarrow{1\Diamond 1} {}^{*}\boldsymbol{G};$$
$$\boldsymbol{F} \xleftrightarrow{1\Diamond 1} {}^{*}\boldsymbol{F},$$

where the symbol $\mathbf{1}\Diamond\mathbf{1}$ means transformations over matrices, similar to the transformations (4.28).

All information relatively $q_k(t)$ is contained in the corresponding base or conjugated matrices and is determined by the elementary relation

$$q_k(t+1) = \bigoplus_{i=1}^{n} h_{i,k} \cdot s_i(t),$$

where $h_{i,k}$ are the elements of the transformation matrix (the Galois or Fibonachi matrices), the rows of matrices being numbered from bottom to top, and the columns from right to left starting at number 1; $s_i(t)$ - the state of the i-th trigger at the time t.

4.4. Feedbacks in Galois generators

We note that if the basic generators of the PRN, which are shown in Fig. 4.1 and 4.2, the feedback circuit (OS) "twisted" in a clockwise direction, the conjugate generators (Figure 4.5 and 4.6.) - Counterclockwise. General rules for the conversion of linear circuits operating the generator to the well-known schemes feedbacks any of the remaining generators are summarized in Table. 4.6.

Table 4.6. transformation operators of feedback in generators PRS

	G	F	${}^{*}G$	${}^{*}F$
G	–	1∘1	∘1	1∘
F	1∘1	–	1∘	∘1
${}^{*}G$	∘1	1∘	–	1∘1
${}^{*}F$	1∘	∘1	1∘1	–

The meaning of the term "feedback circuit" PR- generators of PRS (on generators example, block diagrams of which are shown in Fig. 4.1, 4.2, 4.5 and 4.6) can be explained by referring to their stylized display, shown in Fig. 4.10.

In contrast to Table. 4.5, in which by symbols $G, {}^{*}G, F$ and ${}^{*}F$ denote the primitive matrix of the PRS generators, in Table. 4.6 by the same symbols are schematically indicated schemes of feedbacks in the corresponding generators.

The meaning of the term "feedback circuits" of PR-generators of PRS (using the example of generators whose block diagrams are presented in Figures 4.1, 4.2, 4.5 and 4.6) can be explained by referring to their stylized display shown in Fig. 4.10.

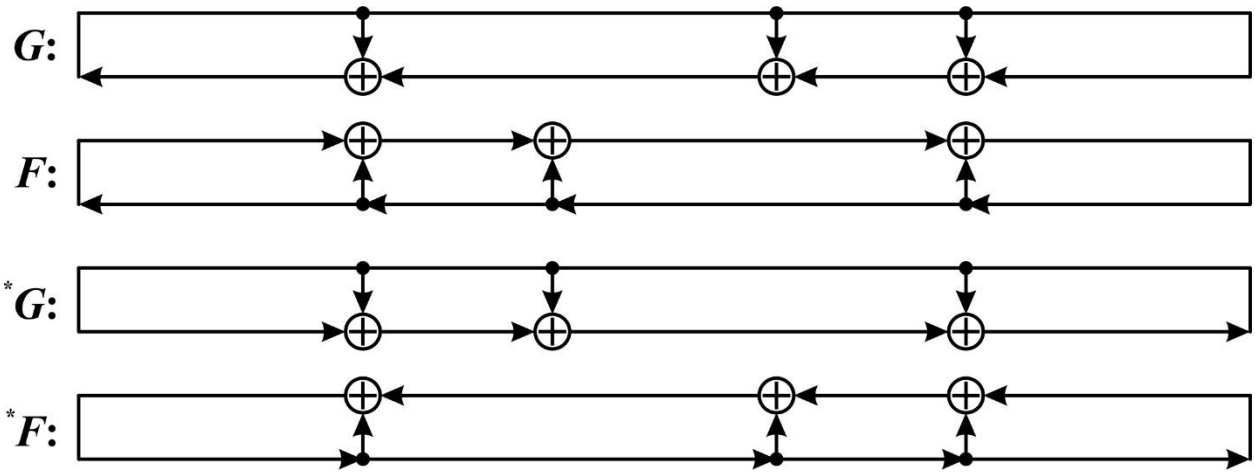

Figure 4.10. The stylized representation feedbacks in PR-generators of PRS

Let's pay attention to such features of the connections shown in Fig. 4.10, in the considered PRS generators. The feedback in the registers of the basic generators $\boldsymbol{G}$ and $\boldsymbol{F}$ is carried out in the clockwise direction, while in the registers of the conjugate generators ${}^{*}\boldsymbol{G}$ and ${}^{*}\boldsymbol{F}$ - in the counterclockwise direction.

Let us clarify the physical meaning of the transformation operators in Table. 4.6. The operator $\circ 1$ means that the feedback scheme, indicated by a symbol $\circ$, undergoes rotation on 180° relatively vertical axis. Such transformations occur, as follows from Fig. 4.10, in pairs of generators $(\boldsymbol{G}, {}^{*}\boldsymbol{G})$ or $(\boldsymbol{F}, {}^{*}\boldsymbol{F})$. The operation $\circ 1$ is similar to the operation of inverse permutation of columns of the matrix $\boldsymbol{M}$, which is realized if we multiply it from the right by the inverse permutation matrix. The operator $1\circ$ rotates the feedback circuit relative to the horizontal axis. Thus, the operation $1\circ$ is similar to the operation of inverse permutation of rows of the matrix $\boldsymbol{M}$, if we multiply it from the left by the inverse permutation matrix. These transformations of feedbacks take place in the pairs of generators $(\boldsymbol{G}, {}^{*}\boldsymbol{F})$ or $(\boldsymbol{F}, {}^{*}\boldsymbol{G})$. And, finally, the operator $1\circ 1$ means that the feedback circuit undergoes rotation on 180° a relatively vertical and horizontal axes. Such transformations of feedback circuits are performed in pairs of generator $(\boldsymbol{G}, \boldsymbol{F})$ or $({}^{*}\boldsymbol{G}, {}^{*}\boldsymbol{F})$.

4.5. Generalized matrices and Galois generators over field *GF*(2)

In the section of the section below we propose an algorithm for constructing Galois matrices $\boldsymbol{G}_{f,\omega}^{(n)}$, as forming elements of which are applied elements

$\omega \geq p = 10$ of the field $GF(2^n)$ over arbitrary irreducible polynomials f_n (not necessarily primitive) degrees n.

We first introduce the definition of generalized Galois matrices (GGM).

Definition 4.2. *We call generalized Galois matrices* $\boldsymbol{G}_{f,\omega}^{(n)}$ *of* $n-$ *th order, forming an element of which* ω *is not necessarily a primitive element* θ *of the field* $GF(2^n)$ *generated by an arbitrary irreducible polynomial* f_n *degree* n.

To solve the matrix synthesis problem $\boldsymbol{G}_{f,\omega}^{(n)}$ we use the generalized rule of diagonal filling, the essence of which is as follows. Let $\omega-$ Forming an element of the matrix, which can be chosen as any element of the field $GF(2^n)$, generated NPLP f_n. OE ω is written to the right in the lower (first) row of the matrix being formed. Elements of this line, located to the left ω, are filled with zeros. The subsequent rows of the matrix (in the direction of the bottom-up) will be obtained by shifting the previous row one digit to the left. If, at the same time, the highest nonzero bit of the string is outside the matrix, then the vectors corresponding to such rows are reduced to the remainder modulo the NP f_n and, thus, the row of the matrix also becomes $n-$ bit.

Let $n = 6$, $f_6 = 1011011$ and $\omega = 11001$. We come to the generalized Galois matrix

$$\boldsymbol{G}_{f,\omega}^{(6)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}. \qquad (4.29)$$

OMG $\boldsymbol{G}$ corresponds to the generalized Fibonacci matrix $\boldsymbol{F}$, formed by the operator of right-sided transposition $\perp$ matrix (4.29), that is,

$$\boldsymbol{G}_{f,\omega}^{(6)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}. \tag{4.30}$$

Operator $1\circ 1$ The matrices (4.29) and (4.30) can easily be transformed into generalized conjugate Galois matrices ${}^{*}\boldsymbol{G}$ or Fibonacci ${}^{*}\boldsymbol{F}$.

Let us consider an example of synthesis of generalized primitive matrices and Galois generators, choosing as an irreducible binary polynomial of the fourth degree $f_4 = 11111$, which is not primitive, and a primitive OE $\omega = \theta_1$ polynomial f_4, equal to 111. The matrices corresponding to the chosen parameters have the form:

$$\boldsymbol{G}1_{f,\omega}^{(4)} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}; \qquad \boldsymbol{F}1_{f,\omega}^{(4)} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix};$$

$$\tag{4.31}$$

$${}^{*}\boldsymbol{G}1_{f,\omega}^{(4)} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}; \qquad {}^{*}\boldsymbol{F}1_{f,\omega}^{(4)} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

The block diagram of the generalized basic four-digit Galois generator corresponding to the GGM $\boldsymbol{G}1_{f,\omega}^{(4)}$, is shown in Fig. 4.11. Vertically located registers of generators marked with a symbol above $\otimes$, implement the bitwise multiplication operation, and the registers marked with the symbol $\oplus$ — the operation of adding the contents of the register modulo 2.

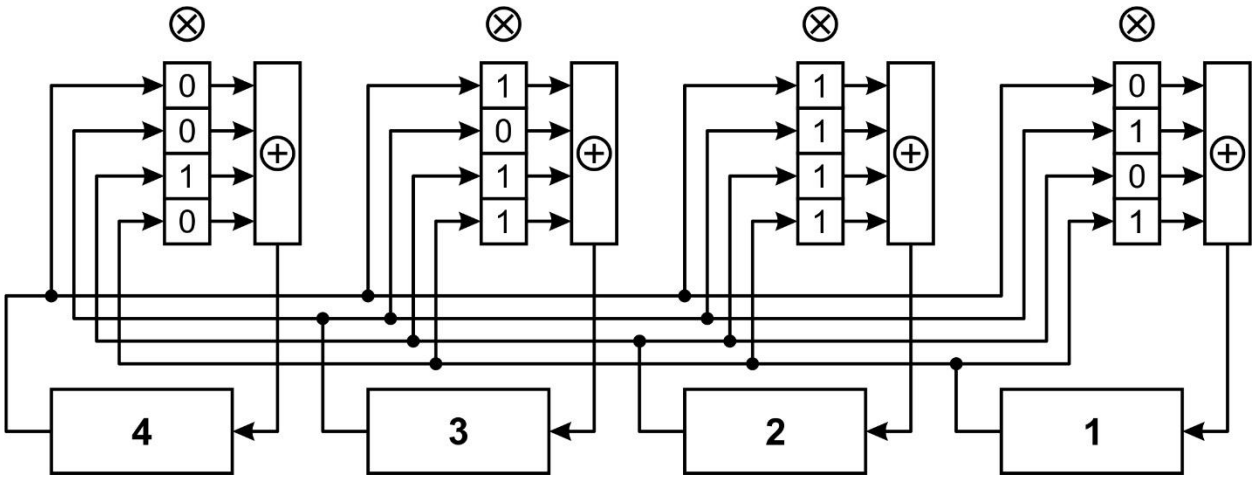

Figure 4.11. Block diagram of a generalized base generator of Galois PRS

The Galois generator (Figure 4.11) is converted into a Fibonacci generator by replacing the contents of the registers $\otimes$ with columns of the matrix $\boldsymbol{F}1_{f,\omega}^{(4)}$ of the system (4.31). The scheme of the generalized PRS generator in the Fibonacci configuration is shown in Fig. 4.12.

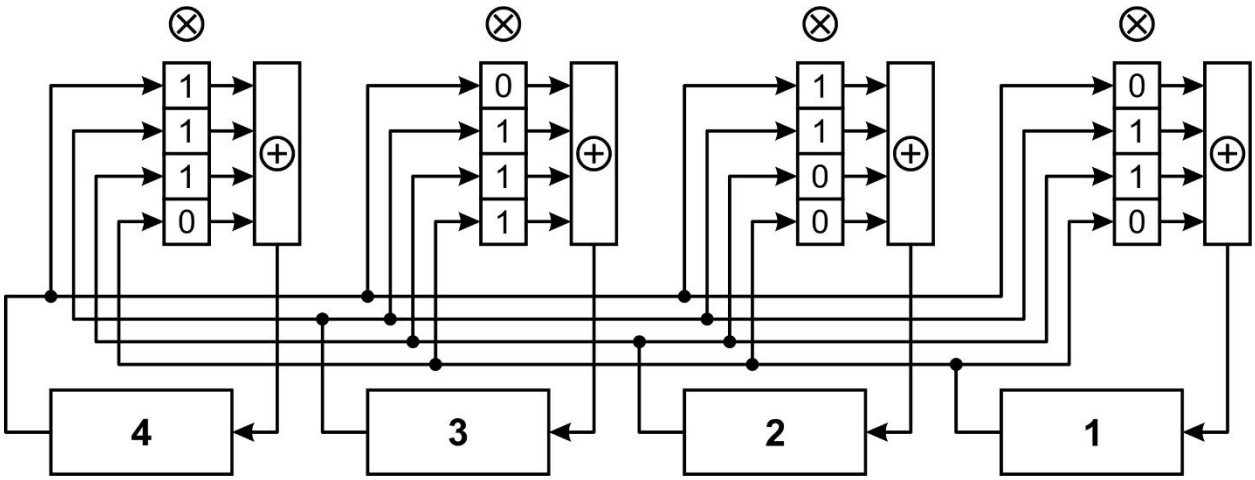

Figure 4.12. Block diagram of a generalized base generator of Fibonacci PRS

Similarly to the basic PRS generators, if in the registers of multiplication of the structural diagram in Fig. 4.11 to place the elements of the columns of the matrix ${}^{*}\boldsymbol{G}1_{f,\omega}^{(4)}$, then we get the generalized conjugate PRS generator according to the Galois scheme (Fig. 4.13). In the case when the elements of the matrix ${}^{*}\boldsymbol{F}1_{f,\omega}^{(4)}$ are placed in the same registers, a conjugate generator of the memory bandwidth in the Fibonacci configuration is formed (Figure 4.14).

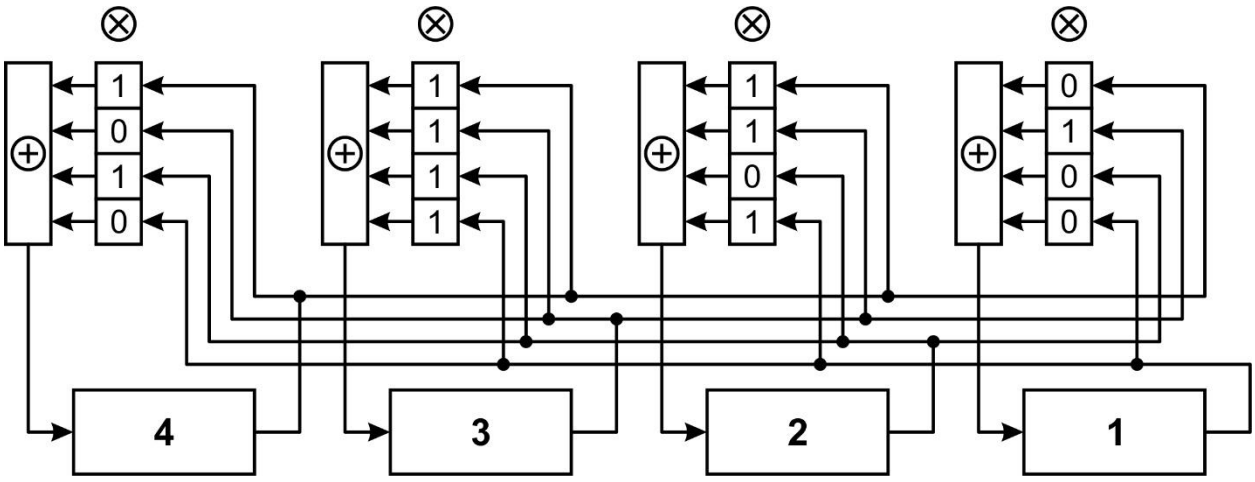

Figure 4.13. Block diagram of a generalized conjugate generator of Galois PRS

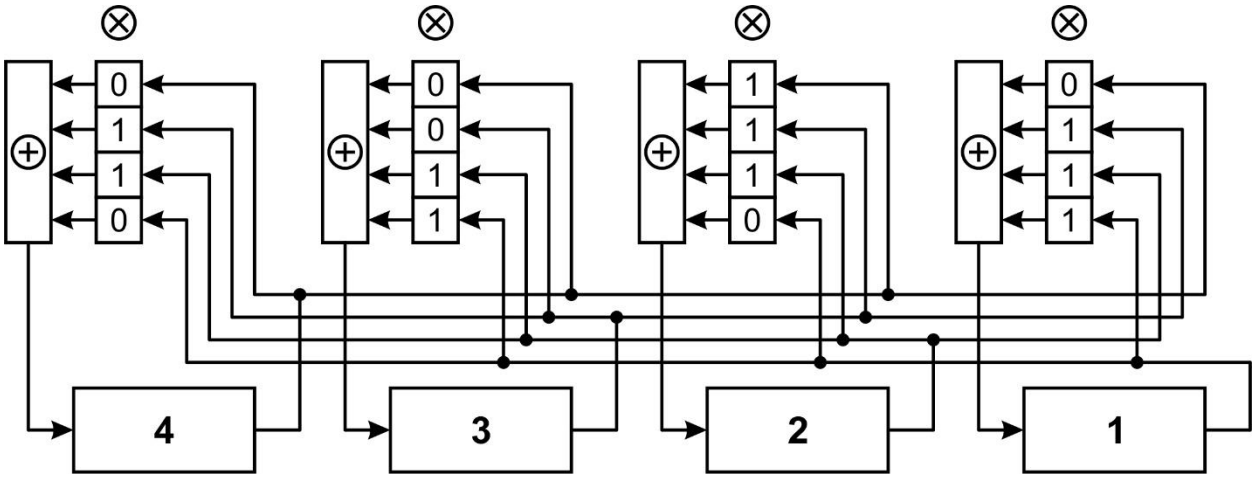

Figure 4.14. Block diagram of a generalized conjugate generator of Fibonacci PRS

Generalized primitive matrices belonging to the same group (Galois or Fibonacci) have a remarkable commutativity property, the essence of which is explained below. Let $\omega = \theta_2 = 1011$ be the second primitive element of the field $GF(2^4)$, different from the GE $\theta_1 = 111$. To forming element θ_2 corresponds such set of primitive matrices:

$$\boldsymbol{G}2^{(4)}_{f,\omega} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}; \qquad \boldsymbol{F}2^{(4)}_{f,\omega} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}. \tag{4.32}$$

$$^{*}\boldsymbol{G}2^{(4)}_{f,\omega} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}; \qquad ^{*}\boldsymbol{F}2^{(4)}_{f,\omega} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}. \tag{4.33}$$

In the set of primitive matrices (4.31) - (4.33) one can select commutative and non-commutative matrices. Any pair of matrices belonging to one of two groups of homogeneous primitive matrices is commutative. The first homogeneous group is made up of the Galois matrices ($\boldsymbol{G}-$group), into which the primitive matrices $\boldsymbol{G} = \{\boldsymbol{G}1, \boldsymbol{G}2, {}^{*}\boldsymbol{G}1, {}^{*}\boldsymbol{G}2\}$ enter. The second ($\boldsymbol{F}-$group) includes primitive Fibonacci matrices $\boldsymbol{F} = \{\boldsymbol{F}1, \boldsymbol{F}2, {}^{*}\boldsymbol{F}1, {}^{*}\boldsymbol{F}2\}$. Thus, for example, the matrix $\boldsymbol{G}1$ is commutative with any of the three matrices $\boldsymbol{G}2, {}^{*}\boldsymbol{G}1$ or ${}^{*}\boldsymbol{G}2$, but not commutative with any of the primitive matrices included in the $\boldsymbol{F}-$group, as shown in Table. 4.7.

Table 4.7. Signs of commutativity primitive matrices

	$\boldsymbol{G}1$	$\boldsymbol{F}1$	${}^{*}\boldsymbol{G}1$	${}^{*}\boldsymbol{F}1$	$\boldsymbol{G}2$	$\boldsymbol{F}2$	${}^{*}\boldsymbol{G}2$	${}^{*}\boldsymbol{F}2$
$\boldsymbol{G}1$	×	–	+	–	+	–	+	–
$\boldsymbol{F}1$	–	×	–	+	–	+	–	+
${}^{*}\boldsymbol{G}1$	+	–	×	–	+	–	+	–
${}^{*}\boldsymbol{F}1$	–	+	–	×	–	+	–	+
$\boldsymbol{G}2$	+	–	+	–	×	–	+	–
$\boldsymbol{F}2$	–	+	–	+	–	×	–	+
${}^{*}\boldsymbol{G}2$	+	–	+	–	+	–	×	–
${}^{*}\boldsymbol{F}2$	–	+	–	+	–	+	–	×

Signs + are placed in the elements of Table. 4.7, which are located at the intersection of commutative matrices, and signs – on the intersection of non-commutative matrices.

4.6. Isomorphism of Galois matrices

According to the above rule of diagonal filling at the initial stage of matrix $\boldsymbol{G}_{f,\omega}^{(n)}$ synthesis, the forming element ω is placed in the lower (right) digits of the lower row of the matrix of $n-$order. The subsequent rows of the matrix (bottom-up) are formed by shifting one digit to the left of the preceding line, and after shifting to the released right digit 0 is written. In the event that the non-zero leading element of the shifted string exceeds the bounds of the matrix, this $(n+1)-$bit binary vector is reduced to the remainder modulo f_n. Thus, the string returns to the boundaries of the matrix and the process of filling its lines continues according to the scheme already described. From the theory of polynomials of one variable, it is known that multiplication of an arbitrary polynomial $\omega_k(x)$ of degree k by x an equivalent shift of the polynomial by one digit to the left and, correspondingly, an increase by one degree of the polynomial. In other words,

$$x \cdot \omega_k(x) \to \omega_{k+1}(x), \tag{4.34}$$

Using (4.34) and taking into account the way forming GGM, we write the chain of transformations:

$$\boldsymbol{G}_{f,\omega}^{(n)} \Rightarrow \begin{pmatrix} x^{n-1}\cdot\omega \\ x^{n-2}\cdot\omega \\ \cdots \\ x\cdot\omega \\ \omega \end{pmatrix} \bmod f_n = \omega \cdot \begin{pmatrix} x^{n-1} \\ x^{n-2} \\ \cdots \\ x \\ 1 \end{pmatrix} \bmod f_n. \tag{4.35}$$

The elements of the right column vector in relation (4.35) are monomials that, when presented in binary form, invert the column vector into the unit matrix $\boldsymbol{E}$, i.e.

$$\begin{pmatrix} x^{n-1} \\ x^{n-2} \\ \cdots \\ x \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix} = \boldsymbol{E}, \tag{4.36}$$

which allows us to formulate the following assertion.

Assertion 4.1. *A generalized binary Galois matrix* $\boldsymbol{G}_{f,\omega}^{(n)}$ *of order* n *over an irreducible polynomial* f_n *is isomorphic to its generator element* ω, *which is an element of the extended field* $GF(2^n)$ *of characteristic 2*

$$\boldsymbol{G}_{f,\omega}^{(n)} \leftrightarrow \omega. \tag{4.37}$$

Consequently, according to the expressions (4.35) and (4.36) between GGM $\boldsymbol{G}_{f,\omega}^{(n)}$ and its GE ω, there is a one-to-one correspondence (isomorphism), which is mapped by (4.37). In addition, it is easy to establish that the isomorphism (4.37) leads to such consequences.

Corollary 4.1.1. *Generalized Galois matrices* $\boldsymbol{G}_{f,\omega}^{(n)}$ *are non-degenerate for any parameters* f_n *and* ω, *since they are formed, as is easy to verify on the basis of relation (4.36), by linearly independent rows of matrices*.

Corollary 4.1.2. *In order to raise the matrix* $\boldsymbol{G}_{f,\omega}^{(n)}$ *to the power* k, *it is sufficient to calculate the GE* $\omega_k = \omega^k (\mathrm{mod}\, f_k)$ *and, using the method of diagonal filling, make up the matrix* $\boldsymbol{G}_{f,\omega}^{(n)}$.

Corollary 4.1.3. *The minimum non-zero value of the power of e, ensuring equality* $\left(\boldsymbol{G}_{f,\omega}^{(n)}\right)^e = \boldsymbol{E}$, *coincides with the order ord of the element* ω *that forms the matrix* $\boldsymbol{G}_{f,\omega}^{(n)}$.

Corollary 4.1.4. *The generalized Galois matrix* $\boldsymbol{G}_{f,\omega}^{(n)}$ *is primitive if the element* ω *forming it is primitive, that is. if* $\omega = \theta$.

Corollary 4.1.5. *The matrices* $\boldsymbol{G}_{f,\omega_1}^{(n)}$ *and* $\boldsymbol{G}_{f,\omega_2}^{(n)}$ *are commutative, since they are elements of the same multiplicative group of maximal order* GF^* *composed from degrees of the matrix* $\boldsymbol{G}_{f,\omega}^{(n)}$, *an arbitrary generating primitive element of which* θ *belongs to the field* $GF(2^n)$ *over IP* f_n.

Corollary 4.1.6. *Algebraic transformations (summation, subtraction, multiplication and division) over a Galois matrix or over a set of Galois matrices are isomorphic to the same transformations over the generator elements of these matrices.*

Corollary 4.1.7. *The set of GGMs can be extended by introducing similar Galois matrices* $\hat{\boldsymbol{G}}_{f,\omega}^{(n)}$, *defined by*

$$\hat{\boldsymbol{G}}_{f,\omega}^{(n)} = \boldsymbol{P}^{-1} \cdot \boldsymbol{G}_{f,\omega}^{(n)} \cdot \boldsymbol{P}, \tag{4.38}$$

where $\boldsymbol{P}-$ *the similarity transformation matrix*.

As $\boldsymbol{P}-$matrices for the transformation (4.38), permutational matrices of the $n-$order are preferable, since for them it is sufficient to simply calculate the inverse matrices, namely $\boldsymbol{P}^{-1} = \boldsymbol{P}^{-T}$.

Unlike GGM $\boldsymbol{G}_{f,\omega}^{(n)}$ matrices $\hat{\boldsymbol{G}}_{f,\omega}^{(n)}$ while remaining commutative, they lose the isomorphism property. This feature of similar Galois matrices just provides the possibility of constructing one-way functions widely used in cryptography and other applications.

4.7. Primitive Galois matrices

The term "primitive Galois matrix" is similar to the term "primitive element" of the prime $GF(p)$ or extended Galois field $GF(2^n)$ of the characteristic p. The primitive matrix, being formed by the generating element ω of the multiplicative group, delivers the latter a maximal order equal to $p^n - 1$, if only $\omega = \theta$. An example of the MPGMP of the Galois field over any fourth-degree IP is shown in Fig. 4.15.

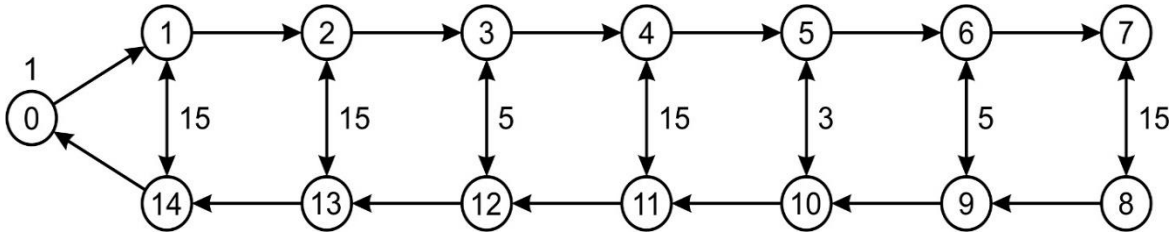

Figure 4.15. The multiplicative group the maximum order of the field $GF(2^4)$

Inside the circles in Fig. 4.15 degrees of the primitive generator (GE) are entered and on the right of the bidirectional arrows are the orders of the elements of the group determined by the cycle period of the closed circuit of the group contour. The traversal begins with the element 0 corresponding to the identity matrix, the next element k is selected, the order of which is computed, and the crawl is completed after returning to the element 0.

In Table. 4.8 shows the multiplicative groups of maximal order of the field $GF(2^4)$ over PP $f_4 = 10011$ generated by the base and conjugate Galois and Fibonacci matrices, the forming element of which is a primitive element $\theta = 10$.

Table 4.8. Elements of the MPGMO over a primitive polynomial $f_4 = 10011$

s	*ord*	***G***	***F***	$^*\boldsymbol{G}$	$^*\boldsymbol{F}$
1	15	$\begin{pmatrix}0&0&1&1\\1&0&0&0\\0&1&0&0\\0&0&1&0\end{pmatrix}$	$\begin{pmatrix}0&0&0&1\\1&0&0&1\\0&1&0&0\\0&0&1&0\end{pmatrix}$	$\begin{pmatrix}0&1&0&0\\0&0&1&0\\1&0&0&1\\1&0&0&0\end{pmatrix}$	$\begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&1&0&0\end{pmatrix}$
2	15	$\begin{pmatrix}0&1&1&0\\0&0&1&1\\1&0&0&0\\0&1&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&1&0\\0&0&1&1\\1&0&0&1\\0&1&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&1&0\\1&0&0&1\\1&1&0&0\\0&1&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&1&0\\0&0&0&1\\1&1&0&0\\0&1&1&0\end{pmatrix}$
3	5	$\begin{pmatrix}1&1&0&0\\0&1&1&0\\0&0&1&1\\1&0&0&0\end{pmatrix}$	$\begin{pmatrix}0&1&0&0\\0&1&1&0\\0&0&1&1\\1&0&0&1\end{pmatrix}$	$\begin{pmatrix}1&0&0&1\\1&1&0&0\\0&1&1&0\\0&0&1&0\end{pmatrix}$	$\begin{pmatrix}0&0&0&1\\1&1&0&0\\0&1&1&0\\0&0&1&1\end{pmatrix}$
4	15	$\begin{pmatrix}1&0&1&1\\1&1&0&0\\0&1&1&0\\0&0&1&1\end{pmatrix}$	$\begin{pmatrix}1&0&0&1\\1&1&0&1\\0&1&1&0\\0&0&1&1\end{pmatrix}$	$\begin{pmatrix}1&1&0&0\\0&1&1&0\\1&0&1&1\\1&0&0&1\end{pmatrix}$	$\begin{pmatrix}1&1&0&0\\0&1&1&0\\0&0&1&1\\1&1&0&1\end{pmatrix}$
5	3	$\begin{pmatrix}0&1&0&1\\1&0&1&1\\1&1&0&0\\0&1&1&0\end{pmatrix}$	$\begin{pmatrix}0&0&1&1\\1&0&1&0\\1&1&0&1\\0&1&1&0\end{pmatrix}$	$\begin{pmatrix}0&1&1&0\\1&0&1&1\\0&1&0&1\\1&1&0&0\end{pmatrix}$	$\begin{pmatrix}0&1&1&0\\0&0&1&1\\1&1&0&1\\1&0&1&0\end{pmatrix}$
6	5	$\begin{pmatrix}1&0&1&0\\0&1&0&1\\1&0&1&1\\1&1&0&0\end{pmatrix}$	$\begin{pmatrix}0&1&1&0\\0&1&0&1\\1&0&1&0\\1&1&0&1\end{pmatrix}$	$\begin{pmatrix}1&0&1&1\\0&1&0&1\\1&0&1&0\\0&1&1&0\end{pmatrix}$	$\begin{pmatrix}0&0&1&1\\1&1&0&1\\1&0&1&0\\0&1&0&1\end{pmatrix}$
7	15	$\begin{pmatrix}0&1&1&1\\1&0&1&0\\0&1&0&1\\1&0&1&1\end{pmatrix}$	$\begin{pmatrix}1&1&0&1\\1&0&1&1\\0&1&0&1\\1&0&1&0\end{pmatrix}$	$\begin{pmatrix}0&1&0&1\\1&0&1&0\\1&1&0&1\\1&0&1&1\end{pmatrix}$	$\begin{pmatrix}1&1&0&1\\1&0&1&0\\0&1&0&1\\1&1&1&0\end{pmatrix}$

Continuation of the table 4.8

8	15	$\begin{pmatrix}1&1&1&0\\0&1&1&1\\1&0&1&0\\0&1&0&1\end{pmatrix}$	$\begin{pmatrix}1&0&1&0\\0&1&1&1\\1&0&1&1\\0&1&0&1\end{pmatrix}$	$\begin{pmatrix}1&0&1&0\\1&1&0&1\\1&1&1&0\\0&1&0&1\end{pmatrix}$	$\begin{pmatrix}1&0&1&0\\0&1&0&1\\1&1&1&0\\0&1&1&1\end{pmatrix}$
9	5	$\begin{pmatrix}1&1&1&0\\0&1&1&1\\1&0&1&0\\0&1&0&1\end{pmatrix}$	$\begin{pmatrix}0&1&0&1\\1&1&1&1\\0&1&1&1\\1&0&1&1\end{pmatrix}$	$\begin{pmatrix}1&1&0&1\\1&1&1&0\\1&1&1&1\\1&0&1&0\end{pmatrix}$	$\begin{pmatrix}0&1&0&1\\1&1&1&0\\0&1&1&1\\1&1&1&1\end{pmatrix}$
10	3	$\begin{pmatrix}1&1&0&1\\1&1&1&1\\1&1&1&0\\0&1&1&1\end{pmatrix}$	$\begin{pmatrix}1&0&1&1\\1&1&1&0\\1&1&1&1\\0&1&1&1\end{pmatrix}$	$\begin{pmatrix}1&1&1&0\\1&1&1&1\\0&1&1&1\\1&1&0&1\end{pmatrix}$	$\begin{pmatrix}1&1&1&0\\0&1&1&1\\1&1&1&1\\1&0&1&1\end{pmatrix}$
11	15	$\begin{pmatrix}1&0&0&1\\1&1&0&1\\1&1&1&1\\1&1&1&0\end{pmatrix}$	$\begin{pmatrix}0&1&1&1\\1&1&0&0\\1&1&1&0\\1&1&1&1\end{pmatrix}$	$\begin{pmatrix}1&1&1&1\\0&1&1&1\\0&0&1&1\\1&1&1&0\end{pmatrix}$	$\begin{pmatrix}0&1&1&1\\1&1&1&1\\1&0&1&1\\1&0&0&1\end{pmatrix}$
12	5	$\begin{pmatrix}0&0&0&1\\1&0&0&1\\1&1&0&1\\1&1&1&1\end{pmatrix}$	$\begin{pmatrix}1&1&1&1\\1&0&0&0\\1&1&0&0\\1&1&1&0\end{pmatrix}$	$\begin{pmatrix}0&1&1&1\\0&0&1&1\\0&0&0&1\\1&1&1&1\end{pmatrix}$	$\begin{pmatrix}1&1&1&1\\1&0&1&1\\1&0&0&1\\1&0&0&0\end{pmatrix}$
13	15	$\begin{pmatrix}0&0&1&0\\0&0&0&1\\1&0&0&1\\1&1&0&1\end{pmatrix}$	$\begin{pmatrix}1&1&1&0\\0&0&0&1\\1&0&0&0\\1&1&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&1&1\\0&0&0&1\\1&0&0&0\\0&1&1&1\end{pmatrix}$	$\begin{pmatrix}1&0&1&1\\1&0&0&1\\1&0&0&0\\0&1&0&0\end{pmatrix}$
14	15	$\begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&1\end{pmatrix}$	$\begin{pmatrix}1&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&1\end{pmatrix}$	$\begin{pmatrix}1&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&0\end{pmatrix}$
15	1	$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$	$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$	$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$	$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$

In the column s of Table. 4.8 the values of the degree of the generators of the matrices of multiplicative groups are indicated, i.e. matrices located in the top row of the table, and in the column *ord* - the exponent (indicator, order) of the element (matrix) of the group.

If the degree n of the binary polynomial f_n generating the Galois MPG, to which we also refer Fibonacci MPGs (both basic and conjugate) is a prime number, then the indices of all matrix groups reach a maximum value equal to $2^n - 1$, that is, all elements of the group are primitive.

Below, with an example of a composite degree $n = 6$ of an IP, we formulate a rather simple rule for determining the exponents $k - \text{x}$ of the powers of matrices of the MPG Galois, $G \in \{\boldsymbol{G}, {}^*\boldsymbol{G}, \boldsymbol{F}, {}^*\boldsymbol{F}\}$, as elements of finite fields $GF(2^6)$ over irreducible polynomials, which are not necessarily primitive. A graphical representation of the MPGMO over the IP f_6 is shown in Fig. 4.16.

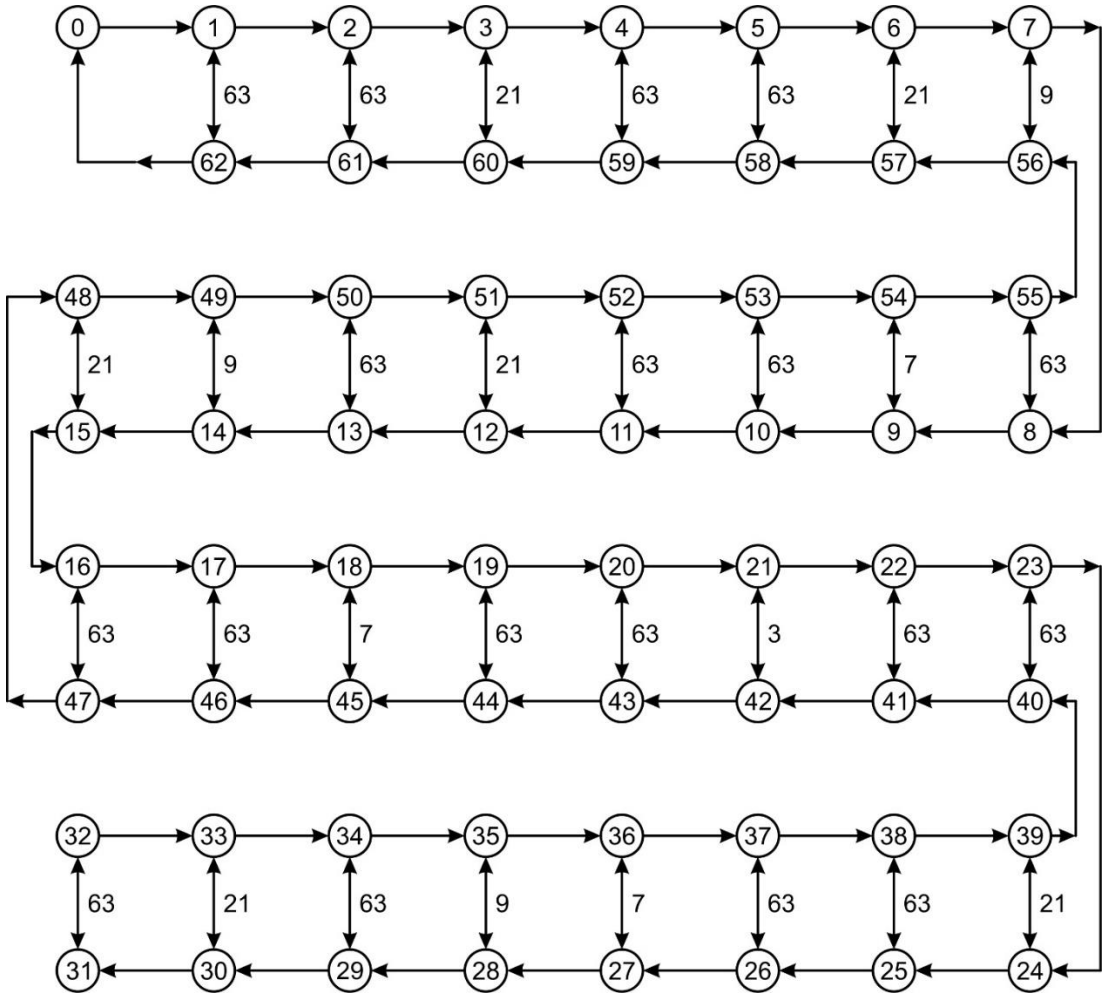

Figure 4.16. The multiplicative group the maximum order of the field

The one shown in Fig. 4.16 the graph defines the structure of the multiplicative group of maximal order generated by the primitive Galois matrix $\boldsymbol{G}_{f,\omega}^{(n)}$ over any irreducible polynomial f_n of sixth degree. In turn, according to Corollary 4.4.1 of Assertion 4.1 (§ 4.6), the Galois matrix $\boldsymbol{G}_{f,\omega}^{(n)}$ turns out to be primitive if the generator of the matrix $\boldsymbol{G}$ is a primitive field element θ of the field $GF(2^6)$ over the same IP f_n.

The order *ord* of any element α_k of the multiplicative group of $K-$ order over an arbitrary irreducible polynomial f_n of degree n is defined by the relation

$$ord\left(\alpha_k\right)=\left(K,k\right), \tag{4.39}$$

where k is the ordinal number of the element α_k located inside the circle in the contour of the graph of the MPG, and $\left(a,b\right)$ is the GCD of the numbers a and b.

The relation (4.39) is valid not only for the MPGMO, but also for cyclic subgroups of any order.

Let us turn to the MPGMO and other cyclic subgroups generated by the fourth degree of IP (Table 4.9-4.11), representing the elements of groups by a sequence of natural numbers, with 1 representing a unit matrix, 2 representing the first degree of the matrix $\boldsymbol{G}$, 3 representing the second degree, and so on.

It is easy to see that matrices α_k whose exponent *ord* is three, and such are the Galois matrices formed by the generators $\omega=6$ и 7 in Table. 4.9, $\omega=A$ и B in Table. 4.10 and, finally, the elements $\omega=C$ и D in Table. 4.11, occupy according to the graphical representation of fifteenth-order MPGMO (Figure 4.12) the fifth or tenth circle of the graph.

Table 4.9. Summary characteristic of the graph of MPGMO over a primitive polynomial $f_4 = 10011$

Degree of the matrix G	Generating element of Galois matrix													
	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	2	2	2	2	2	2	2	2	2	2	2	2	2	2
2	3	3	3	3	3	3	3	3	3	3	3	3	3	3
3	4	4	4	4	1	1	4	4	4	4	4	4	4	4
4	5	5	5	5			5	5	5	5	5	5	5	5
5	6	6	6	6			1	6	1	6	1	6	6	1
6	7	7	7	7				7		7		7	7	
7	8	8	8	8				8		8		8	8	
8	9	9	9	9				9		9		9	9	
9	A	A	A	A				A		A		A	A	
A	B	B	B	B				B		B		B	B	
B	C	C	C	C				C		C		C	C	
C	D	D	D	D				D		D		D	D	
D	E	E	E	E				E		E		E	E	
E	F	F	F	F				F		F		F	F	
F	1	1	1	1				1		1		1	1	

Table 4.10. Summary characteristic of the graph of MPGMO over a primitive polynomial $f_4 = 11001$

Degree of the matrix G	Generating element of Galois matrix													
	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	2	2	2	2	2	2	2	2	2	2	2	2	2	2
2	3	3	3	3	3	3	3	3	3	3	3	3	3	3
3	4	4	4	4	4	4	4	4	1	1	4	4	4	4
4	5	5	5	5	5	5	5	5			5	5	5	5
5	6	1	6	1	6	6	1	6			6	6	6	1
6	7		7		7	7		7			7	7	7	
7	8		8		8	8		8			8	8	8	
8	9		9		9	9		9			9	9	9	
9	A		A		A	A		A			A	A	A	
A	B		B		B	B		B			B	B	B	
B	C		C		C	C		C			C	C	C	
C	D		D		D	D		D			D	D	D	
D	E		E		E	E		E			E	E	E	
E	F		F		F	F		F			F	F	F	
F	1		1		1	1		1			1	1	1	

Table 4.11. Summary characteristic of the graph of MPGMO over a primitive polynomial $f_4 = 11111$

Degree of the matrix GG	Generating element of Galois matrix													
	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	2	2	2	2	2	2	2	2	2	2	2	2	2	2
2	3	3	3	3	3	3	3	3	3	3	3	3	3	3
3	4	4	4	4	4	4	4	4	4	4	1	1	4	4
4	5	5	5	5	5	5	5	5	5	5			5	5
5	1	6	1	6	6	6	1	6	6	6			6	1
6		7		7	7	7		7	7	7			7	
7		8		8	8	8		8	8	8			8	
8		9		9	9	9		9	9	9			9	
9		A		A	A	A		A	A	A			A	
A		B		B	B	B		B	B	B			B	
B		C		C	C	C		C	C	C			C	
C		D		D	D	D		D	D	D			D	
D		E		E	E	E		E	E	E			E	
E		F		F	F	F		F	F	F			F	
F		1		1	1	1		1	1	1			1	

4.8. Galois matrices over the field *GF* (*p*)

The Galois matrices over $GF(p)$, $p > 2$, have the same properties and are synthesized according to the same rules (diagonal filling) as the matrices over $GF(2)$. Let us choose, for example, $n = 4$, $p = 3$, and irreducible over $GF(3)$ unitary polynomial of degree four $f_4 = 12101$. Primitive elements θ margins $GF(3^4)$ over the IP f_4 are summarized in Table. 4.12.

Table 4.12. Primitive elements of the field $GF(3^4)$ over the IP $f_4 = 12101$

j	i							
	1	2	3	4	5	6	7	8
0	101	102	120	122	201	202	210	211
8	1010	1012	1021	1022	1102	1111	1112	1122
16	1200	1211	1220	1222	2011	2012	2020	2021
24	2100	2110	2111	2122	2201	2211	2221	2222

The number $(i, j)-$th primitive element of Table. 4.12 is determined by the sum of numbers the column i and the row j.

Let the primitive generating element $\theta = 1102$ is hilited in tab. 4.12 by shading. Basic $\boldsymbol{G}, \boldsymbol{F}$ and conjugate ${}^{*}\boldsymbol{G}, {}^{*}\boldsymbol{F}$ generalized Galois and Fibonacci matrices corresponding to the chosen parameters n, ω and f_4, have the form:

$$\boldsymbol{G} = \begin{pmatrix} 1 & 1 & 1 & 2 \\ 1 & 0 & 2 & 1 \\ 2 & 2 & 2 & 2 \\ 1 & 1 & 0 & 2 \end{pmatrix}; \qquad \boldsymbol{F} = \begin{pmatrix} 2 & 2 & 1 & 2 \\ 0 & 2 & 2 & 1 \\ 1 & 2 & 0 & 1 \\ 1 & 2 & 1 & 1 \end{pmatrix}. \tag{4.40}$$

$${}^{*}\boldsymbol{G} = \begin{pmatrix} 2 & 0 & 1 & 1 \\ 2 & 2 & 2 & 2 \\ 1 & 2 & 0 & 1 \\ 2 & 1 & 1 & 1 \end{pmatrix}; \qquad {}^{*}\boldsymbol{F} = \begin{pmatrix} 1 & 1 & 2 & 1 \\ 1 & 0 & 2 & 1 \\ 1 & 2 & 2 & 0 \\ 2 & 1 & 2 & 2 \end{pmatrix}. \tag{4.41}$$

Structural diagrams of generalized PC- generators PRS are invariant to the field characteristic p. In particular, the structural scheme of a four-digit Galois linear SR, feedbacks in which are given by a matrix $\boldsymbol{G}$ of the system (4.40) is shown in Fig. 4.17, and $\oplus$ is the operator modulo addition $p = 3$, and $\otimes$ – multiplication operator.

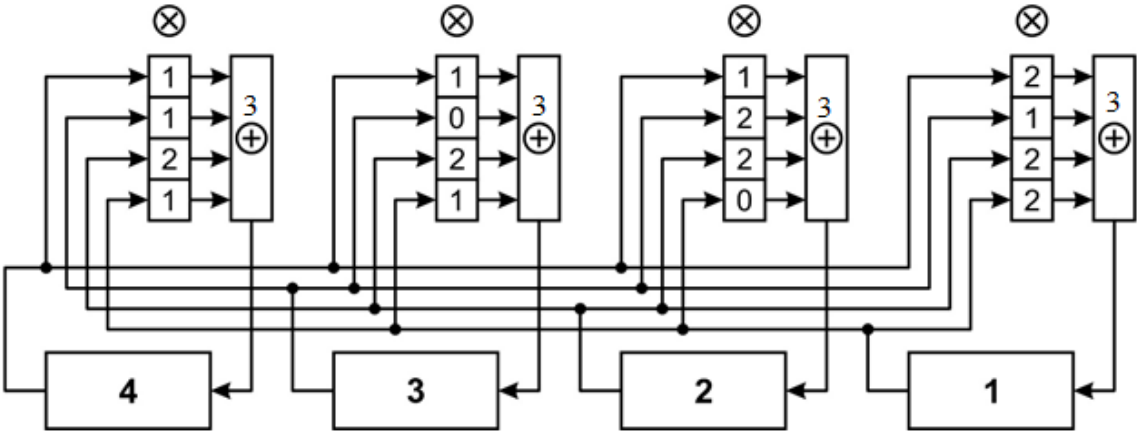

Figure 4.17. The block diagram of the generalized PR-generator Galois over $GF(3)$

Using the value of the matrix $\boldsymbol{G}$ in the system (4.40), we calculate by the formula (4.1) the set of register states at the instants of time $t = j \,||\, i$ (Table 4.13).

Table 4.13. The complete group of nonzero states of a generalized Galois PR-generator over $GF(3)$

j	i									
	0	1	2	3	4	5	6	7	8	9
0	0001	1102	1001	2211	1221	2001	0020	1111	2121	2122
1	0221	1222	0100	1021	0022	0012	1120	0211	2000	2221
2	0110	0210	1201	1220	1202	2022	2200	1200	0121	0201
3	0111	1012	2202	0101	2120	1020	2220	2011	2212	2020
4	0002	2201	2002	1122	2112	1002	0010	2222	1212	1211
5	0112	2111	0200	2012	0011	0021	2210	0122	1000	1112
6	0220	0120	2102	2110	2101	1011	1100	2100	0212	0102
7	0222	2021	1101	0202	1210	2010	1110	1022	1121	1010

By direct verification it is easy to verify that the sequence of states of the register shown in Fig. 4.17, coincides with the sequence of states summarized in Table. 4.13.

For the transition to the circuit of PR-generator in the Fibonacci configuration, it is enough in the registers of Fig. 4.17, marked by the operator $\otimes$, change elements corresponding to the columns of the Galois matrix $\boldsymbol{G}$ (4.40), by the corresponding elements of the columns of the Fibonacci matrix $\boldsymbol{F}$.

The block diagram of a four-digit conjugate Fibonacci PR-generator whose feedbacks are given by the matrix ${}^{*}\boldsymbol{F}$ of the system (4.41) is shown in Fig. 4.18.

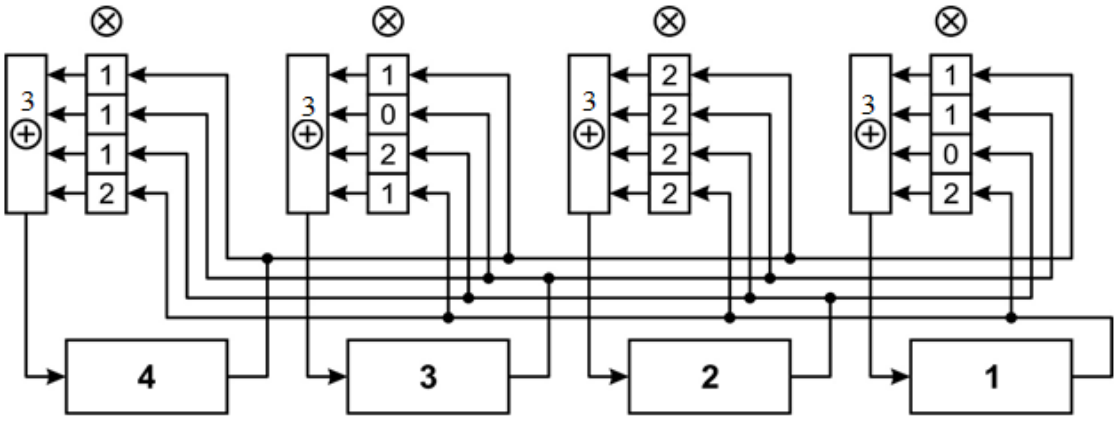

Figure 4.18. Structural diagram of the conjugate Fibonacci PC-generator over $GF(3)$

The sequence of nonzero states of the register, formed by the conjugate Fibonacci generator (see Figure 4.18), is summarized in Table. 4.14.

Table 4.14. The complete group of nonzero states of Fibonacci PR-generalized over $GF(3)$

j	i									
	0	1	2	3	4	5	6	7	8	9
0	0001	2122	0221	0211	2021	0111	1000	1121	0011	0012
1	2101	2022	2200	1221	1002	2002	0120	0101	0110	2211
2	1200	0100	1021	2020	1022	1112	1210	1020	0201	1101
3	1201	2222	1212	2201	0010	1220	2210	2111	0212	1110
4	0002	1211	0112	0122	1012	0222	2000	2212	0022	0021
5	1202	1011	1100	2112	2001	1001	0210	0202	0220	1122
6	2100	0200	2012	1010	2011	2221	2120	2010	0102	2202
7	2102	1111	2121	1102	0020	2110	1120	1222	0121	2220

4.9. Characteristic polynomials of Galois matrices

Definition 4.3. *The characteristic polynomial* $\chi(\lambda)$ *of the nondegenerate square matrix* $\boldsymbol{A}$ *of order* $n-$*is called the polynomial of* $n-$ *degree of the argument* λ

$$\chi(\lambda) = \det(\boldsymbol{A} - \lambda \boldsymbol{E}),$$

where $\boldsymbol{E}$ *– is the unit matrix of the same order as the matrix* $\boldsymbol{A}$.

The matrix $\boldsymbol{A} - \lambda \boldsymbol{E}$ is called the *characteristic matrix* for $\boldsymbol{A}$, and its determinant is the *characteristic polynomial* of the matrix $\boldsymbol{A}$. So if

$$\boldsymbol{A} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix},$$

then

$$\chi(\lambda)=\begin{vmatrix} a_{1,1}-\lambda & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2}-\lambda & \cdots & a_{2,n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n}-\lambda \end{vmatrix},$$

where $|\boldsymbol{A}|-$ is the determinant of $\boldsymbol{A}$.

A remarkable property of the characteristic polynomials of matrices is that if some matrices $\boldsymbol{A}$ and $\boldsymbol{B}$ are similar, then their characteristic polynomials coincide. The converse is also true: if the characteristic polynomials of the matrices coincide, then they are similar.

Let us turn to a numerical analysis of the characteristic polynomials of the Galois matrices, the Fibonacci matrices, and the conjugate matrices. The following is true

Assertion 4.2. *The characteristic polynomials of primitive Galois and Fibonacci matrices (both basic and conjugate) over* $GF(p)$, $p\geq 2$, *with generators* $\theta=10$ *coinside with irreducible polynomials that generate the matrices*.

The essence of the statement is that

$$\chi(x)=\det(\boldsymbol{A}_{f_n}-x\boldsymbol{E})=f_n(x), \qquad (4.42)$$

where $\boldsymbol{A}_{f_n}$ are matrices $\boldsymbol{G}, \boldsymbol{F}, {}^{*}\boldsymbol{G}$ or ${}^{*}\boldsymbol{F}$, generated by PrP $f_n(x)$ and GE $\omega=10$.

The proof of the statement can be carried out by a method of direct verification. Indeed, let us choose, for example ПрП a third-degree PrP $f_n(x)=1011$, $p=2$, for which

$$\chi_G(x)=\begin{vmatrix} -x & 1 & 1 \\ 1 & -x & 0 \\ 0 & 1 & -x \end{vmatrix}; \quad \chi_F(x)=\begin{vmatrix} -x & 0 & 1 \\ 1 & -x & 1 \\ 0 & 1 & -x \end{vmatrix};$$

$$\chi_{{}^{*}G}(x)=\begin{vmatrix} -x & 1 & 0 \\ 0 & -x & 1 \\ 1 & 1 & -x \end{vmatrix}; \quad \chi_{{}^{*}F}(x)=\begin{vmatrix} -x & 1 & 0 \\ 1 & -x & 1 \\ 1 & 0 & -x \end{vmatrix}.$$

It is easy to see that for all four matrices CP are the same, such that $\chi(x)=x^3+x+1$, coinside with PrP $f_3(x)$.

The equality (4.42) is also verified in the same way for matrices generated by irreducible polynomials that are not primitive, but under the condition that their generating elements are equal 10.

At the same time, for generalized matrices $\boldsymbol{G}$, $\boldsymbol{F}$, ${}^{*}\boldsymbol{G}$ and ${}^{*}\boldsymbol{F}$, that is, for which the GE $\omega > 10$, the statement is not always fulfilled. Let's consider an example.. Let $p = 2$, $f_3(x) = 1011$ and $\omega = 101$. We have

$$\boldsymbol{G} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}; \quad \chi_G(x) = \begin{vmatrix} -x & 1 & 0 \\ 0 & -x & 1 \\ 1 & 0 & 1-x \end{vmatrix} = x^3 + x^2 + 1,$$

that is $\chi_G(x)$ does not coincide with $f_3(x)$.

4.10. Spatial matrices and Galois fields

For finite fields generated by primitive Galois matrices, a number of standard axioms (conditions) should be respected. We verify the feasibility of axioms using the example of an extended field whose elements constitute the complete set of Galois matrices generated by an irreducible binary polynomial of the fourth degree $f_4 = 11111$, which is not, incidentally, primitive. The forming elements of the set of Galois matrices are 16 binary vectors 0, 1, 10, …, 1111. All these matrices are shown in Table. 4.15, where the elements ω, which are the generators of the corresponding Galois matrices, are distinguished by bold digits in the lower rows of these matrices.

Table 4.15. The complete set of binary Galois matrices of the fourth order over IP $f_4 = 11111$

$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{0} \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \mathbf{1} \end{pmatrix}$	$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \mathbf{1} & \mathbf{0} \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & \mathbf{1} & \mathbf{1} \end{pmatrix}$
$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & \mathbf{1} & \mathbf{0} & \mathbf{0} \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & \mathbf{1} & \mathbf{0} & \mathbf{1} \end{pmatrix}$	$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & \mathbf{1} & \mathbf{1} & \mathbf{0} \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & \mathbf{1} & \mathbf{1} & \mathbf{1} \end{pmatrix}$

Continuation of the table 4.15

$\begin{pmatrix}0&0&1&0\\0&0&0&1\\1&1&1&1\\\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}\end{pmatrix}$	$\begin{pmatrix}1&0&1&0\\0&1&0&1\\1&1&0&1\\\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{1}\end{pmatrix}$	$\begin{pmatrix}1&1&0&1\\1&0&0&1\\1&0&1&1\\\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{0}\end{pmatrix}$	$\begin{pmatrix}0&1&0&1\\1&1&0&1\\1&0&0&1\\\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{1}\end{pmatrix}$
$\begin{pmatrix}0&0&1&1\\1&1&1&0\\0&1&1&1\\\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{0}\end{pmatrix}$	$\begin{pmatrix}1&0&1&1\\1&0&1&0\\0&1&0&1\\\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{1}\end{pmatrix}$	$\begin{pmatrix}1&1&0&0\\0&1&1&0\\0&0&1&1\\\mathbf{1}&\mathbf{1}&\mathbf{1}&\mathbf{0}\end{pmatrix}$	$\begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\\mathbf{1}&\mathbf{1}&\mathbf{1}&\mathbf{1}\end{pmatrix}$

The set of primitive elements of the field $GF(2^4)$ over IP $f_4 = 11111$ is summarized in Table 4.16.

Table 4.16. Primitive elements of the field $GF(2^4)$ over IP $f_4 = 11111$

11	101	110	111	1001	1010	1011	1110

For example, let's choose a primitive element $\theta = 111$, separated in Table. 4.16 shading, and from Table 4.15 - corresponding to this element primitive Galois matrix, denoting it as $\boldsymbol{G}_\theta$. We have

$$\boldsymbol{G}_\theta = \begin{pmatrix}0&1&1&0\\0&0&1&1\\1&1&1&0\\0&\mathbf{1}&\mathbf{1}&\mathbf{1}\end{pmatrix}. \qquad (4.43)$$

By Corollary 1.4 of Assertion 4.1 stated above, the matrix $\boldsymbol{G}$, given by (4.43) is primitive, since the element $\theta = 111$ forming it is primitive over IP $f_4 = 11111$. Successively raising the matrix $\boldsymbol{G}$ to the power s, starting with $s = 0$, we arrive at a multiplicative group $GF^*(2_2^4)$ of order 15. The set of fourth-order binary matrices, supplemented by the zero matrix, is the set of elements of the field $GF(2_2^4)$, generated by the IP $f_4 = 11111$ and the primitive generator $\theta = 111$.

We make sure that the standard axioms in the field $GF(p_2^n)$ are realizable by choosing a binary field $GF(2_2^4)$ as a basis. We introduce the notation $\boldsymbol{GF}.k$ for the $k-$axiom.

$\boldsymbol{GF}.1$. From two operations of the Galois field over the elements a and b, one operation is called an addition and is denoted as $a+b$, and the other by multiplication and is denoted as $a\cdot b$ or ab. Let

$$\boldsymbol{A}=\begin{pmatrix}1&1&1&0\\0&1&1&1\\1&1&0&0\\0&\mathbf{1}&\mathbf{1}&\mathbf{0}\end{pmatrix},\ \boldsymbol{B}=\begin{pmatrix}1&1&0&0\\0&1&1&0\\0&0&1&1\\\mathbf{1}&\mathbf{1}&\mathbf{1}&\mathbf{0}\end{pmatrix}\text{ and }\boldsymbol{C}=\begin{pmatrix}1&0&1&1\\1&0&1&0\\0&1&0&1\\\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{1}\end{pmatrix},\quad(4.43)$$

be selected elements of the field $GF(2_2^4)$, over which the calculations are carried out in the residue ring by $\bmod 2$. We have

$$\boldsymbol{A}\cdot\boldsymbol{B}=\begin{pmatrix}0&0&1&0\\0&0&0&1\\1&1&1&1\\\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}\end{pmatrix},\ \boldsymbol{A}+\boldsymbol{B}=\begin{pmatrix}1&0&0&1\\1&0&1&1\\1&0&1&0\\0&\mathbf{1}&\mathbf{0}&\mathbf{1}\end{pmatrix}.\quad(4.44)$$

The transformations (4.44), firstly, satisfy the condition $\boldsymbol{GF}.1$ and, secondly, confirm the observance of the following axiom of Galois fields.

$\boldsymbol{GF}.2$. The result of addition or multiplication of two field elements is the third element from the same finite set.

In fact, according to relations (4.44) and tab. 4.14, both the sum $\boldsymbol{A}+\boldsymbol{B}$, and the product $\boldsymbol{A}\cdot\boldsymbol{B}$ of elements of the field $GF(2_2^4)$ belong to the same field, that is, the set of elements of the field $GF(2_2^4)$ are closed relative to the operations of addition and multiplication.

$\boldsymbol{GF}.3$. The field always contains a multiplicative unit $\mathbf{1}$, which is the unit matrix of the $n-$order, and the additive unit which is a zero $n-$dimensional matrix $\mathbf{0}$ such that $a\cdot\mathbf{1}=a$, and $a+\mathbf{0}=a$, for all elements of the field.

GF.4. For any element a there exists an inverse element in addition $(-a)$ and an inverse element in multiplication a^{-1} (if $a \neq 0$) such that $a+(-a)=0$ and $a \cdot a^{-1}=1$.

For example, the elements (4.43) are answered by inverse elements

$$\boldsymbol{A}^{-1}=\begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & \mathbf{1} & \mathbf{0} & \mathbf{1} \end{pmatrix},\ \boldsymbol{B}^{-1}=\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} \end{pmatrix},$$

$$\boldsymbol{C}^{-1}=\begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} \end{pmatrix}, \tag{4.45}$$

possessing the property that, first, belong, like the elements (4.43), to the field $GF(2_2^4)$ and, secondly, they are Galois matrices, the generators of which are arranged in bold type in the lower rows of the matrices. It is easy to verify that the products of the matrices (4.43) by the corresponding inverse matrices (4.45) are equal to the identity matrices, as it should be.

GF.5. For operations of addition and multiplication in the field $GF(2_2^n)$ the usual associativity rules

$$a+(b+c)=(a+b)+c,\ a(bc)=(ab)c,$$

commutativity rules

$$a+b=b+a,\ ab=ba$$

and distributivity rules

$$a(b+c)=ab+ac,$$

are satisfied, which can be verified uniquely by the example of matrices (4.43).

The above axioms are observed not only for the binary field $GF(2_2^n)$, but also for any field $GF(p_2^n)$ of the characteristic p. Thus, it can be considered proved that the complete set of elements $\boldsymbol{G}_\omega$, belonging to $GF(p_2^n)$, satisfies all the classical

axioms of fields and so, the proof of the fact that the set $\{\boldsymbol{G}_{\omega}\}$ forms an extended Galois matrix field $GF(p_2^n)$ is completed.

Primitive elements θ of the field $GF(p_2^n)$ over irreducible polynomials f_n are generators of not only primitive Galois matrices $\boldsymbol{G}_{\theta}$, but also the right-sided transpose of primitive Fibonacci matrices $\boldsymbol{F}_{\theta}$, associated with them, and also primitive conjugate Galois ${}^{*}\boldsymbol{G}_{\theta}$ and Fibonacci matrices ${}^{*}\boldsymbol{F}_{\theta}$.

It follows that the multiplicative groups $GF^{*}(p_2^n)$ of Galois matrix fields $GF(p_2^n)$ can be constructed not only on the basis of matrices $\boldsymbol{G}_{\theta}$, but also with the help of matrices $\boldsymbol{F}_{\theta}$, ${}^{*}\boldsymbol{G}_{\theta}$ and ${}^{*}\boldsymbol{F}_{\theta}$.

As elements of extended finite fields, not only two-dimensional Galois matrices can be used, but also the so-called *spatial Galois matrices*, that is, matrices of three and more dimensions, generalizing the concept of an ordinary square matrix of $n-$th order over the field $GF(p)$.

Any system of elements n^3 of the field $GF(p)$, located at the points of a three-dimensional space defined by coordinates i, j, k, is called a three-dimensional (cubic) matrix of $n-$th order over the field $GF(p)$. We introduce the notation $\boldsymbol{G}_{i\,jk}$ for these matrices. An example of a three-dimensional matrix of the fourth order is shown in Fig. 4.19.

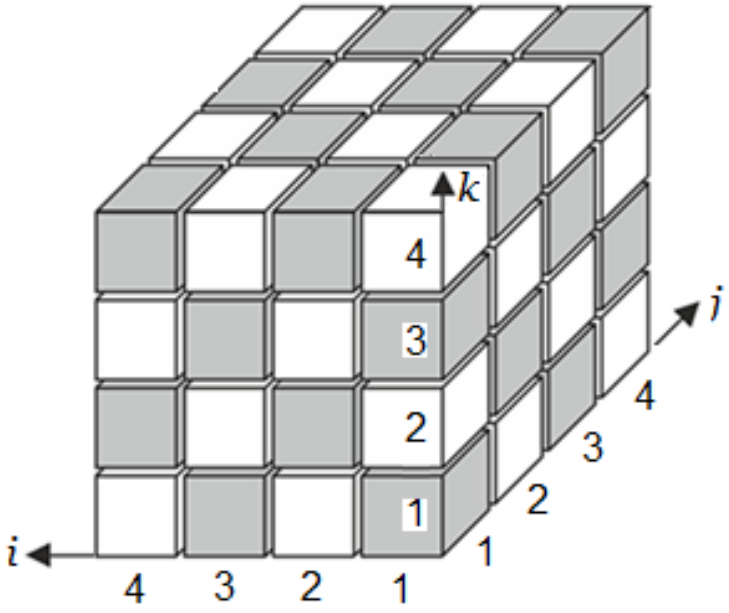

Figure 4.19. Cubic matrix of the fourth order

The set of elements of the matrix $\boldsymbol{G}_{i\,jk}$ with a fixed index value k is called the *cross-section of the orientation* (k). All n cross-sections of the orientation (k) in the matrix $\boldsymbol{G}_{i\,jk}$ are parallel to each other and are ordinary two-dimensional matrices of $n-$th order.

One of the possible methods for constructing a three-dimensional Galois space matrix over $GF(p)$, that generated by an IP f_n and isomorphic to the GE ω, is as follows. Let, for example, $n=4$. Put at the base of a fourth-order cube a primitive matrix (4.43), which is the $ij1$ section of the spatial matrix shown in Fig. 4.19. All subsequent sections of the cube in the direction from the bottom up along the axis k are formed from the previous sections by multiplying by x. This means, in particular, that the rows of a two-dimensional matrix $\boldsymbol{G}_{i\,j2}$ are the result of a shift to the left by the corresponding rows of the matrix $\boldsymbol{G}_{i\,j1}$, reduced to modulus $f_4=11111$.

$$\boldsymbol{G}_{i\,j1}=\begin{pmatrix}0&1&1&0\\0&0&1&1\\1&1&1&0\\0&\mathbf{1}&\mathbf{1}&\mathbf{1}\end{pmatrix};\ \boldsymbol{G}_{i\,j2}=\begin{pmatrix}1&1&0&0\\0&1&1&0\\0&0&1&1\\\mathbf{1}&\mathbf{1}&\mathbf{1}&\mathbf{0}\end{pmatrix}; \tag{4.46}$$

$$\boldsymbol{G}_{i\,j3}=\begin{pmatrix}0&1&1&1\\1&1&0&0\\0&1&1&0\\0&0&\mathbf{1}&\mathbf{1}\end{pmatrix};\ \boldsymbol{G}_{i\,j4}=\begin{pmatrix}1&1&1&0\\0&1&1&1\\1&1&0&0\\0&\mathbf{1}&\mathbf{1}&\mathbf{0}\end{pmatrix}. \tag{4.47}$$

It is easy to verify that all sections of the cube of the orientation (j) coincide with the corresponding sections of the orientation (k), represented by systems of matrix (4.46) and (4.47). In other words, cube sections, collinear of the plane ij, are equivalent to sections that are collinear to the plane ik.

As well as for two-dimensional Galois matrices, the statement is true.

Statement 4.3. *Spatial Galois matrices* $\boldsymbol{G}_r^{[n]}$ *are isomorphic to their generating elements, which are elements of the field* $GF(p^n)$ *over an irreducible polynomial* f_n.

Corollary 4.3.1. *The sequence of powers of the spatial* $r-$*dimensional Galois matrix* $\boldsymbol{G}_r^{[n]}$*, of the* $n-$*order, which generating element is a primitive element* θ *of the field* $GF(p^n)$*, generated by an irreducible over* $GF(p)$ *polynomial* f_n*, forms the multiplicative group* $GF^*(p_r^n)$ *of maximal order* $L=p^n-1$ *of matrix extended fields* $GF(p_r^n)$.

Corollary 4.3.2. *Any pairs of spatial Galois matrices belonging to the group* $GF(p_r^n)$*, are commutative.*

Corollary 4.3.2 emphasizes the peculiarity of matrices $\boldsymbol{G}_r^{[n]}$, which consists in the fact that *an arbitrary pair of* $r-$*dimensional spatial Galois matrices is always commutative, whereas in the general case even ordinary two-dimensional matrices do not possess the commutative property*.

The most important result of this part of the section is the confirmation of the possibility of constructing matrix fields based on spatial Galois matrices that are isomorphic to the elements of the field $GF(p^n)$. The distinctive feature of matrix fields is as follows. If elements ω of classical fields $GF(p^n)$ are invariant to irreducible polynomials f_n, forming fields, then elements $\boldsymbol{G}_{i\,j\ldots r}$ of matrix fields $GF(p_r^n)$ depend on IP f_n. Consequently, it can be argued that the spectrum of the proposed matrix Galois fields $GF(p_r^n)$ is much richer than the spectrum of classical fields $GF(p^n)$, which are a special case of the extended matrix fields if we put the parameter in them $r=1$.

This is the first. And, secondly, one should not exclude the fact that, in addition to $r-$dimensional spatial matrix $\boldsymbol{G}_\omega$ of the $n-$order, isomorphic to elements of the field $GF(p^n)$, other $r-$dimensional objects other than matrices $\boldsymbol{G}_{i\,j\ldots r}$ will be offered, but which will be acceptable for the construction of fields $GF(p_r^n)$.

However, many important questions, for example, are: what is the structure of a single cube, or what will the elements $\boldsymbol{G}_{i\,j\ldots r}$ of the field $GF(p_r^n)$, $r\geq 4$ look like and a number of others, are not disclosed and can be the subject of a separate study.

It is interesting to note some features that accompany the expansion of the dimension of the space of algebraic objects. So, if the product of two one-dimensional vectors $\boldsymbol{X}$ and $\boldsymbol{Y}$ of the same order is commutative, then for two-dimensional square matrices $\boldsymbol{A}$ and $\boldsymbol{B}$ their product is not necessarily commutative.

But if some matrix is $\boldsymbol{C}$ nondegenerate, then at least the equality $\boldsymbol{C}\cdot\boldsymbol{C}^{-1}=\boldsymbol{C}^{-1}\cdot\boldsymbol{C}$ is always satisfied. At the same time, for two spatial (in particular, cubic) matrices $\boldsymbol{U}$ and $\boldsymbol{V}$ of the $n-$th order in the general case, not only $\boldsymbol{U}\cdot\boldsymbol{V}\neq\boldsymbol{V}\cdot\boldsymbol{U}$, but also $\boldsymbol{U}\cdot\boldsymbol{U}^{-1}\neq\boldsymbol{U}^{-1}\cdot\boldsymbol{U}$, as well as $\boldsymbol{V}\cdot\boldsymbol{V}^{-1}\neq\boldsymbol{V}^{-1}\cdot\boldsymbol{V}$. Such a feature of cubic matrices is explained by the fact that for them the *left inverse matrix*, as a rule, does not coincide with the *right inverse matrix*.

4.11. Properties of the Galois PR-generators

Let us turn to the structural-logical scheme of the generalized four-digit PR-generator of pseudo-random numbers in the basic Galois configuration (Fig. 4.20), the feedback in the register of which is determined by the primitive polynomial $f_4=10011$, and on the basis of this scheme, we will try to establish the basic properties of similar generators of the PRN.

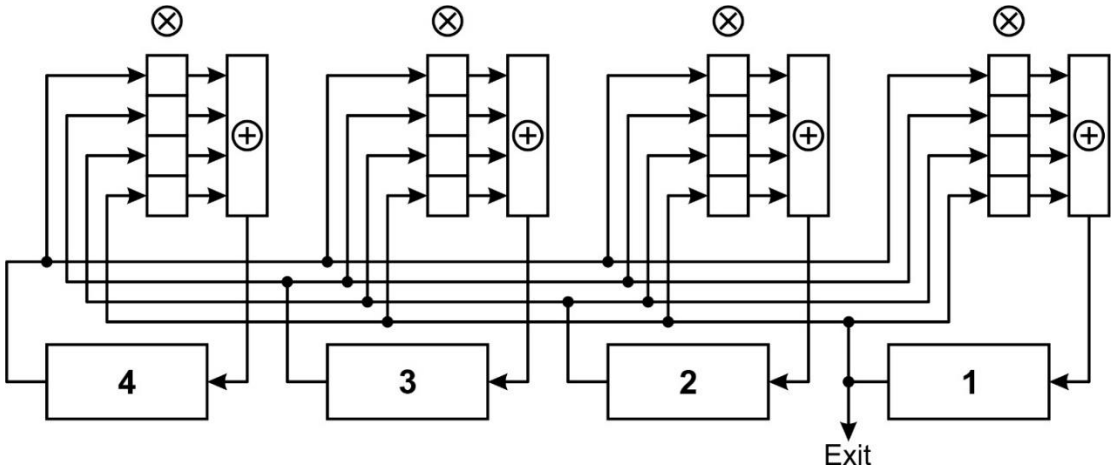

Figure 4.20. Structural diagram of the base PR-generator of Galois PRN

In Table. 4.17 brought together binary numbers taken from the low (right) digit of the generator. Feedbacks in the register of the generator are formed by primitive Galois matrices, generating elements of which are given in the second row of Table. 4.17.

We call *straight* a binary sequence of pseudo-random numbers if it can be obtained from the classical sequence (the first column of the GE of Table 4.17 for which $\omega=10$) as a result of shifting the latter by a certain number of positions. To

the *straight* ones in Table. 4.17 are the sequences to which the constituent elements ω are equal, 10, 11, 100 and 101. In particular, if the sequence of pseudo-random numbers (SPRN) $\sim\omega=11$ (symbol ~ should be read as "formed by a generating element") cyclically shift up $k=3$ position, we arrive to the SPRN $\sim\omega=10$. For $\omega=100$ and $\omega=101$ parameter k is 7 and 1, respectively. In columns of Table. 4.17, which correspond to the GE $\omega=11,100$ и 101 shaded elements, starting from which in the direction of the arrow (from top to bottom, i.e. in the forward direction), sequences of PRNs repeating the SPRN $\sim\omega=10$.

Table 4.17. PRN generated by the Galois generator over PP $f_4=10011$

Degree GE	Primitive generative elements							
	10	11	100	101	1001	1011	1101	1110
0	↑1↓	1	1	1	1	1	1	↑1
1	0	1	0	1↓	1	1	↑1	0
2	0	1	1	0	1	↑1	0	1
3	0	1↓	0	0	↑1	0	0	0
4	1	0	1	0	0	1	1	1
5	0	0	1	1	1	0	0	1
6	0	0	1	0	0	1	0	0
7	1	1	1↓	0	1	1	0	0
8	1	0	0	1	1	0	1	1
9	0	0	0	1	0	0	1	0
10	1	1	0	0	0	1	1	0
11	0	1	1	1	1	0	1	0
12	1	0	0	0	0	0	0	1
13	1	1	0	1	0	0	1	1
14	1	0	1	1	0	1	0	1

The sequences of binary numbers are invertible (or inverse) if the direction of the formation of numbers by the PRN generators is back to the direction of formation of these numbers by the PRN generator $\sim\omega=10$. The inverses include the sequences to which the GE ω, equal to 1001, 1011, 1101 and 1110, i. e. exactly half the set Ω of GЭ $\omega\in\Omega$ in Table. 4.17. In the columns of this table that correspond to the GE $\omega=1001,1011,1101$ и 1110, the elements are selected starting from which, in the direction of the arrow (bottom-up, i.e., in the inverse direction), the sequences of the PRN repeating the SPRN $\sim\omega=10$.

As the results of the analysis showed, similar properties are possessed the PRN generators synthesized on the basis of PP 11001 and NP 11111. These generators, as well as the generators generated by PP 10011, form four direct and as many inverse SPRN, the direction of the oscillator sequences over IP 11111 being determined with respect to the sequence the PRN, formed by a minimal GE $\omega_{\min} = 11$.

Similar properties are possessed by PPSCH, built on the basis of almost all PrPs of the fifth degree. Namely, out of 30 sequences formed by primitive field elements $GF(2^5)$ over the fifth degree of the PrP, exactly four of them, as well as in the set of sequences corresponding to the fourth-degree PrP, are either direct or inverse. From this rule, the sequences corresponding to the primitive elements of the field $GF(2^5)$ over the PrP $f_5 = 101001$ In this case, the set of 30 sequences is split into six groups, each of which contains five identical sequences, the sequences entering into groups starting with the second (the first group is the group generated by the OE $\omega = 10$), are neither direct nor inverse. This phenomenon can be called an artifact of the PSP generator, which manifests itself in the fact that there are various primitive elements that form the same (in the group) multiplicative $m-$ sequences for $\mod 101001$. The marked artifact is illustrated in Table. 4.18.

Table 4.18. Confirmation of the artifact, manifested in the PrP $f_5 = 101001$

№ GE	Number of the group					
	I	II	III	IV	V	VI
1	10	11	110	111	1000	1001
2	100	101	1010	1011	10010	10011
3	1100	1101	1110	1111	11000	11001
4	10000	10001	10100	10101	11100	11101
5	11010	11011	10110	10111	11110	11111

According to the data in this table, even GEs correspond to odd groups, while even groups have odd generators, and the values of the last GEs are exactly one more than the values of the preceding even elements.

And at the conclusion of this section, we note the features $GF(2^6)$. So for PrP $f_6 = 1000011$ of 36 sequences 11 are inverse and none that belong to direct sequences. The remaining RR form five straight lines and the same number of inverse sequences.

Summary of the section

1. The term of the Galois matrix, like the bijectively related with it the Fibonacci matrix, is borrowed from the theory of cryptography, in which generators of binary pseudo-random sequences in Galois and Fibonacci configurations are widely used. The generators are constructed on the based of linear feedback registers with linear feedbacks.

2. Shift register of the length n bit can be in one of the $2^n - 1$ nonzero internal states $S_k, k = \overline{0, 2^n - 2}$

3. Only the shift register with specially selected feedback functions can pass through all $2^n - 1$ internal states. These are so-called maximum period registers (generators).

4. The essence of the term "primitive" Galois matrix is similar, to a certain extent, the essence of the term "primitive element" of the Galois field.

5. The Galois matrix $\boldsymbol{G}$ of the $n-$th order over the field $GF(p)$ is primitive if the minimal non-zero exponent of degree e, reversing $\boldsymbol{G}^e$ in the identity matrix is determined by the relation $e = p^n - 1$.

6. In order for the shift register to be a pseudo-random sequence generator of the maximum period, the corresponding feedback polynomial must be a primitive polynomial.

7. Each linear SRLFB-generator of the pseudo-random sequence (PRS) of the maximum period can be represented by an equivalent to it the primitive Galois matrix $\boldsymbol{G}$, forming the same $m-$ sequence, as the PRS generator.

8. Feedbacks in classical Galois generators of the maximum period are uniquely determined by the chosen primitive polynomial (PP) and are formed in this way: the responses of each digit ($D-$trigger) the shift register of the generator is fed to the inputs of the subsequent digits, being for them excitation functions. In addition, the response of the upper register bit is fed (according to the XOR scheme) to the inputs of those and only those digits whose numbers coincide with the numbers of non-zero monomials of the PP.

9. The Galois and Fibonacci matrices are interconnected by right-sided transposition.

10. Element x^* of some group X is a conjugate to an element x of the same group if there is an element $z \in X$ such that ${}^*x = z^{-1} \cdot x \cdot z$.

11. Feedbacks in the registers of the basic Galois and Fibonacci generators are performed in the clockwise direction, whereas in the conjugate generator registers it is counterclockwise.

12. We will call generalized the Galois matrices of $n-$th order, the forming element ω of which is not necessarily a primitive element θ of the field $GF(2^n)$, generated by an arbitrary irreducible polynomial f_n degree n.

13. The essence of the generalized rule of diagonal filling (synthesis) of Galois matrices is as follows. Let $\omega-$ forming element (GE) of the matrix, which can be chosen as any element of the field $GF(2^n)$, generated by an irreducible polynomial (IP) f_n. GE ω is written to the right in the lower (first) row of the matrix being formed. The subsequent rows of matrices (in the direction of the bottom-up) will be obtained by shifting the previous row one digit to the left. If, at the same time, the highest nonzero bit of the string is outside the matrix, then the vectors corresponding to such rows are reduced to the remainder modulo the IP f_n and, thus, the row of the matrix also becomes $n-$ bit.

14. Generalized Galois matrices $\boldsymbol{G}_{f,\omega}^{(n)}$ are non-degenerate for any parameters f_n and ω, since they are formed by linearly independent rows of matrices.

15. In order to raise the matrix $\boldsymbol{G}_{f,\omega}^{(n)}$ to a degree k it is enough to calculate the GE $\omega_k = \omega^k (\mathrm{mod}\, f_k)$ and by the use of the method of diagonal filling to form a matrix $\boldsymbol{G}_{f,\omega}^{(n)}$.

16. The minimum non-zero degree value e ensuring equality $\left(\boldsymbol{G}_{f,\omega}^{(n)}\right)^e = \boldsymbol{E}$, coincides with the order *ord* of the element ω, forming a matrix $\boldsymbol{G}_{f,\omega}^{(n)}$.

17. Generalized Galois matrix $\boldsymbol{G}_{f,\omega}^{(n)}$ is primitive if the element ω forming it is primitive i.e. if $\omega = \theta$.

18. The matrices $\boldsymbol{G}_{f,\omega_1}^{(n)}$ and $\boldsymbol{G}_{f,\omega_2}^{(n)}$, $\omega_1 \neq \omega_2$, are commutative, since they are elements of the same multiplicative group of maximal order GF^*, which is composed from the degrees of the matrix $\boldsymbol{G}_{f,\omega}^{(n)}$, an arbitrary generating primitive element θ of which belongs to the field $GF(2^n)$ over the IP f_n.

19. Algebraic transformations (summation, subtraction, multiplication and division) over a Galois matrix or a set of Galois matrices are isomorphic to the same transformations over the generator elements of these matrices.

20. The set of generalized Galois matrices can be extended by introducing similar Galois matrices $\hat{\boldsymbol{G}}_{f,\omega}^{(n)}$, defined by the relation $\hat{\boldsymbol{G}}_{f,\omega}^{(n)} = \boldsymbol{P}^{-1} \cdot \boldsymbol{G}_{f,\omega}^{(n)} \cdot \boldsymbol{P}$, where $\boldsymbol{P}-$similarity transformation matrix.

21. Multiplication of an arbitrary polynomial $\omega_k(x)$ of degree k on x is equivalent to a shift of the polynomial by one digit to the left and, correspondingly, an increase by one degree of the polynomial.

22. The generalized Galois binary matrix of $n-$th order over an irreducible polynomial f_n is isomorphic to its generating element ω, which is an element of the extended field $GF(2^n)$ characteristics 2

23. The characteristic polynomial $\chi(\lambda)$ of a nondegenerate square matrix $\boldsymbol{A}$ of $n-$th order is a polynomial of $n-$ th power from the argument λ such that $\chi(\lambda) = \det(\boldsymbol{A} - \lambda \boldsymbol{E})$, where $\boldsymbol{E}$ is the unit matrix of the same order as the matrix $\boldsymbol{A}$.

24. A remarkable property of the characteristic polynomials of matrices is that if some matrices $\boldsymbol{A}$ and $\boldsymbol{B}$ are similar, then their characteristic polynomials coincide. The converse is also true: if the characteristic polynomials of the matrices coincide, then they are similar.

25. Characteristic polynomials of primitive Galois and Fibonacci matrices (both basic and conjugate) over $GF(p)$, $p \geq 2$, with generating elements $\theta = 10$ coincide with the irreducible polynomials that generate the given matrices.

26. Any system of n^3 elements of the field $GF(p)$, located at the points of three-dimensional space, determined by the coordinates i, j, k, is called a three-dimensional (cubic) matrix of $n-$th order over the field $GF(p)$.

27. Spatial Galois matrices $\boldsymbol{G}_r^{[n]}$ are isomorphic to the elements forming them, which are elements of the field $GF(p^n)$ over an irreducible polynomial f_n.

28. The sequence of degrees of spatial $r-$ dimensional Galois matrix of $n-$ th order $\boldsymbol{G}_r^{[n]}$, the forming element of which is a primitive element θ of the field $GF(p^n)$, generated by the irreducible over $GF(p)$ polynomial f_n, forms a

multiplicative group $GF^*(p_r^n)$ of the maximum order $L = p^n - 1$ of matrix extended fields $GF(p_r^n)$.

29. An arbitrary pair of $r-$ dimensional Galois spatial matrices is always commutative, whereas in the general case even ordinary two-dimensional matrices do not possess the commutativity property.

Questions for self-examination

1. Explain the basis of the origin of the terms "Galois matrix" and "Fibonacci matrix".

2. Give the formula for the number of non-zero states of the linear shift register of the $n-$th order.

3. What is the linear shift register of the maximum period and how are feedbacks formed in it?

4. Give a definition of a primitive Galois matrix over a field (p) .

5. What should be the feedback polynomial of the generator of the maximum-period pseudo-random sequence (PRS)?

6. Draw up the structural-logic diagrams of the linear shift registers (generators of PRS) Galois and Fibonacci of the maximum period over the given primitive polynomial.

7. Is there a relationship between the linear Galois generator of the PRS of maximum period and the equivalent Galois primitive matrix that forms the same sequence as the PRS generator?

8. Give the formula for the recursive calculation of the states of the Galois generator on the basis of the corresponding Galois matrix.

9. In what transposition are the Galois and Fibonachi matrices interconnected?

10. Give an expression for the similarity transformation of conjugate elements of a group.

11. Give a table of the relationship between the basic and conjugate Galois andFibonacci matrices.

12. In which directions (clockwise or counter-clockwise) are feedback in the registers of basics and conjugate generators Galois and Fibonacci?

13. Give the definition of the generalized Galois matrix.

14. Explain the essence of the generalized rule of diagonal filling (synthesis) of Galois matrices.

15. For what reason are the generalized Galois matrices non-degenerate?

16. How can raise a matrix $\boldsymbol{G}_{f,\omega}^{(n)}$ to the power k ?

17. Condition for the primitiveness of the generalized Galois matrix?

18. Explain the reason for the commutativity of two arbitrary generalized Galois matrices generated by the same irreducible polynomial.

19. How is the generalized similar Galois matrix formed?

20. What is the principle of isomorphism of Galois matrices?

21. Give the structural-logical schemes of the basic and conjugate generalized Galois and Fibonacci generators.

21. Give the structural and logical diagrams of basic and conjugate generalized Galois and Fibonacci generators.

22. What are the consequences of multiplying an arbitrary polynomial $\omega_k(x)$ of degree k on a formal variable x?

23. Define the characteristic polynomial $\chi(\lambda)$ of a nondegenerate square matrix $\boldsymbol{A}$ of $n-$th order.

24. Formulate the property of characteristic polynomials of similar matrices.

25. What are the basic axioms of the field $GF(p_2^n)$

26. Give the definition of a three-dimensional (cubic) matrix $n-$th order over the field $GF(p)$.

27. The reason for the commutativity of an arbitrary pair $r-$ dimensional spatial Galois matrices?

BASIC ABBREVIATIONS

LFB - linear feedbacks;

MIP - matrix of inverse permutation;

MS - multiplicative sequence;

MPG - multiplicative group;

MPGMO - multiplicative group of maximal order;

SFT - small Fermat theorem;

IP – irreducible polynomial;

GGM – generalized Galois matrix;

FB – feedbacks;

GE – generating element;

SPRN - Sequence of pseudorandom numbers;

PP – primitive polynomial;

PRS – pseudorandom sequence;

PNS – positional number system;

PRN pseudorandom numbers;

SR – shift register;

SRLFB - shift register with linear feedbacks;

XOR – logical operation of addition modulo 2, otherwise – exclusive “OR”;

THE RECOMMENDED LITERATURE

1. Algebra and Number Theory. Uch. allowance under the ed. N. Ya. Vilenkina. — Moscow: Education, 1984. — 194 p.

2. I.M. Vinogradov, Fundamentals of Number Theory. I.M. Vinogradov. — Moscow: Regular and chaotic dynamics, 2003. — 178 p.

3. Glyn-Jones T. Oddities of digits and numbers. Trans. from English. / T. Glyn-Jones. — Moscow: RIPOL classic, 2009. — 208 p.

4. N. Ya. Vilenkin, Congruences and residue classes, Kvant, No. 10, 1978. — P. 4-8.

5. Prasolov V.V. Polynomials — M .: MCCME, 2001. — 336 p.

6. Liddle R., Niderider G. Finite fields / R. Liddle, H. Niderair. — Moscow: Mir, 1988. — T. 1. — 432 p.

7. Benyash-Krivets V.V. Lectures on algebra: groups, rings, fields. — Syllabus / V.V. Benyash-Krivets, O.V. Melnikov. — Minsk: BSU, 2008. — 116 p.

Educational edition

Anatoly Beletsky
Nikolay Glazunov
Denis Navrotskyi

Algebraic foundations of coding theory and cryptography

Textbook

160