BELARUSIAN STATE UNIVERSITY
OF INFORMATICS AND RADIOELECTRONICS

APPLIED MATHEMATICS

Ministry of Education of the Republic of Belarus
Belarusian State University of Informatics and Radioelectronics

APPLIED MATHEMATICS

Course Materials
Prepared by
D.N. Oleshcevich, N.V. Spichekova

Minsk 2013

CONTENTS

Introduction

Students of BSUIR study the whole range of issues related to handling, storage, transfer and protection information against interference and unauthorized access. Relevant lecture courses are relatively new, many of them are in the dynamics of formation or development in accordance with the technological revolution and needs of time, and require to explore new areas of mathematics which are not included in the classical course "Higher Mathematics" – appropriate facilities of higher technical education. Such courses as "Digital Signal Processing", "Applied Coding Theory", "Cryptographic methods of information protection", and a number of others require a thorough knowledge of modern algebra.

Therefore Department of Higher Mathematics develops the course "Applied Mathematics", which lays a foundation of modern applied algebra and creates a mathematical foundation for information protection against interference and unauthorized access. Over the years, this course is successfully read to BSUIR students of specialities "Information", "Telecommunication Networks", "Multimedia Information Distribution Systems", "Information Security in Telecommunications".

Experience shows that deep and reliable acquisition of new material is not possible without its thorough elaboration during practical and laboratory classes. This publication is a study guide to carry out practical and laboratory classes on the course named above. A working model for eight practical and laboratory studies on the main themes of the course is proposed. Depending on tradition, lab assignments can be considered as hometasks for self-study and personal development.

Laboratory Study № 1 «Number Theory»

Necessary Theoretical Data

Below we consider: the set of natural numbers, denoted by N; the set of integers, denoted by Z.

The set of integers Z is countable, consists of elements 0; ±1; ±2;...; $\pm n$;... . Two algebraic operations are defined on it – addition and multiplication. These operations have the following properties (for any $a,b,c \in Z$):

1. associativity: $a+(b+c)=(a+b)+c$; $a\cdot(b\cdot c)=a\cdot(b\cdot c)$;
   commutativity: $b+a=a+b$; $a\cdot b=b\cdot a$;
2. there exist the identity elements 0 and 1:
$$a+0=0+a=a; \quad a\cdot 1=1\cdot a=a;.$$
3. $(a+b)\cdot c=a\cdot c+b\cdot c$ – distributive law;
4. for every integer $a \in Z$ there exists a unique additive inverse, i.e., there exists a unique integer b such that $a+b=b+a=0$. The additive inverse of a number $a \in Z$ is also called the opposite number of a.

Theorem 1.1 (the division algorithm). *For any integers a and b, $b \neq 0$, there exist unique integers q and r, $0 \le r < |b|$, such that $a=b\cdot q+r$.*

In this equality r is called the *remainder* and q is called the *quotient* (the *incomplete quotient* if $r \neq 0$) resulting from division of a by b. If $r=0$ then b and q are called divisors or factors of a. Everyone has been able to find the quotient and remainder by long division method since one's school-days.

Corollary. Let b be a natural number, $b>1$. For any integer a and the maximal integer $m \ge 0$ that satisfies the condition $a > b^m$ there exist unique integers a_i, $0 \le a_i < b$, $0 \le i \le m$, such that

$$a=\pm(a_m b^m + a_{m-1} b^{m-1} + ... + a_0).$$

This equality is written shortly as $a=\pm(a_m a_{m-1}...a_0)_b$ or $a=\pm a_m a_{m-1}...a_0$ (if b is known from context) and is called the notation of a in positional base b numeral system or in numeral system of base b. The usual positional base 10 numeral system (it is also called the decimal system) seems to be normal and natural. But in different situations other bases are more convenient. For instance, on a computer's micro level all calculations are carried out in the binary (base 2) numeral system. The hexadecimal (base 16) positional numeral system is used for conversion from the decimal to the binary numeral system.

Lemma 1.1. *If in the equality $a_1+a_2+\ldots+a_n=b_1+b_2+\ldots+b_m$ all items are integers and all except maybe one are divided by an integer d, then this excluded item is also divided by d.*

Definition 1.1. If integers $a_1,a_2,\ldots,a_n$ are divided by an integer d then d is called their common divisor.

Subsequent discussion deals only with positive integer divisors.

Definition 1.2. The largest positive *integer* among all common divisors of integers $a_1, a_2, \dots, a_n$ is called their greatest common divisor and is written as *GCD*($a_1, a_2, \dots, a_n$).

Theorem 1.2. *If* $a = b \cdot q + c$ *then GCD(a,b)=GCD(b,c).*

Theorem 1.2 allowed Euclid (approximately 2300 years ago) to base the following fact.

Theorem 1.3. *The greatest common divisor of integers a and b (a>b) is equal to the last different from zero remainder in the chain of equalities:*

$$a = b \cdot q_1 + r_1;$$
$$b = r_1 \cdot q_2 + r_2;$$
$$\dots\dots\dots\dots\dots\dots$$
$$r_{n-2} = r_{n-1} \cdot q_n + r_n;\ i.e.,\ r_n = GCD(a,b).$$
$$r_{n-1} = r_n \cdot q_{n+1}.$$

Theorem 1.3 formulates the Euclidean algorithm (also called Euclid's algorithm) for computing the greatest common divisor of two integers. The Euclidean algorithm can also be formulated in another way that gives us the second method to find the greatest common divisor. Namely, we compute the differences $a - b = c;\ b - c = d; \dots$ until we get the last non-zero difference which coincides with *GCD(a,b)*.

Example 1.1. Using the Euclidean algorithm find GCD(72, 26).

Solution. In accordance with Theorem 2.2 we have $72 = 26 \cdot 2 + 20$; $26 = 20 \cdot 1 + 6$; $20 = 6 \cdot 3 + 2$; $6 = 2 \cdot 3$. Hence, GCD(72, 26) $= 2$.

Theorem 1.4. *If* $d = GCD(a,b)$ *then there exist two integers u and v such that the following identity (Bezout's identity) takes place:* $d = au + bv$.

Example 1.2. It follows from example 1.1 that

$$2 = 20 + 6 \cdot (-3) = 20 + (26 + 20 \cdot (-1)) \cdot (-3) = 20 \cdot 4 + 26 \cdot (-3) =$$
$$= (72 + 26 \cdot (-2)) \cdot (4 + 26 \cdot (-3)) = 72 \cdot 4 + 26 \cdot (-11).$$

Such a way of computing the integers *u* and *v* for Bezout's identity is called the extended Euclidean algorithm. It consists of two steps. The first one (up-sweep step) is actually the Euclidean algorithm. On the second step (it is called down-sweep step) we sequentially express remainders for every stage of the previous step and combine like terms.

Definition 1.3. A natural number $p > 1$ is called a prime number if it has no positive integer divisors other than 1 and *p* itself.

Theorem 1.5. *Every natural number* $n > 1$ *is either prime or has a prime divisor.*

Suppose that *p* and *q* are natural numbers greater than 1; then from the formula $n = p \cdot q$ it follows that either p or q lies in the interval $[2; \sqrt{n}]$. We obviously have that the least natural divisor $p > 1$ of a natural number $n > 1$ is a prime number. Historically the first method of verifying whether a natural number $n > 1$ is prime or not was a method called "the sieve of Eratosthenes". It works as follows: one divides a given natural number $n > 1$ by all prime numbers less than or equal to $\sqrt{n}$. If any of the divisions come out as an integer then the original number is not a prime. Otherwise it is a prime. The sieve of Eratosthenes was created by Eratosthenes, an ancient Greek mathematician. Nowadays there are fairly large number of primality tests.

Theorem 1.6 (Euclid's theorem). *The number of primes is infinite. .*

Theorem 1.5 establishes importance of prime numbers: every nonzero natural number can be factored into primes. Therefore primes are building blocks of all natural numbers.

Definition 1.4. Two integers a and b are said to be coprime or relatively prime if $GCD\,(a,b)=1$.

Theorem 1.7 (coprimeness criterion). *Two integers a and b are relatively prime iff there exist integers u and v such that $a \cdot u + b \cdot v = 1$.*

Corollary. $GCD(ac,b)=1$ if and only if $GCD(a,b)=1,\ GCD(c,b)=1$.

The following property of primes is very important in number theory and its applications.

Lemma 1.2. Let the product ab of integers a and b is divided by an integer c and $GCD(a,c)=1$. Then b is divided by c.

Theorem 1.8 (the fundamental theorem of arithmetic). *Every integer $n > 1$ can be written as a unique product (up to the order of the factors) of prime numbers*

$$n = \pm p_1 \cdot p_2 \cdot \ldots \cdot p_s.$$

If we collect the same factors in this equality we obtain the canonical decomposition of n: $n = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots p_t^{r_t}$.

Example 1.3. Let consider examples of the canonical decomposition of integers:

a) $196 = 2{\cdot}98 = 2{\cdot}2{\cdot}49 = 2^2{\cdot}7^2$; b) $2^{12} - 1 = 4095 = 3^2 \cdot 5 \cdot 7 \cdot 13$.

Theorem 1.9. *Let m be a natural number, $m > 1$; then for any integers a and b the following conditions are equivalent:*

1) *a and b leave the same remainder upon division by m;*

2) *$a - b$ is divided by m, i.e., $a - b = mq$ for a suitable integer q;*

3) *$a = b + mq$ for some integer q.*

Definition 1.5. Two integers a and b are said to be congruent modulo m if they satisfy one of the conditions of Theorem 1.9. It is denoted by the symbol $a \equiv b(\mathrm{mod}\, m)$ or $a \equiv b(m)$ which is read "*a* is congruent to *b* modulo *m*". *m* is called the modulus of the congruence.

Example 1.4. $-5 \equiv 7(\mathrm{mod}\ 4) \equiv 11(\mathrm{mod}\ 4) \equiv 23(\mathrm{mod}\ 4) \equiv 3(\mathrm{mod}\ 4)$.

Example 1.5. Suppose $a = mq + r$; then $a \equiv r(\mathrm{mod}\, m)$, i.e., every integer is congruent modulo *m* to its remainder upon division by *m*. It follows from definition 1.5 and the second condition of theorem 1.9 (because $a - r$ is divided by m).

Basic properties of congruences

1. Let be $a \equiv b(\mathrm{mod}\, m)$. Then $(a \pm c) \equiv (b \pm c)(\mathrm{mod}\, m)$ for any integer c. It means that we can add (subtract) the same integer on both sides of a congruence.

2. We can add and subtract congruences term by term: if $a \equiv b(\mathrm{mod}\, m)$, $c \equiv d(\mathrm{mod}\, m)$ then $(a+c) \equiv (b+d)(\mathrm{mod}\, m)$; $(a-c) \equiv (b-d)(\mathrm{mod}\, m)$.

3. We can also multiply congruences term by term: if $a \equiv b(\mathrm{mod}\, m)$, $c \equiv d(\mathrm{mod}\, m)$ then $ac \equiv bd(\mathrm{mod}\, m)$.

4. We can raise both sides of a congruence to the same natural power: if $a \equiv b(\mathrm{mod}\, m)$ then $a^n \equiv b^n(\mathrm{mod}\, m)$.

5. If in the congruence $a \equiv b(\mathrm{mod}\, m)$ integers a, b, m have a common factor d then the congruence can be reduced by it: $\frac{a}{d} \equiv \frac{b}{d}\left(\mathrm{mod}\left(\frac{m}{d}\right)\right)$.

6. A congruence can be reduced by a common multiple coprime to modulus: if $a = da_1, b = db_1$, $GCD\,(d, m) = 1$ then from the congruence $da_1 \equiv db_1(\mathrm{mod}\, m)$ we obtain: $a_1 \equiv b_1(\mathrm{mod}\, m)$.

7. We can multiply both sides of a congruence on an arbitrary integer factor: if $a \equiv b(\mathrm{mod}\, m)$ then $at \equiv bt(\mathrm{mod}\, m)$ for an arbitrary integer t.

8. Reflexivity: $a \equiv a\,(\mathrm{mod}\, m)$ for an arbitrary integer a and any natural number $m > 1$.

9. Symmetry: if $a \equiv b\,(\mathrm{mod}\, m)$ then $b \equiv a\,(\mathrm{mod}\, m)$.

10. Transitivity: if $a \equiv b\,(\mathrm{mod}\, m)$ and $b \equiv c\,(\mathrm{mod}\, m)$ then $a \equiv c\,(\mathrm{mod}\, m)$.

Theorem 1.10 (Fermat's Little Theorem). *Let p be a prime number which does not divide an integer a. Then $a^{p-1} \equiv 1(\mathrm{mod}\, p)$.*

Congruence theory and little Fermat's theorem allow us to find the remainder in division of a large natural number by a prime number.

Example 1.6. Find the remainder in division of 39^{149} by 31.

Solution. 31 is a prime. 39 is not divided by 31. Therefore $39^{30} \equiv 1(\mathrm{mod}\, 31)$. Hence $39^{149} = 39^{30 \cdot 3+29} \equiv 39^{29}(\mathrm{mod}\, 31)$. Further $39 \equiv 8(\mathrm{mod}\, 31)$. Therefore in accordance with the fourth property of congruences we have $39^2 \equiv 8^2 \equiv 2(\mathrm{mod}\, 31)$. In binary notation we obtain: $29 = 11101$. Hence, for an arbitrary natural a we have $a^{29} = a^{2^4} \cdot a^{2^3} \cdot a^{2^2} \cdot a$. Further, $39^4 \equiv 8^4 \equiv 2^2(\mathrm{mod}\, 31)$. Therefore, $39^8 = (39^4)^2 \equiv 4^2(\mathrm{mod}\, 31)$. Then $39^{16} = (39^8)^2 \equiv 16^2(\mathrm{mod}\, 31) \equiv 8(\mathrm{mod}\, 31)$. Hence,

$$39^{29} \equiv 8 \cdot 16 \cdot 4 \cdot 8(\mathrm{mod}\, 31) \equiv 4 \cdot 4 \cdot 8(\mathrm{mod}\, 31) \equiv 4(\mathrm{mod}\, 31).$$

Thus, the remainder in division of 39^{149} by 31 is 4.

Problems for Classroom

Problem 1.1. Find the canonical decomposition for numbers $a = 627, b = 399$.

Solution.

627	3	399	3
209	11	133	7
19	19	19	19
1			

Hence $627 = 3{\cdot}11{\cdot}19$, $399 = 3{\cdot}7{\cdot}19$.

Problem 1.2. Find GCD(627, 399) using:
a) the Euclidean algorithm; b) the prime decomposition.

Solution. Let use the Euclidean algorithm:
$627 = 399 \cdot 1 + 228$;
$399 = 228 \cdot 1 + 171$;
$228 = 171 \cdot 1 + 57$;
$171 = 57 \cdot 3$. Hence GCD (627; 399) = 57.

We find GCD(a, b) using the prime decomposition of numbers a and b obtained in the solution of Problem 1.1:

$$627 = 3 \cdot 11 \cdot 19;\; 399 = 3 \cdot 7 \cdot 19.$$

Hence, the greatest common divisor is equal to the product of the same factors in the decomposition of the given numbers: GCD (627; 399) = $3 \cdot 19 = 57$.

Let find GCD(a, b) by the subtraction method:
$627 - 399 = 228$; $399 - 228 = 171$; $228 - 171 = 57$; $171 - 57 = 114$;
$114 - 57 = 57$; $57 - 57 = 0$. Hence, GCD(627; 399) = 57.

Problem 1.3. Using the extended Euclidean algorithm find integers u, υ, satisfying the Bezout's identity: $au + b\upsilon = GCD\,(a, b)$ for the integers $a = 110$; $b = 48$.

Solution. At first we find GCD (110, 48) by the Euclidean algorithm:
$110 = 48 \cdot 2 + 14$;
$48 = 14 \cdot 3 + 6$;
$14 = 6 \cdot 2 + 2$;
$6 = 3 \cdot 2$. Hence, GCD (110, 48) = 2.

Now we construct the Bezout's identity for the given a and b:
$110 = 48 \cdot 2 + 14$; therefore $14 = 110 + 48 \cdot (-2)$;
$48 = 14 \cdot 3 + 6$; therefore $6 = 48 + 14 \cdot (-3)$;
$14 = 6 \cdot 2 + 2$; therefore $2 = 14 + 6 \cdot (-2)$. In this equality we substitute the above expression for 6 and combine like terms relatively 48 and 14.
So $2 = 14 + 6 \cdot (-2) = 14 + (48 + 14 \cdot (-3))(-2) = 14 \cdot 7 + 48 \cdot (-2)$.

Substituting the above expression for 14 in the resulting expression for GCD(110, 48) = 2 we get $2 = 14 \cdot 7 + 48 \cdot (-2) = (110 + 48 \cdot (-2))\,7 + 48 \cdot (-2) = 110 \cdot 7 + 48 \cdot (-16) = 2$.

Problem 1.4.

a) represent the decimal number 137 in the binary numeral system.

Solution. We iteratively divide 137 by 2:

```
_137 |_2
 12  |_68 |_2
 _17   68 |_34 |_2
  16    0   34 |_17 |_2
   1         0   16 |_8 |_2
                  1   8 |_4 |_2
                      0   4 |_2 |_2
                          0   2 |_1 |_2
                              0   0 | 0
                                  1
```

The required representation is formed by the remainders written in the reverse order:

$$137 = 10001001_2;$$

b) transfer the number 10001001_2 to the decimal system:

$1\,0\,0\,0\,1\,0\,0\,1_2 = (1 \cdot 2^7 + 0 \cdot 2^6 + 0 \cdot 2^5 \cdot 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0) =$
$= 7\ \ 6\ \ 5\,4\,3\ \ 2\,1\,0.$

$(2^7 + 2^3 + 1)_{10} = 128 + 8 + 1 = 137_{10};$

c) transfer the number 10000 to base 8 number system:

```
_10000 |_8
  8    |_1250 |_8
 _20      8   |_156 |_8
  16     _45     8  |_19 |_8
  _40     40    _76  16 |_2 |_8
   40    _50     72   3   0 | 0
    0     48      4       2
           2
```

$10000_{10} = 23420_8.$

Problem 1.5. Multiplication and addition in base 16 number system.

The hexadecimal numeral system uses numbers 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 and letters A, B, C, D, E, F. Symbols A, B, C, D, E, F are used to represent the following decimal values: letter A – value 10, letter C – 11, C – 12, D – 13, E – 14, F – 15.

Let construct Table 1.1 and Table 1.2 to perform arithmetic operations in the hexadecimal numeral system.

Table 1.1Hexadecimal Addition Table

+	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10
2	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11
3	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11	12
4	4	5	6	7	8	9	A	B	C	D	E	F	10	11	12	13
5	5	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14
6	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14	15
7	7	8	9	A	B	C	D	E	F	10	11	12	13	14	15	16
8	8	9	A	B	C	D	E	F	10	11	12	13	14	15	16	17
9	9	A	B	C	D	E	F	10	11	12	13	14	15	16	17	18
A	A	B	C	D	E	F	10	11	12	13	14	15	16	17	18	19
B	B	C	D	E	F	10	11	12	13	14	15	16	17	18	19	1A
C	C	D	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B
D	D	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C
E	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D
F	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E

Table 1.2

Hexadecimal Multiplication Table

×	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
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	10	12	14	16	18	1A	1C	1E
3	0	3	6	9	C	F	12	15	18	1B	1E	21	24	27	2A	2D
4	0	4	8	C	10	14	18	1C	20	24	28	2C	30	34	38	3C
5	0	5	A	F	14	19	1E	23	28	2D	32	37	3C	41	46	4B
6	0	6	C	12	18	1E	24	2F	30	36	3C	42	48	4E	54	5A
7	0	7	E	15	1C	23	2A	31	38	3F	46	4D	54	5B	62	69
8	0	8	10	18	20	28	30	38	40	48	50	58	60	68	70	78
9	0	9	12	1B	24	2D	36	3F	48	51	5A	63	6C	75	7E	87
A	0	A	14	1E	28	32	3C	46	50	5A	64	6E	78	82	8C	96
B	0	B	16	21	2C	37	42	4D	58	63	6E	79	84	8F	9A	A5
C	0	C	18	24	30	3C	48	54	60	6C	78	84	90	9C	A8	B4
D	0	D	1A	27	34	41	4E	5B	68	75	82	8F	9C	A9	B6	C3
E	0	E	1C	2A	38	46	54	62	70	7E	8C	9A	A8	B6	C4	D2
F	0	F	1E	2D	3C	4B	5A	69	78	87	96	A5	B4	C3	D2	E1

Now let consider on a n example how two numbers can be added directly and with Table 1.1.

$$\begin{array}{r} 8A97F \\ +\ 29873 \\ \hline B41F2 \end{array}$$

$F+3=12$ (write down 2, transfer 1 to the senior level);

$7+7=E+1=F$ (write down F in the sum);

$9+8=11$ (write down 1, transfer 1 to the senior level);

$A+9+1=13+1=14$ (write down 4, transfer 1 to the senior level);

$8+2+1=A+1=B$ (write down B).

Table 1.1 is used as follows: the first addend (in the given example F, 7, 9, A or 8) is found in the top row of the table; the second addend (in the given example accordingly 3, 7, 8, 9 or 2) is found in the leftmost column, and the sum of numbers is found at the intersection of columns and rows:

$$\begin{array}{r} 7AC93.F94 \\ +\ 9C78F.F89 \\ \hline 117423.F1D \end{array}$$

Addition table (see Table 1.1) can be used as subtraction table:

$$\begin{array}{r} 13086 \\ -\ 8988 \\ \hline A6FE \end{array}$$

6 – 8 (subtract the ones columns. Since we can’t subtract 8 from 6 we need to borrow “1” from the tens column. Our “6” in the ones column becomes “16”. The “8” in the tens column becomes “7”);

$10+6-8=16-8=$ E;

7 – 8 (subtract the tens column. Since we can’t subtract 8 from 7 we need to borrow “1” from the hundreds column. The hundreds column contains 0. Therefore we need to borrow “1” from the next column to the left. As a result “1” from the fourth column becomes “10” for the third column; “7” in the tens column increases to “17”. “3” in the fourth column is replaced by “2”; “0” in the hundreds column becomes “F”);

$10+7-8=17-8=F$;

$F-9=6$;

2 – 8 (subtract the fourth column. Since we can’t subtract 8 from 2 we need to borrow “1” from the fifth column. “2” in the fourth column becomes “12”);

$10+2-8=12-8=A$.

To find the difference between two numbers with Table 1.1 we find the subtrahend in the top row, find the minuend in the column corresponding to the subtrahend, and take the difference in the leftmost column in accordance with the minuend.

The multiplication is carried out as follows: $8\cdot 4=20$ (write down 0, carry 2 to the senior level).

$8\cdot 9 = 4\underbrace{8+2}_{10=A} = 4A$ (write down A, transfer 4 to the hundreds level);

$8\cdot 7 = 3\overbrace{8+4}^{12=C} = 3C$ (write down 3, write down C);

$7\cdot 4 = 1C$ (write down C, carry 1 to the senior level);

$7\cdot 9 - 1 = 3\overset{\frown}{F} + 1 = 40$ (write down 0, transfer 4 to the senior level);

$7\cdot 7 + 4 = 31 + 4 = 35$ (write down 3, write down 5);

$3\cdot 4 = C$ (write down C);

$3\cdot 9 = 1B$ (write down B, carry 1 to the senior level);

$3\cdot 7^{+1} = 15 + 1 = 16$ (write down 1, write down 6).

Let sketch the scheme of solution (we use table 1.2):

×	…	8
…		↓
4	→	20
…		↓
7	→	38
…		↓
9	→	48

×	…	7
…		↓
4	→	1C
…		↓
7	→	35
…		↓
9	→	3F

×	…	3
…		↓
4	→	C
…		↓
7	→	15
…		↓
9	→	1B

Problem 1.6.

a) find the remainder in division of 2^{100} by 3.

Solution. The first method: the remainder when 2 is divided by 3 is 2, the remainder when 2^2 is divided by 3 is 1. If we continue to raise 2 to the power and divide it by 3 we find that the remainders alternate: 2, 1, 2, 1, 2 … . Due to evenness of 100 the remainder of division of the required number by 3 is equal to 1.

The second method: using congruences and arguing as in Example 1.6 we see: $2^{100} = 4^{50} = (3+1)^{50} \equiv 1^{50} = 1$;

b) find the remainder of $1989\cdot 1990\cdot 1991 + 1992^3$ upon division by 7.

Solution. Replace every number with its remainder of division by 7:

```
_1989 |_7_        _1990 |_7_        1991 = 7 · 284 + 3;
 14   | 284        14   | 284
 _58               _59              1992 = 7 · 284 + 4.
  56                56
  _29               _30
   28                28
    1                 2
```

$1 \cdot 2 \cdot 3 + 4^3 = 6 + 64 = 70$. $70 : 7 = 10$. Hence the remainder is equal to 0.

c) find the remainder in division of 9^{100} by 8.

Solution. Replace 9 with its remainder 1 of division by 8. We have $1^{100} = 1$. Hence the remainder of division of 9^{100} by 8 is equal to 1;

d) find the remainder of 3^{1989} upon division by 7.

Solution. The remainder when 3 is divided by 7 is 3. The remainder when 3^2 is divided by 7 is 2. Further it is sufficient to multiply the remainder by 3 and make a conclusion. The remainder when 3^3 is divided by 7 is 6, the remainder when 3^4 is divided by 7 is 4, the remainder when 3^5 is divided by 7 is 5, the remainder when 3^6 is divided by 7 is 1, the remainder when 3^7 is divided by 7 is 3. We got one of the previous remainders, i.e., we have a cycle. The number 3^7 has the same remainder upon division by 7 as 3^1. Therefore the length of the cycle is 6. $1989 = 331 \cdot 6 + 3$. The number 3^{1989} gives the same remainder upon division by 7 as 3^3, i.e., 6.

Self Instructional Problems for Laboratory Study № 1 «Number Theory»

1. Find the canonical decomposition of the integers a and b.

2. Find GCD(a,b) using:

a) the Euclidean algorithm; b) the prime decomposition of integers.

3. Using the extended Euclidean algorithm find integers u, υ satisfying Bezout's identity: $au + b\upsilon = GCD\,(a, b)$.

4. Represent the given decimal number c in base q, 16, and 2 numeral systems.

5. Evaluate … in base 16 numeral system.

Variant 1.

1–3. $a = 101398751$, $b = 326147777$. 4. $q = 7$, $c = 972405821$.

5. Evaluate the determinant $\begin{vmatrix} A2 & -D & BC \\ -3B & 1F & 5C \\ -EA & 18 & 98 \end{vmatrix}$

6. Find the remainder in division of 1998^{2001} by 29.

Variant 2.

1–3. $a = 5999801$, $b = 48685811$. 4. $q = 5$, $c = 5999801$.

5. Solve the system of equations $\begin{cases} DAx - Fy = 8, \\ 20x + 8y = 90. \end{cases}$

6. Find the remainder in division of 2005^{2003} by 17.

Variant 3.

1–3. $a = 660422941$, $b = 36481301$. 4. $q = 8$, $c = 5999801$.

5. Solve the system of equations $\begin{cases} Dx - F1y = -6F, \\ Bx + 61y = \tilde{N}F. \end{cases}$

6. Find the remainder in division of 2001^{2005} by 17.

Variant 4.

1–3. $a = 9002242397$, $b = 433817903$. 4. $q = 7$, $c = 5090801$.

5. Evaluate the product of two matrices:

$$\begin{pmatrix} BF & -3A & CD \\ 10 & 3E & -F2 \\ -90 & AE & FA \end{pmatrix} \begin{pmatrix} A1 & BB & -17 \\ -AD & CF & 9E \\ 2A & -BA & FB \end{pmatrix}.$$

6. Find the remainder in division of 2004^{2998} by 19.

Variant 5.

1–3. $a = 9118515943$, $b = 3386496689$. 4. $q = 7$, $c = 75928301$.

5. Evaluate the product of two matrices:

$$\begin{pmatrix} B3 & -3B & FD \\ A0 & 7E & -FA \\ -9C & BE & DA \end{pmatrix} \begin{pmatrix} CA & BF & -E7 \\ -AC & DF & B0 \\ 7A & -BC & 3B \end{pmatrix}.$$

6. Find the remainder in division of 1999^{2005} by 23.

Variant 6.

1–3. $a = 5336161097$, $b = 196210799$. 4. $q = 9$, $c = 73425826$.

5. Evaluate the determinant $\begin{vmatrix} AB & -2D & FC \\ -3C & AF & BC \\ -EF & 1A & A8 \end{vmatrix}$.

6. Find the remainder in division of 1998^{2001} by 19.

Variant 7.

1–3. $a = 7049964661$, $b = 168687989$. 4. $q = 7$, $c = 93475825$.

5. Evaluate the determinant $\begin{vmatrix} 2B & -AD & BC \\ -9C & A8 & B6 \\ -EE & 4C & AF \end{vmatrix}$.

6. Find the remainder in division of 1997^{2004} by 17.

Variant 8.

1–3. $a = 83748733$, $b = 73435591$. 4. $q = 7$, $c = 86425836$.

5. Evaluate the determinant $\begin{vmatrix} 7B & -2D & FC \\ -3C & AF & BE \\ -E3 & 10 & A8 \end{vmatrix}$.

6. Find the remainder in division of 1996^{2003} by 11.

Variant 9.

1–3. $a=$ 16254559, $b=$ 1029073. 4. $q=7$, $c=$ 86425836.

5. Evaluate the product $(Fx^2+1Ax-3F)(Cx^2-ABx+E3)$.

6. Find the remainder in division of 2006^{1998} by 19.

Variant 10.

1–3. $a=$ 6099377, $b=$ 9568217. 4. $q=8$, $c=$ 87625859.

5. Evaluate the product $(F1x^2+BAx-35)(CAx^2-A3x+ED)$.

6. Find the remainder in division of 2010^{1999} by 17.

Variant 11.

1–3. $a=$ 7957549, $b=$ 23118553. 4. $q=7$, $c=$ 89605809.

5. Evaluate the product $(B5x^2+CAx-3A)(CDx^2-ABx+E9)$.

6. Find the remainder in division of 2005^{1999} by 19.

Variant 12.

1–3. $a=$ 16088437, $b=$ 18216949. 4. $q=7$, $c=$ 38615802.

5. Evaluate the product $(5Ax^2+CBx-2A)(CEx^2-A8x+EF)$.

6. Find the remainder in division of 1995^{2004} by 16.

Variant 13.

1–3. $a=$ 244604911, $b=$ 61875907. 4. $q=8$, $c=$ 79605819.

5. Evaluate the product $(F5x^2+CBx-BA)(C5x^2-A0x+F9)$.

6. Find the remainder in division of 2011^{1999} by 17.

Variant 14.

1–3. $a=$ 356216713, $b=$ 31238065. 4. $q=7$, $c=$ 85678539.

5. Evaluate the product $(45x^2+C2x-3B)(C5x^2-FBx+E0)$.

6. Find the remainder in division of 2005^{2004} by 19.

Variant 15.

1–3. $a = 7409621$, $b = 6793883$. 4. $q = 7$. $c = 9605801$.

5. Evaluate the product $(A5x^2 + CCx - 5A)(CFx^2 - 5Bx + EF)$.

6. Find the remainder in division of 2005^{2002} by 29.

Laboratory Study № 2 «Residue Classes»

Necessary Theoretical Data

When we divide an arbitrary integer by a natural number $m > 1$ we obtain one of m different remainders: $0, 1, 2, \ldots, m-1$. In accordance with these remainders the set of integers Z is divided into m disjoint classes of integers having the same remainder when divided by m. Such classes are called congruence classes modulo m or residue classes modulo m. Depending on the remainders upon division by m the residue classes are denoted as $\bar{0}, \bar{1}, \ldots, \overline{m-1}$. Thus we have class $\bar{i} = (mq + i \mid q \in Z)$ for every integer $i = 0,1,2,\ldots,m-1$. Every residue class is uniquely defined by any its representative: for every natural number $mq + i$ the class is $\overline{mq+i} = \bar{i}$. The set of congruence classes modulo m is denoted as Z/mZ. From the above it follows that Z/mZ has m elements and can be written as $Z/mZ = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$.

By the second property of congruences (see theoretical data for the first laboratory study) we obtain that for arbitrary classes $\bar{k}, \bar{l} \in Z/mZ$ and for arbitrary $k_1, k_2 \in \bar{k}, l_1, l_2 \in \bar{l}$ the sums $k_1 + l_1$ and $k_2 + l_2$ are congruent modulo m. Therefore $k_1 + l_1$ and $k_2 + l_2$ belong to the same class Z/mZ. In a similar manner the products $k_1 \cdot l_1$ and $k_2 \cdot l_2$ lie in the same class from Z/mZ. Let define addition and multiplication on Z/mZ. For any two residue classes $\bar{k} \in Z/mZ$, $\bar{l} \in Z/mZ$ we determine a sum class $\bar{k} \oplus \bar{l}$ so that the sum $k + l$ lie in the sum class for any $k \in \bar{k}, l \in \bar{l}$. Similarly for any two residue classes $\bar{k} \in Z/mZ$, $\bar{l} \in Z/mZ$ we define a product class $\bar{k}\,\bar{l}$ so that the products $\tilde{k} \cdot \tilde{l}$ lie in the product class for any $\tilde{k} \in \bar{k}, \tilde{l} \in \bar{l}$.

Since addition and multiplication in Z/mZ are uniquely determined by addition and multiplication of class representatives, properties 1 – 5 of addition and multiplication of integers (see theoretical data for the first laboratory study) are also valid in Z/mZ:

1) $\bar{k} \oplus \bar{i} = \bar{i} \oplus \bar{k}$; $\bar{l}\bar{k} = \bar{k}\bar{l}$ – commutativity;

2) $\bar{k} \oplus (\bar{l} \oplus r) = (\bar{k} \oplus \bar{l}) \oplus r$; $\bar{k}(\bar{l}r) = (\bar{k}\bar{l})\, r$ – associativity;

3) there exists the identity element (or the neutral element): $\bar{k} \oplus \bar{0} = \bar{k}$; $\bar{k}\,\bar{1} = \bar{k}$;

4) for every $\bar{k} \in Z/mZ$ there exists a unique class $\bar{l}$, such that $\bar{k} \oplus \bar{l} = \bar{0}$. It is obvious that $\bar{l} = \overline{m-k}$;

5) $(\bar{k} \oplus \bar{l})\bar{r} = (\bar{k}\bar{r}) \oplus (\bar{l}\bar{r})$ – distributive law.

As the operations of addition and multiplication in Z/mZ have the properties mentioned above Z/mZ belongs to the class of commutative rings with a multiplicative identity and is variously called quotient ring, factor ring, residue class ring or simply residue ring of Z modulo m.

Definition 2.1. An element $\bar{k} \in Z/mZ$ is called invertible if there exists a class $\bar{l} \in Z/mZ$ such that $\overline{kl} = \bar{1}$. The class $\bar{l}$ is called the inverse class of $\bar{k}$.

From the associative law for Z/mZ it follows that if $\bar{k}$ is an invertible class, then the inverse class is uniquely determined.

Lemma 2.1. Let $\bar{k} \in Z/mZ$ be a class such that $GCD(k, m) = 1$. Then:

1) for any $\bar{l} \neq \bar{0}$ we have $\bar{k}\,\bar{l} \neq \bar{0}$;

2) $\bar{k} \cdot \bar{l}_1 \neq \bar{k} \cdot \bar{l}_2$, if $\bar{l}_1 \neq \bar{l}_2$;

3) the mapping $f : \bar{x} \to \bar{k} \cdot \bar{x}$ is injective and hence bijective on the set Z/mZ (on the set of nonzero elements from Z/mZ);

4) $\bar{k}$ is invertible in the ring Z/mZ.

Remark. Under the conditions of Lemma 2.1 we have $GCD(d, m) = 1$. Therefore according to the coprimeness criterion there exist integers $u, v \in Z$ such that $ku + mv = 1$. Then $\bar{1} = \overline{ku} + \overline{mv} = \bar{k}\bar{u}$. Hence $\bar{u}$ is the inverse class for $\bar{k}$.

Lemma 2.2. Let $\bar{k} \in Z/mZ$ be a class such that $GCD(k, m) = d > 1$. Then:

1) there exists a class $\bar{l} \neq \bar{0}$ such that $\bar{k}\,\bar{l} = \bar{0}$;

2) there exists classes $\bar{l}_1 \neq \bar{l}_2$, such that $\bar{k} \cdot \bar{l}_1 = \bar{k} \cdot \bar{l}_2$;

3) for all $\bar{l} \neq \bar{0}$ we get $\bar{k} \cdot \bar{l} \neq 1$, i.e., the class $\bar{l}$ is not invertible in the ring Z/mZ.

Theorem 2.1. *A class $\bar{k} \in Z/mZ$ Z/mZ is invertible iff* $GCD(k, m) = 1$. *If $m = p$ is a prime number then every nonzero class in Z/pZ is invertible. An inverse class is also invertible. The product of invertible classes is also an invertible class.*

Since Z/mZ consists of finite number of elements, addition and multiplication can be set elementwise in the form of tables.

Example 2.1. Let write down the addition and multiplication tables for the ring $Z/3Z$

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$

$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

From the multiplication table it is immediately clear that classes $\overline{1}$ and $\overline{2}$ are inverse of themselves, i.e., all nonzero classes of $Z/3Z$ are invertible in full accordance with Theorem 2.1.

Definition 2.2. The Euler's totient function (Euler function phi, the totient, Euler's phi function, the phi function) $\varphi(m)$ is a function of a natural argument $m > 1$, counting the number of integers which are less than or equal to m and coprime to m.

Here are the basic multiplicative properties of the Euler's totient function.

Property 1. $\varphi(p) = p - 1$ for any prime p.

Property 2. $\varphi(p^n) = p^n - p^{n-1}$ for any prime p and an arbitrary natural number $n \geq 1$.

Property 3. If $GCD(n, m) = 1$ then $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$.

Property 4. If $n = p_1^{S_1} p_2^{S_2} \ldots p_t^{S_t}$ is a canonical decomposition of n then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_t}\right).$$

Example 2.2. Let calculate $\varphi(48)$. From the obvious equality $48 = 3 \cdot 2^4$ and property 4 we get $\varphi(48) = 48 \cdot (1 - 1/3) \cdot (1 - 1/2) = 16$.

Example 2.3. Theorem 2.1 implies that there are exactly $\varphi(m)$ invertible classes in the ring Z/mZ. For example, $\varphi(12) = 4$. Hence there are exactly 4 invertible elements in the ring $Z/12Z$. Direct verification shows that these classes are $\overline{1}, \overline{5}, \overline{7}, \overline{11}$.

Theorem 2.2 (Euler's' theorem). *If m is a natural number and a is a positive integer coprime to m then* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

An equation of the form

$$a_n x^n + a^{n-1} + \ldots + a_1 x + a_0 x^0 \equiv 0 \pmod{m},$$

where $a_n, a_{n-1}, \ldots, a_0 \in Z$, $n \in N$, $a_n \not\equiv 0 \pmod{m}$, is called an algebraic congruence equation of the *n*th degree and one unknown *x*.

Assume that when we substitute x_0 instead of x in a congruence we get a correct numeric congruence. In this case x_0 is called a solution of the congruence. At the same time any integer of the form $x_0 + mt$ is also a solution of the congruence. Therefore the residue class $\overline{x_0}$ can be considered as a solution of the algebraic congruence. The universal method to solve the algebraic congruence is to examine it with a complete system of residues modulo m, i.e., integers $0, 1, 2, \ldots, m - 1$. The number of solutions of the congruence is equal to number of elements which belong to the complete residue system and satisfy the congruence.

Example 2.4. Solve the congruence $x^5 + x + 1 \equiv 0 \pmod{7}$.

Solution. Let consider the complete system of residues modulo 7: 0,1, 2, 3, 4, 5, 6. Substituting the elements of this system into the congruence we obtain that only two numbers $x = 2$, $x = 4$ satisfy the congruence. Therefore the given congruence has two solutions: $x \equiv 2 (\mathrm{mod}\, 7)$, $x \equiv 4 (\mathrm{mod}\, 7)$.

While solving a congruence it is convenient to use transformations leading to equivalent congruences.

Problems for Classroom

Problem 2.1. Compute $\varphi(n)$ for all natural numbers n from 2 till 12.

Problem 2.2. Compute $\varphi(60)$, $\varphi(81)$, $\varphi(89)$, $\varphi(2017)$, $\varphi(2018)$.

Solution. $60 = 2^2 \cdot 3 \cdot 5$. By the property 4 of the Euler's totient function we have

$$\varphi(60) = 60\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 2 \cdot 2 \cdot 4 = 16.$$

$81 = 3^4$. Therefore in accordance with property 2 of the Euler's totient function, we obtain

$$\varphi(81) = 3^4 - 3^{3-1} = 3^4 - 3^3 = 81 - 27 = 54.$$

$\sqrt{89} < 10$; 89 is not divided by 2, 3, 5, 7 (any prime number less than 10) without a remainder. Hence 89 is a prime number. Therefore $\varphi(89) = 88$.

Problem 2.3. Write down the addition and multiplication tables for the rings $Z/5Z$ and $Z/6Z$. Find pairs of mutually multiplicative inverse elements in these rings. Calculate number of such pairs and compare this number with $\varphi(5)$ and $\varphi(6)$ respectively.

Solution is similar to the solution of Example 2.1.

Problem 2.4. Find the inverse element for every invertible element in the residue class ring modulo 15.

Solution can be obtained by writing down the multiplication table in the ring $Z/15Z$. Let consider another way to solve this problem.

By Theorem 2.1 there are $\varphi(15) = 8$ residue classes comprime to modulo $m = 15$ in the ring $Z/15Z$. Direct verification shows that these classes form the set $G = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \overline{11}, \overline{13}, \overline{14}\}$.

In terms of congruences the equality $\bar{a} \cdot \bar{x} = \bar{1}$ in case of $\bar{a} \in G$ looks like $ax \equiv 1 \pmod{15}$. From Euler's theorem it follows that $a^8 \equiv 1 \pmod{15}$. Multiplying both sides of the congruence $ax \equiv 1 (\mathrm{mod}\, 15)$ by a^7, we get $x \equiv a^7 (\mathrm{mod}\, 15)$ in accordance with congruence properties. Successively we compute:

$2^7 = 2^3 \cdot 2^4 = 8 \cdot 16 \equiv 8 \pmod{15}$. Therefore $\left(\bar{2}\right)^{-1} = \bar{8}$;

$4^7 = 4^6 \cdot 4 = 16^3 \cdot 4 \equiv 4 \pmod{15}$. Hence $\left(\bar{4}\right)^{-1} = \bar{4}$;

$7^7 = 49^3 \cdot 7 \equiv 4^3 \cdot 7 \equiv 13, \left(\bar{7}\right)^{-1} \equiv \overline{13};$

$11^7 = 121^3 \cdot 11 = 1^3 \cdot 11 \equiv 11(\mathrm{mod}\,15), \left(\overline{11}\right)^{-1} = 11;$

$14^7 = 2^7 \cdot 7^7 \equiv 8 \cdot 13(\mathrm{mod}\,15) \equiv (-7)\cdot(-2)(\mathrm{mod}\,15) = 14(\mathrm{mod}\,15); \left(\overline{14}\right)^{-1} = \overline{14}.$

Problem 2.5. Find the inverse elements for the classes $\bar{5}, \bar{6}, \bar{7}$ in the ring: a) $Z/2016Z$; b) $Z/2017Z$.

Solution. $GCD(2016, 5) = 1$. Let find this greatest common divisor by the Euclidean algorithm: $2016 = 5 \cdot 403 + 1$. From the last formula we can easily obtain Bezout's identity for $GCD(2016, 5) = 1$: $1 = 2016 \cdot 1 + 5 \cdot (-403)$. In accordance with the remark to Lemma 2.1 we have: $5^{-1} = \overline{-403} = 2016 - 403 = 1613$. Verification:

$$5 \cdot 1613 = 8065 = 2016 \cdot 4 + 1 \equiv 1\,(\mathrm{mod}\,2016).$$

$GCD(2016, 6) = 6 > 1$. Therefore 6^{-1} does not exist in the ring $Z/2016Z$.

Self Instructional Problems for Laboratory Study № 2 «Residue Classes»

1. Write down the addition and multiplication tables in the rings:
a) Z/kZ; b) Z/nZ.

2. Compute $\varphi(k), \varphi(n)$ for k, n from the first problem; compute $\varphi(m)$ for the integer m from the fourth problem.

3. Find pairs of mutually multiplicative inverse elements in the rings Z/kZ and Z/nZ from the first problem.

4. Find the inverse elements for classes $\bar{5}, \bar{6}, \bar{7}$ in the ring Z/mZ.

5. Solve the congruence.

6. Solve the system of equations in the ring Z/nZ: $\begin{cases} \overline{13}x + \bar{5}y = \overline{11}; \\ \bar{7}x + \overline{11}y = \overline{13}. \end{cases}$

7. Solve the equation $x^2 + \bar{5}x + \bar{7} = 0$ in the ring Z/kZ.

Variant 1.

1. $k = 11$; $n = 24$. 4. $m = 2001$. 5. $132x^3 + 143x^2 + 23x - 19 \equiv 5\,(\mathrm{mod}\,11)$.

Variant 2.

1. $k = 13$; $n = 18$. 4. $m = 2002$. 5. $169x^3 + 143x^2 + 23x - 19 \equiv 5\,(\mathrm{mod}\,13)$.

Variant 3.

1. $k = 23$; $n = 12$. 4. $m = 2000$. 5. $253x^3 + 46x^2 + 29x - 49 \equiv 5\,(\mathrm{mod}\,23)$.

Variant 4.

1. $k=17$; $n=21$. 4. $m=2003$. 5. $187x^3+34x^2+23x-19\equiv 5 \pmod{17}$.

Variant 5.

1. $k=19$; $n=26$. 4. $m=2004$. 5. $132x^3+143x^2+23x-19\equiv 5 \pmod{11}$.

Variant 6.

1. $k=13$; $n=27$. 4. $m=2005$. 5. $117x^3+143x^2+3x-19\equiv 5 \pmod{13}$.

Variant 7.

1. $k=7$; $n=28$. 4. $m=2006$. 5. $63x^3+154x^2+23x-19\equiv 5 \pmod{7}$.

Variant 8.

1. $k=29$; $n=12$. 4. $m=2007$. 5. $319x^3+145x^2+23x-19\equiv 5 \pmod{29}$.

Variant 9.

1. $k=23$; $n=14$. 4. $m=2008$. 5. $253x^3+115x^2+12x-9\equiv 5 \pmod{23}$.

Variant 10.

1. $k=31$; $n=12$. 4. $m=2009$. 5. $341x^3+155x^2+23x-19\equiv 5 \pmod{31}$.

Variant 11.

1. $k=17$; $n=30$. 4. $m=2010$. 5. $85x^3+204x^2+13x-19\equiv 5 \pmod{17}$.

Variant 12.

1. $k=29$; $n=9$. 4. $m=2011$. 5. $145x^3+348x^2+23x-17\equiv 5 \pmod{29}$.

Variant 13.

1. $k=17$; $n=22$. 4. $m=2012$. 5. $153x^3+187x^2+11x-9\equiv 5 \pmod{17}$.

Variant 14.

1. $k=19$; $n=14$. 4. $m=2013$. 5. $361x^3+209x^2+23x-11\equiv 5 \pmod{19}$.

Variant 15.

1. $k=16$; $n=23$. 4. $m=2014$. 5. $95x^3+228x^2+23x-9\equiv 5 \pmod{19}$.

Laboratory Study № 3 «Group Theory»

Necessary Theoretical Data

Definition 3.1. A group is a nonempty set G, equipped with a binary operation $(\cdot)$, such that the following conditions hold:

1) associativity: $a\cdot(b\cdot c)=(a\cdot b)\cdot c$ for all $a, b, c \in G$;

2) there exists an identity element (neutral element), i.e., there exists an element $e\in G$ such that $g\cdot e=e\cdot g=g$ for all $g\in G$;

3) for every element $g\in G$ there exists an inverse element, i.e., an element $h\in G$ such that $g\cdot h=h\cdot g=e$ (written $h=g^{-1}$).

The groups are distinguished by the number of elements and properties of the binary operation (commutative and noncommutative) in accordance with the following

Definition 3.2. A group G is said to be commutative or abelian if the operation defined on it has (in addition to properties 1) – 3)) property·

4) $b\cdot a=a\cdot b$ for all $a, b\in G.$

Definition 3.3. The number of elements in a finite group G is called the order of G, denoted by $|G|$.

Traditionally all additive groups (with addition operation) belong to the class of commutative groups. For every natural number n there exists a commutative finite group of order n. For example, $(Z/nZ, +)$.

Theorem 3.1. *Let a be a fixed element of an arbitrary group G. Let* $<a>=\{a^0=e, a, a^2, ..., a^{-1}, a^{-2}, ...\}$ *be the set of all possible powers of the element a. Then* $<a>$ *is an abelian group.*

Definition 3.4. The group $<a>$ from Theorem 3.1 is called the cyclic group generated by the element a.

Theorem 3.2. *Let an element* $a\in G$ *has the property:* $a^n=e$ *for some integer n and* $a^k\neq e$ *for all integers k,* $1\leq k<n$. *Then the cyclic group* $<a>$ *has order n and* $<a>=\{a, a^2, ..., a^n=e\}$.

Definition 3.5. The value n from Theorem 3.2 is called the order of the element $a\in G$. If no such n exists for an element $a\in G$ we say that $a\in G$ has infinite order.

From Definition 3.4, it follows that any cyclic group is abelian, contains a countable or finite set of elements, and in the second case has a clear structure, expressed by Theorem 3.2.

Theorem 3.3. *For every prime p the set of nonzero congruence classes in the* *residue class ring Z/pZ form a group Z/pZ^* under multiplication and this group is cyclic.*

Let Ω be a finite set of n elements. Since the nature of its elements is not essential, it is convenient to suppose that $\Omega = \{1, 2, ..., n\}$.

Definition 3.6. Every bijection, i.e., a one-to-one correspondence from Ω to itself, is called a permutation of Ω.

It is convenient to present a permutation $f: i \to f(i)$, $i = 1, 2, ..., n$, in the form of a table with two rows: $f = \begin{pmatrix} 1 & 2 & ... & n \\ f(1) & f(2) & ... & f(n) \end{pmatrix}$. In this table one lists numbers $1, 2, ..., n$ in the first row and their image under permutation below it in the second row. The composition of two permutations is just the composition of the associated functions: $(gf)(i) = g(f(i))$. This composition is called the product of permutations. Most often $gf \neq fg$, i.e., the product of permutation is not commutative. Obviously the identity permutation $e = \begin{pmatrix} 1 & 2 & ... & n \\ 1 & 2 & ... & n \end{pmatrix}$ is the neutral element for this product. Since composition of functions is associative, the product of permutations is associative too. For every permutation there exists the inverse one. To find the inverse permutation f^{-1} it is sufficient to interchange two lines in the table $\begin{pmatrix} 1 & 2 & ... & n \\ f(1) & f(2) & ... & f(n) \end{pmatrix}$ and then sort columns so that elements of the first row are placed in ascending order.

Thus, the set of all permutations of Ω forms a group under product of permutations. It is called the symmetric group on n elements and is denoted by S_n.

Theorem 3.4. *The symmetric group S_n has order $n!$.*

Let f be an arbitrary permutation from S_n. We delete columns with the same elements from the table with two rows specifying f.

Definition 3.7. A cycle of length k is a permutation of the form

$$f_k = (i, f(i), ..., f^{t_k - 1}(i)) = \begin{pmatrix} i & f(i) & ... & f^{t_k - 1}(i) \\ f(i) & f^2(i) & ... & i \end{pmatrix}.$$

A cycle of length 2 is also called a transposition. Cycles without common elements are called *independent cycles* or *disjoint cycles*.

Theorem 3.5. *Every permutation $f \in S_n$ can be decomposed into a product of disjoint cycles of length $l \geq 2$. This representation is unique up to the order of the cycles.*

Theorem 3.6. *Every permutation $f \in S_n$ can be expressed as a product of transpositions. Any two decompositions of f contain either even or odd number of transpositions.*

Example 3.1. Factor the following permutation into a product of cycles and transpositions:

$$g=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 2 & 4 & 5 & 3 & 1 & 7 & 9 & 6 & 8\end{pmatrix}.$$

Solution.

$g=(1\ \ 2\ \ 4\ \ 3\ \ 5)(6\ \ 7\ \ 9\ \ 8)=(1\ \ 5)(1\ \ 3)(1\ \ 4)(1\ \ 2)(6\ \ 8)(6\ \ 9)(6\ \ 7).$

Decomposition of a permutation into a product of transpositions is not unique. For example, the above permutation can be expressed as the following product of transpositions:

$g=(1\ \ 2\ \ 4\ \ 3\ \ 5)(6\ \ 7\ \ 9\ \ 8)=(1\ \ 5)(1\ \ 3)(1\ \ 4)(1\ \ 2)(6\ \ 8)(3\ \ 4)(6\ \ 9)(3\ \ 4)(6\ \ 7).$

Definition 3.8. A permutation f is called even (odd) if it can be written as the product of even (odd) number of transpositions.

Problems for Classroom

Problem 3.1. Give ten examples of a group. Why do you think that this is really a group? Is this an abelian group? Is your group finite?

Problem 3.2. Determine whether the set $\widetilde{C}$ of all complex numbers having unit absolute value form a group under multiplication.

Solution. 1) $z_1\cdot(z_2\cdot z_3)=(z_1\cdot z_2)\cdot z_3$ holds for any complex numbers;
2) for all complex number z we have $z\cdot 1=1\cdot z=z$. Hence $e=1$ is the identity;
3) for every $z=x+iy\in\widetilde{C}$ we have $|z|=\sqrt{x^2+y^2}=1$ by condition, i.e., $x^2+y^2=1$; therefore $\bar{z}=x-iy$ is the inverse for $z=x+iy\in\widetilde{C}$:

$$z\cdot\bar{z}=(x+iy)\cdot(x-iy)=z\cdot\bar{z}=(x-iy)\cdot(x+iy)=x^2+y^2=1.$$

Thus $\widetilde{C}$ is a group.

Problem 3.3. Determine whether the set of all positive real numbers is a group under binary operation of raising to the power.

Solution. The answer is no because the associative law is not valid for this operation. For example, $(2^3)^4=2^{12}$, and $2^{(3^4)}=2^{81}$.

Problem 3.4. Factor the following permutation into a product of cycles and transpositions:

$$f=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 7 & 4 & 3 & 1 & 6 & 5 & 2\end{pmatrix}.$$

Determine the parity (oddness or evenness) of f.

Solution. The permutation f moves 1 into 7, 7 into 2, 2 into 4, 4 into 1. By Definition 3.7 a permutation acting on 1, 7, 2, 4 in accordance with this rule and leaving all other elements unchangeable is called a cycle of length 4. In compliance with Definition 3.7 this cycle is shortly written as (1724). Also f moves 3 to 3, 5 to 6, and 6 to 5. So the record $f=(1724)(3)(56)$ indicates how f moves elements of the set $\{1,2,3,4,5,6,7\}$. Since a cycle consisting of one element coincides with the identity permutation, it is usually omitted, i.e., $f=(1\ 7\ 2\ 4)(5\ 6)$ is the product of cycles. Hence we obtain the decomposition of f into the product of transpositions: $f=(1\,4)(1\,2)(1\,7)(5\,6)$. As we see f is even.

Problem 3.4. Evaluate the product $f\cdot g^{-1}$ for $f=\begin{pmatrix}1&2&3&4&5&6&7\\3&6&5&2&1&7&4\end{pmatrix}$ and $g=\begin{pmatrix}1&2&3&4&5&6&7\\7&3&2&6&4&1&5\end{pmatrix}$.

Solution. $g^{-1}=\begin{pmatrix}1&2&3&4&5&6&7\\6&3&2&5&7&4&1\end{pmatrix}$. Then $f\cdot g^{-1}=\begin{pmatrix}1&2&3&4&5&6&7\\7&5&6&1&4&2&3\end{pmatrix}$.

Problem 3.5. Find the product of cycles and transpositions

$$(3\ \ 2\ \ 8\ \ 9)(1\ \ 6\ \ 8)(7\ \ 3)(9\ \ 6\ \ 4\ \ 5)(1\ \ 9).$$

Solution.

$$(3\ \ 2\ \ 8\ \ 9)(1\ \ 6\ \ 8)(7\ \ 3)(9\ \ 6\ \ 4\ \ 5)(1\ \ 9)=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\9&8&7&5&3&4&2&1&6\end{pmatrix}.$$

Problem 3.6. Write down the cyclic group generated by the permutation

$$f=\begin{pmatrix}1&2&3&4&5&6&7\\3&6&5&2&1&7&4\end{pmatrix}.$$

Solution. $f^2=\begin{pmatrix}1&2&3&4&5&6&7\\5&7&1&6&3&4&2\end{pmatrix}$; $f^3=\begin{pmatrix}1&2&3&4&5&6&7\\1&4&3&7&5&2&6\end{pmatrix}$;

$f^4=\begin{pmatrix}1&2&3&4&5&6&7\\3&2&5&4&1&6&7\end{pmatrix}$; $f^5=\begin{pmatrix}1&2&3&4&5&6&7\\5&6&1&2&3&7&4\end{pmatrix}$;

$f^6=\begin{pmatrix}1&2&3&4&5&6&7\\1&7&3&6&5&4&2\end{pmatrix}$; $f^7=\begin{pmatrix}1&2&3&4&5&6&7\\3&4&5&7&1&2&6\end{pmatrix}$;

$f^8=\begin{pmatrix}1&2&3&4&5&6&7\\5&2&1&4&3&6&7\end{pmatrix}$; $f^9=\begin{pmatrix}1&2&3&4&5&6&7\\1&6&3&2&5&7&4\end{pmatrix}$;

$f^{10}=\begin{pmatrix}1&2&3&4&5&6&7\\3&7&5&6&1&4&2\end{pmatrix}$; $f^{11}=\begin{pmatrix}1&2&3&4&5&6&7\\5&4&1&7&3&2&6\end{pmatrix}$;

$f^{12}=\begin{pmatrix}1&2&3&4&5&6&7\\1&2&3&4&5&6&7\end{pmatrix}=e$.

By Theorem 3.2 the group $<f>$ has order 12.

Problem 3.7. Determine whether the matrix $A=\begin{pmatrix}1&0&0\\0&1&0\\0&1&1\end{pmatrix}$ with elements from the residue class ring $Z/2Z$ is invertible.

Solution. Let find the determinant of A: $\det A=1\neq 0$. Hence matrix A is invertible.

Problem 3.8. Write down the cyclic group generated by the matrix from the previous problem and determine its order.

Solution. $A^2=\begin{pmatrix}1&0&0\\0&1&0\\0&1&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&0\\0&1&1\end{pmatrix}=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}=E$. Thus $<A>=\{A,A^2=E\}$ has order 2.

Problem 3.9. Determine whether an additive group G is cyclic:

a) G is the group of real numbers;

b) G is the group of rational numbers.

Self Instructional Problems for Laboratory Study № 3 «Group Theory»

1. Determine whether the given set equipped with the operation is a group.

2. a) factor the permutation f into the product of cycles and transpositions. Determine its parity;

b) evaluate the commutator $h=g^{-1}f^{-1}gf$ for the given permutations f and g;

c) find the product of cycles and transpositions.

3. Write down the cyclic group $<f>$. Determine its order.

4. Determine whether the matrix B with elements from $Z/2Z$ is invertible.

5. Write down the cyclic group $<B>$. Determine its order.

6. Find f^{1000} for the permutation f from Problem 2 and B^{1000} for the matrix B from Problem 4.

Variant 1

1. The set of integers, Z, with subtraction operation.

2. a) $f=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&9&5&6&8&4&1&3&7\end{pmatrix}$; b) $g=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\4&1&8&6&9&7&3&2&5\end{pmatrix}$;

c) $(7\ 1\ 8\ 5)(4\ 6\ 3)(8\ 2)(9\ 1\ 3\ 5)$. 4. $B=\begin{pmatrix}1&0&1\\1&1&1\\1&1&0\end{pmatrix}$.

Variant 2

1. The set of all positive real numbers with division operation.

2. a) $f=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\3&6&9&1&7&8&5&2&4\end{pmatrix}$; b) $g=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\4&1&8&6&9&7&3&2&5\end{pmatrix}$;

c) $(3\ 1\ 9\ 5)(4\ 2\ 3)(8\ 9)(7\ 1\ 6\ 5)$. 4. $B=\begin{pmatrix}0&1&1\\1&1&0\\1&1&1\end{pmatrix}$.

Variant 3

1. The set of integers with operation $m*n=mn+m$.

2. a) $f=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\5&9&8&3&1&4&2&6&7\end{pmatrix}$; b) $g=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\4&1&8&6&9&7&3&2&5\end{pmatrix}$;

c) $(4\ \ 2\ \ 6\ \ 9)(5\ \ 2\ \ 7)(7\ \ 9)(7\ \ 3\ \ 8\ \ 1)$. 4. $B=\begin{pmatrix}1&0&1\\1&1&1\\1&0&0\end{pmatrix}$.

Variant 4

1. The set of integers with operation $m*n=m+2n$.

2. a) $f=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\9&6&2&8&1&3&4&7&5\end{pmatrix}$; b) $g=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\4&1&8&6&9&7&3&2&5\end{pmatrix}$;

c) $(2\ \ 4\ \ 9\ \ 5)(1\ \ 3\ \ 7)(5\ \ 8)(7\ \ 1\ \ 3\ \ 6)$. 4. $B=\begin{pmatrix}0&0&1\\0&1&1\\1&1&0\end{pmatrix}$.

Variant 5

1. The set of integers with multiplication.

2. a) $f=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\3&4&5&6&7&8&9&2&1\end{pmatrix}$; b) $g=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\4&1&8&6&9&7&3&2&5\end{pmatrix}$;

c) $(9\ \ 1\ \ 3\ \ 5)(6\ \ 2\ \ 8)(2\ \ 9)(7\ \ 1\ \ 4\ \ 8)$. 4. $B=\begin{pmatrix}1&0&1\\0&0&1\\0&1&1\end{pmatrix}$.

Variant 6

1. The set of real numbers with division operation.

2. a) $f=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\9&6&5&1&7&2&3&4&8\end{pmatrix}$; b) $g=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\4&1&8&6&9&7&3&2&5\end{pmatrix}$;

c) $(7\ \ 3\ \ 9\ \ 5)(4\ \ 1\ \ 3)(8\ \ 6)(9\ \ 1\ \ 2\ \ 5)$. 4. $B=\begin{pmatrix}1&0&1\\0&0&1\\1&1&0\end{pmatrix}$.

Variant 7

1. The set of complex numbers with operation $z_1\otimes z_2=\sqrt{z_1z_2}$.

2. a) $f=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\9&8&1&6&3&7&4&5&2\end{pmatrix}$; b) $g=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\4&1&8&6&9&7&3&2&5\end{pmatrix}$;

c) $(9\ \ 1\ \ 4\ \ 5)(3\ \ 2\ \ 7)(3\ \ 6)(7\ \ 2\ \ 6\ \ 8)$. 4. $B=\begin{pmatrix}1&0&1\\0&0&1\\1&1&1\end{pmatrix}$.

Variant 8

1. The set of complex numbers with division operation.

2. a) $f=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\4&8&7&5&9&3&6&1&2\end{pmatrix}$; b) $g=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\4&1&8&6&9&7&3&2&5\end{pmatrix}$;

c) $(4\ \ 2\ \ 9\ \ 5)(7\ \ 9\ \ 3)(6\ \ 1)(8\ \ 6\ \ 5\ \ 1)$. 4. $B=\begin{pmatrix}1 & 0 & 1\\ 1 & 0 & 0\\ 0 & 1 & 1\end{pmatrix}$.

Variant 9

1. Determine whether the symmetric difference of two subgroups is a subgroup.

2. a) $f=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 9 & 6 & 5 & 1 & 7 & 2 & 8 & 4 & 3\end{pmatrix}$; b) $g=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 4 & 1 & 8 & 6 & 9 & 7 & 3 & 2 & 5\end{pmatrix}$;

c) $(9\ \ 1\ \ 3\ \ 5)(4\ \ 2\ \ 3)(5\ \ 7)(9\ \ 1\ \ 6\ \ 8)$. 4. $B=\begin{pmatrix}0 & 0 & 1\\ 1 & 0 & 1\\ 1 & 1 & 0\end{pmatrix}$.

Variant 10

1. Determine whether the relative complement of two subgroups is a subgroup.

2. a) $f=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 9 & 5 & 6 & 1 & 7 & 2 & 8 & 4 & 3\end{pmatrix}$; b) $g=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 4 & 1 & 8 & 6 & 9 & 7 & 3 & 2 & 5\end{pmatrix}$;

c) $(8\ \ 1\ \ 9\ \ 5)(1\ \ 2\ \ 3)(7\ \ 9)(4\ \ 1\ \ 6\ \ 5)$. 4. $B=\begin{pmatrix}1 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 0\end{pmatrix}$.

Variant 11

1. Determine whether the union of two subgroups is a subgroup.

2. a) $f=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 9 & 5 & 6 & 7 & 1 & 2 & 8 & 4 & 3\end{pmatrix}$; b) $g=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 4 & 1 & 8 & 6 & 9 & 7 & 3 & 2 & 5\end{pmatrix}$;

c) $(4\ \ 1\ \ 9\ \ 5)(7\ \ 2\ \ 3)(2\ \ 6)(3\ \ 1\ \ 6\ \ 8)$. 4. $B=\begin{pmatrix}0 & 0 & 1\\ 1 & 1 & 1\\ 1 & 0 & 0\end{pmatrix}$.

Variant 12

1. Determine whether the intersection of two subgroups is a subgroup.

2. a) $f=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 9 & 6 & 5 & 1 & 7 & 4 & 8 & 2 & 3\end{pmatrix}$; b) $g=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 4 & 1 & 8 & 6 & 9 & 7 & 3 & 2 & 5\end{pmatrix}$;

c) $(8\ \ 1\ \ 9\ \ 5)(9\ \ 2\ \ 3)(6\ \ 7)(7\ \ 2\ \ 4\ \ 5)$. 4. $B=\begin{pmatrix}0 & 1 & 1\\ 1 & 1 & 1\\ 1 & 1 & 0\end{pmatrix}$.

Variant 13

1. All complex numbers of the upper half plane with multiplication.

2. a) $f=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\9&6&2&1&7&5&8&4&3\end{pmatrix}$; b) $g=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\4&1&8&6&9&7&3&2&5\end{pmatrix}$;

c) $(1\ 6\ 9\ 5)(2\ 4\ 7)(3\ 9)(6\ 1\ 7\ 8)$. 4. $B=\begin{pmatrix}0&0&1\\1&0&0\\1&1&1\end{pmatrix}$.

Variant 14

1. All complex numbers of the right half plane with multiplication.

2. a) $f=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\9&6&5&1&7&2&4&8&3\end{pmatrix}$; b) $g=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\4&1&8&6&9&7&3&2&5\end{pmatrix}$;

c) $(2\ 1\ 7\ 3)(4\ 9\ 3)(4\ 7)(5\ 2\ 6\ 9)$. 4. $B=\begin{pmatrix}1&1&1\\1&0&1\\1&1&0\end{pmatrix}$.

Variant 15

1. All complex numbers of the lower half plane with multiplication.

2. a) $f=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\9&6&5&1&7&2&4&8&3\end{pmatrix}$; b) $g=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\4&1&8&6&9&7&3&2&5\end{pmatrix}$;

c) $(8\ 3\ 9\ 5)(4\ 1\ 3)(7\ 9)(6\ 1\ 2\ 5)$. 4. $B=\begin{pmatrix}1&1&1\\1&0&1\\1&1&0\end{pmatrix}$.

Laboratory Study № 4 «Subgroups»

Necessary Theoretical Data

Definition 4.1. A subgroup of a group $(G,\cdot)$ is a nonempty subset H of G that forms a group under the same operation. A subgroup H of a group G is called a proper subgroup if $H \neq G$ and $H \neq \{e\}$.

Theorem 4.1 (subgroup criterion). *A nonempty subset H of a group $(G,\cdot)$ is a subgroup iff $a, b \in H$ implies that $a\,b^{-1} \in H$.*

Typically each group has a lot of different subgroups. For example, various degrees of a fixed element of a group form a cyclic subgroup.

Theorem 4.2. *Every subgroup of a cyclic group is cyclic.*

In every non-commutative group G a maximal subgroup of elements commuting with all elements of G is of interest. This subgroup is called the center of G and is usually denoted by $Z(G)$; subgroups of $Z(G)$ are said to be central subgroups of G.

Definition 4.2. Let H be a proper subgroup of a group $(G,.)$ and $a \in G$. Then the set $aH=\{ah | h \in H\}$ is called a left coset of H in G.

If there exists $b \in G$, $b \notin H \cup aH$ then it is possible to construct a new left coset bH and so on.

Similarly one can construct a right coset. If every left coset coincides with the corresponding right coset $aH = Ha$ then the cosets are said to be two-sided. For example, in any abelian group every left coset is the same as the right one. Therefore every coset in an abelian group is two-sided. Cosets have a number of important properties.

Theorem 4.3. *Let H be a proper subgroup of a group G. Then:*

1) *every element $g \in G$ belongs to some left-coset of H in G;*
2) *two elements $a, b \in G$ belong to the same left coset ıff $a^{-1} \cdot b \in H$;*
3) *any two left cosets of H in G are either identical or disjoint;*
4) *for every $a \in G$ orders of sets aH and H are the same;*
5) *G is a disjoint union of left (right) cosets of H;*
6) *all left cosets and all right cosets of H in G have the same order.*

Definition 4.3. For a subgroup H of a group G the index of H, denoted $|G:H|$, is the number of left cosets of H in G (which is equal to the number of right cosets of H in G).

With properties of cosets the following crucial theorem in the theory of finite groups can be proved:

Theorem 4.4 (Lagrange's Theorem*). The order of a finite group is divided by the order of any its subgroup.*

Corollary 1. In a finite group the index of any subgroup is the quotient upon division of the group order by the subgroup order.

Corollary 2. Groups of prime order are cyclic and do not contain proper subgroups.

Corollary 3. If G is a finite group of n elements, then for every $a \in G$ it holds $a^n = e$. In other words the order of an element of a finite group divides the order of the group.

Definition 4.4. A subgroup H of a group G is called a normal subgroup if for every $a \in G$ it holds $aH = Ha$.

Clearly, every subgroup of index 2 is a normal subgroup.

Problems for Classroom

Problem 4.1. Give examples of a subgroup in the group $(Z,+)$. Determine whether the following set is a subgroup:

a) all negative numbers; all positive numbers;

b) all even numbers; all odd numbers;

c) set of integers from 0 to 10; from –5 to 5;

d) all integers divisible by 2009;

e) all integers with the remainder of 1999 when divided by 2009.

Problem 4.2. Give an example of subgroups a) in the group $(C,+)$ of all complex numbers with addition operation; b) in the group C^*.

Problem 4.3. Give examples of subgroups in the group $GL_n(R)$ of all nonsingular real square matrices of a given order $n \geq 2$. Find the center of this group.

Problem 4.4. How many subgroups are there in an arbitrary group? What is the minimal subgroup containing a given group element? What other elements of the group should it contain?

Problem 4.5. Determine whether the following set is a subgroup: a) the union of subgroups; b) the relative complement of a subgroup; c) the symmetric difference of two subgroups; d) the intersection of subgroups; e) the set of all k-th degrees of all elements of an abelian group.

Problem 4.6. In every group there are cyclic subgroups (sometimes they coincide with the group). Under what conditions does the group have noncyclic subgroups? Give examples.

Problem 4.7. Show that the multiplicative group $Z/8Z^*$ is abelian, but not cyclic, and $Z/9Z^8$ is cyclic.

Problem 4.8. Let $G = M_{1\times 4}(Z/2Z)$ (a set of all row matrices with four coordinates from $Z/2Z$) be a group under the operation of coordinate-wise addition modulo 2. How many elements are there in this group?

Let H be the following subset of elements of the group G:

$$\left\{\underbrace{(0\ \ 0\ \ 0\ \ 0)}_{\bar{0}},\underbrace{(1\ \ 0\ \ 1\ \ 1)}_{e_1},\underbrace{(0\ \ 1\ \ 0\ \ 1)}_{e_2},\underbrace{(1\ \ 1\ \ 1\ \ 0)}_{e_1\cdot e_2}\right\},$$

here $\overline{0} = 0$, $\overline{1} = 1$. Make sure that H is a subgroup, write down the coset table of H in G.

Solution. Since each of the coordinates takes only two values (0 or 1), then G is a group of order 16.

It has been already discussed, that the operation of coordinate-wise addition modulo 2 is associative. If we add two elements from H the result does not lead outside H, i.e., H is closed under addition. H contains the identity (it is the zero vector). Every vector from H is inverse for itself. Thus, H satisfies all axioms of the group definition. Hence H is a subgroup of G.

Write down the coset table of H in G:

№	Класс $a+H$	$\bar{a}+\bar{0}$	$\bar{a}+\bar{e}_1$	$\bar{a}+\bar{e}_2$	$\bar{a}+(\bar{e}_1+\bar{e}_2)$
1	$\bar{0}+H=H$	(0000)	(1011)	(0101)	(1110)
2	$(1000)+H$	(1000)	(0011)	(1101)	(0110)
3	$(0100)+H$	(0100)	(1111)	(0001)	(1010)
4	$(0010)+H$	(0010)	(1001)	(0111)	(1100)

Problem 4.9. List all elements of the multiplicative group $(Z/36Z)^*$, compare the number of elements in this group with $\varphi(36)$. Determine whether this group is cyclic. Write down the coset table $(Z/36Z)^* / <25>$ of the cyclic subgroup $<25>$

in the group $(Z/36Z)^*$.

Solution. $G = (Z/36Z)^* = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$. $|G| = 12$. $\varphi(36) = \varphi(2^2 \cdot 3^2) = 12$. Hence $|G| = \varphi(36)$. G is cyclic if there exists an element of order $|G|$, i.e., the cyclic group generated by an element coincides with the whole group G. Let try to find such an element. At random we select 5 and write down the cyclic group $<5>$.

$<5> = \{5,\ 25,\ 5^3 = 17,\ 5^4 = 17 \cdot 5 = 13,\ 5^5 = 13 \cdot 5 = 29,\ 5^6 = 29 \cdot 5 = 1\}$ is a subgroup of order 6. By Lagrange's Theorem all other elements of this subgroup have orders that are divisors of 6.

$<7> = \{7, 7^2 = 13, 7^3 = 13 \cdot 7 = 19, 7^4 = 19 \cdot 7 = 25, 7^5 = 25 \cdot 7 = 31, 7^6 = 31 \cdot 7 = 1\}$ is a subgroup of order 6. Hence, its elements 7, 19, 31, that do not belong to $< 5 >$, also have an order not exceeding 6.

$<11> = \{11, 11^2 = 13, 11^3 = 13 \cdot 11 = 35, 11^4 = 11 \cdot 35 = 25, 11^5 = 25 \cdot 11 = 23, 11^6 = 23 \cdot 11 = 1\}$ is a subgroup of order 6. Hence, its elements 11, 23, 35, that do not belong to the subgroups $< 7 >$ and $<5>$ also have an order not exceeding 6. Thus all 12 elements of the group G have an order not exceeding 6. Therefore G cannot be a cyclic group.

$H = <25> = \{25, 13, 1\}$ is a subgroup of three elements. Therefore the coset table $(Z/36Z)^* / <25>$ should contain $12 : 3 = 4$ cosets. The subgroup H is a coset. Here are the remaining three cosets: $5H = \{5 \cdot 25 = 17, 5 \cdot 13 = 29, 5\}$;

$7H = \{7 \cdot 25 = 31, 7 \cdot 13 = 19, 7\}$; $11H = \{11 \cdot 25 = 23, 11 \cdot 13 = 35, 11\}$.

Problem 4.10. Does the group $(Z/36Z)^*$ contain a non-cyclic subgroup?

Solution. Yes, it does. There are three elements of the second order in this group: 17, 19, 35. These elements are inverse for themselves, because from the condition $a^2 = e$ we have $a^{-1} = a$. Together with 1 these elements form a system closed under multiplication modulo 36 and hence they form a subgroup – a non-cyclic subgroup of four elements.

Self Instructional Problems for Laboratory Study № 4 «Subgroups»

Variant 1.

1. Make sure that vectors $\overline{0}(00000)$, $\overline{a}(10101)$, $\overline{b}(10011)$, $\overline{c}(00110)$ form a subgroup under addition in the group V_5 of all five-dimensional vectors with coordinates from $Z/2Z$.

2. Write down the coset table of the given subgroup in V_5.

3. List all elements of the multiplicative group of the ring: a) $Z/17Z$; b) $Z/32Z$. Compare the number of elements in this group with $\varphi(17)$ and $\varphi(32)$ correspondingly. Is this group cyclic under multiplication?

4. Write down the coset table :

a) $(Z/17Z)^*/<4>$; b) $(Z/32Z)^*/<17>$.

5. Does the group $Z/32Z$ contain a non-cyclic subgroup?

6. Is the subgroup $<f>$ for the permutation f from Problem 2, laboratory work № 3, is normal in the group S_9?

Variant 2.

1. Make sure that vectors $\overline{0}(00000)$, $\overline{a}(10110)$, $\overline{b}(11001)$, $\overline{c}(01111)$ form a subgroup under addition in the group V_5 of all five-dimensional vectors with coordinates from $Z/2Z$.

2. Write down the coset table of the given subgroup in V_5.

3. List all elements of the multiplicative group of the ring: a) $Z/19Z$; b) $Z/30Z$. Compare the number of elements in this group with $\varphi(19)$ and $\varphi(30)$ correspondingly. Is this group cyclic under multiplication?

4. Write down the coset table :

a) $(Z/19Z)^*/<7>$; b) $(Z/30Z)^*/<17>$.

5. Does the group $(Z/30Z)^*$ contain a non-cyclic subgroup?

6. Is the subgroup $<f>$ for the permutation f from Problem 2, laboratory Study № 3, is normal in the group S_9?

Variant 3.

1. Make sure that vectors $\overline{0}(00000)$, $\overline{a}(10110)$, $b(10101)$, $\overline{c}(00011)$ form a subgroup under addition in the group V_5 of all five-dimensional vectors with coordinates from $Z/2Z$.

2. Write down the coset table of the given subgroup in V_5.

3. List all elements of the multiplicative group of the ring: a) $Z/13Z$; b) $Z/34Z$. Compare the number of elements in this group with $\varphi(13)$ and $\varphi(34)$ correspondingly. Is this group cyclic under multiplication?

4. Write down the coset table :

a) $(Z/13Z)^*/<3>$; b) $(Z/34Z)^*/<19>$.

5.Does the group $(Z/34Z)^*$ contain a non-cyclic subgroup?

6. Is the subgroup $<f>$ for the permutation f from Problem 2, laboratory Study № 3, is normal in the group S_9?

Variant 4.

1. Make sure that vectors $\overline{0}(00000)$, $\overline{a}(11000)$, $b(10110)$, $\overline{c}(01110)$form a subgroup under addition in the group V_5 of all five-dimensional vectors with coordinates from $Z/2Z$.

2. Write down the coset table of the given subgroup in V_5.

3. List all elements of the multiplicative group of the ring: a) $Z/11Z$; b) $Z/28Z$. Compare the number of elements in this group with $\varphi(11)$ and $\varphi(28)$ correspondingly. Is this group cyclic under multiplication?

4. Write down the coset table :

a) $(Z/11Z)^*/<10>$; b) $(Z/28Z)^*/<17>$.

5. Does the group $(Z/28Z)^*$ contain a non-cyclic subgroup?

6. Is the subgroup $<f>$ for the permutation f from Problem 2, laboratory Study № 3, is normal in the group S_9?

Variant 5.

1. Write down all elements of the subgroup generated by vectors $\bar{a}(11011), b(11100), \bar{c}(00111)$ in the additive group V_5 of five-dimensional vectors with coordinates from $Z/2Z$.

2. Write down the coset table of the given subgroup in V_5.

3. List all elements of the multiplicative group of the ring: a) $Z/18Z$; b) $Z/31Z$. Compare the number of elements in this group with $\varphi(18)$ and $\varphi(31)$ correspondingly. Is this group cyclic under multiplication?

4. Write down the coset table :

a) $(Z/31Z)^*/<26>$; b) $(Z/18Z)^*/<17>$.

5. Does the group $(Z/18Z)*$ contain a non-cyclic subgroup?

6. Is the subgroup $<f>$ for the permutation f from Problem 2, laboratory Study № 3, is normal in the group S_9?

Variant 6.

1. Write down all elements of the subgroup generated by vectors $\bar{a}(11001), b(10110), \bar{c}(01111)$ in the additive group V_5 of five-dimensional vectors with coordinates from $Z/2Z$.

2. Write down the coset table of the given subgroup in V_5.

3. List all elements of the multiplicative group of the ring: a) $Z/29Z$; b) $Z/16Z$. Compare the number of elements in this group with $\varphi(29)$ and $\varphi(16)$ correspondingly. Is this group cyclic under multiplication?

4. Write down the coset table :

a) $(Z/29Z)^*/<12>$; b) $(Z/16Z)^*/<7>$.

5. Does the group $(Z/16Z)*$ contain a non-cyclic subgroup?

6. Is the subgroup $<f>$ for the permutation f from Problem 2, laboratory Study № 3, is normal in the group S_9?

Variant 7.

1. Write down all elements of the subgroup generated by vectors $\bar{a}(11001), b(10110), \bar{c}(01111)$ in the additive group V_5 of five-dimensional

vectors with coordinates from $Z/2Z$.

2. Write down the coset table of the given subgroup in V_5.

3. List all elements of the multiplicative group of the ring: a) $Z/17Z$; b) $Z/26Z$. Compare the number of elements in this group with $\varphi(17)$ and $\varphi(26)$ correspondingly. Is this group cyclic under multiplication?

4. Write down the coset table :

a) $(Z/17Z)^*/<2>$; b) $(Z/26Z)^*/<7>$.

5. Does the group $(Z/26Z)*$ contain a non-cyclic subgroup?

6. Is the subgroup $<f>$ for the permutation f from Problem 2, laboratory Study № 3, is normal in the group S_9?

Variant 8.

1. Write down all elements of the subgroup generated by vectors $\bar{a}(11000), b(10110), \bar{c}(01110)$ in the additive group V_5 of five-dimensional vectors with coordinates from $Z/2Z$.

2. Write down the coset table of the given subgroup in V_5.

3. List all elements of the multiplicative group of the ring: a) $Z/23Z$; b) $Z/24Z$. Compare the number of elements in this group with $\varphi(23)$ and $\varphi(24)$ correspondingly. Is this group cyclic under multiplication?

4. Write down the coset table :

a) $(Z/23Z)^*/<2>$; b) $(Z/24Z)^*/<17>$.

5.Does the group $(Z/24Z)*$ contain a non-cyclic subgroup?

6. Is the subgroup $<f>$ for the permutation f from Problem 2, laboratory Study № 3, is normal in the group S_9?

Variant 9.

1. Write down all elements of the subgroup generated by vectors $\bar{a}(11001), b(10110), \bar{c}(01111)$ in the additive group V_5 of five-dimensional vectors with coordinates from $Z/2Z$.

2. Write down the coset table of the given subgroup in V_5.

3. List all elements of the multiplicative group of the ring: a) $Z/23Z$; b) $Z/21Z$. Compare the number of elements in this group with $\varphi(23)$ and $\varphi(21)$ correspondingly. Is this group cyclic under multiplication?

4. Write down the coset table :

a) $(Z/23Z)^*/<3>$; b) $(Z/21Z)^*/<11>$.

5. Does the group $(Z/21Z)*$ contain a non-cyclic subgroup?

6. Is the subgroup $<f>$ for the permutation f from Problem 2, laboratory Study № 3, is normal in the group S_9?

Variant 10.

1. Write down all elements of the subgroup generated by vectors $b(10110), \bar{c}(01111)$ in the additive group V_5 of five-dimensional vectors with coordinates from $Z/2Z$.

2. Write down the coset table of the given subgroup in V_5.

3. List all elements of the multiplicative group of the ring: a) $Z/31Z$; b) $Z/20Z$. Compare the number of elements in this group with $\varphi(31)$ and $\varphi(20)$ correspondingly. Is this group cyclic under multiplication?

4. Write down the coset table :

a) $(Z/31Z)^*/<2>$; b) $(Z/20Z)^*/<17>$.

5. Does the group $(Z/20Z)*$ contain a non-cyclic subgroup?

6. Is the subgroup $<f>$ for the permutation f from Problem 2, laboratory Study № 3, is normal in the group S_9?

Variant 11.

1. Write down all elements of the subgroup generated by vectors $\bar{a}(11001), \bar{b}(10110)$ in the additive group V_5 of five-dimensional vectors with coordinates from $Z/2Z$.

2. Write down the coset table of the given subgroup in V_5.

3. List all elements of the multiplicative group of the ring: a) $Z/14Z$; b) $Z/37Z$. Compare the number of elements in this group with $\varphi(14)$ and $\varphi(37)$ correspondingly. Is this group cyclic under multiplication?

4. Write down the coset table :

a) $(Z/14Z)^*/<11>$; b) $(Z/37Z)^*/<3>$.

5. Does the group $(Z/14Z)*$ contain a non-cyclic subgroup?

6. Is the subgroup $<f>$ for the permutation f from Problem 2, laboratory Study № 3, is normal in the group S_9?

Variant 12.

1. Write down all elements of the subgroup generated by vectors $\bar{a}(11001), \bar{c}(01111)$ in the additive group V_5 of five-dimensional vectors with coordinates from $Z/2Z$.

2. Write down the coset table of the given subgroup in V_5.

3. List all elements of the multiplicative group of the ring: a) $Z/17Z$; b) $Z/25Z$. Compare the number of elements in this group with $\varphi(17)$ and $\varphi(25)$ correspondingly. Is this group cyclic under multiplication?

4. Write down the coset table :

a) $(Z/17Z)^*/<10>$; b) $(Z/25Z)^*/<7>$.

5.Does the group $(Z/25Z)^*$ contain a non-cyclic subgroup?

6. Is the subgroup $<f>$ for the permutation f from Problem 2, laboratory Study № 3, is normal in the group S_9?

Variant 13.

1. Make sure that vectors $\overline{0}(00000), \overline{a}(00110), \overline{b}(01001), \overline{c}(01111)$ form a subgroup under addition in the group V_5 of all five-dimensional vectors with coordinates from $Z/2Z$.

2. Write down the coset table of the given subgroup in V_5.

3. List all elements of the multiplicative group of the ring: a) $(Z/17Z)^*$; b) $(Z/27Z)^*$. Compare the number of elements in this group with $\varphi(17)$ and $\varphi(27)$ correspondingly. Is this group cyclic under multiplication?

4. Write down the coset table :

a) $(Z/17Z)^*/<10>$; b) $(Z/27Z)^*/<10>$.

5.Does the group $(Z/27Z)^*$ contain a non-cyclic subgroup?

6. Is the subgroup $<f>$ for the permutation f from Problem 2, laboratory Study № 3, is normal in the group S_9?

Variant 14.

1. Make sure that vectors $\overline{0}(00000), \overline{a}(11100), \overline{b}(00111), \overline{c}(11011)$ form a subgroup under addition in the group V_5 of all five-dimensional vectors with coordinates from $Z/2Z$.

2. Write down the coset table of the given subgroup in V_5.

3. List all elements of the multiplicative group of the ring: a) $(Z/13Z)^*$; b) $(Z/22Z)^*$. Compare the number of elements in this group with $\varphi(13)$ and $\varphi(22)$ correspondingly. Is this group cyclic under multiplication?

4. Write down the coset table :

a) $(Z/13Z)^*/<10>$; b) $(Z/22Z)^*/<7>$.

5. Does the group $(Z/22Z)^*$ contain a non-cyclic subgroup?

6. Is the subgroup $<f>$ for the permutation f from Problem 2, laboratory Study № 3, is normal in the group S_9?

Variant 15.

1. Make sure that vectors $\overline{0}(00000), \overline{a}(00111), \overline{b}(01001), \overline{c}(01110)$ form a subgroup under addition in the group V_5 of all five-dimensional vectors with coordinates from $Z/2Z$.

2. Write down the coset table of the given subgroup in V_5.

3. List all elements of the multiplicative group of the ring: a) $(Z/15Z)^*$; b) $(Z/29Z)^*$. Compare the number of elements in this group with

$\varphi(15)$ and $\varphi(29)$ correspondingly. Is this group cyclic under multiplication?

4. Write down the coset table :

a) $(Z/15Z)^*/<7>$; b) $(Z/29Z)^*/<10>$.

5. Does the group $(Z/15Z)^*$ contain a non-cyclic subgroup?

6. Is the subgroup $<f>$ for the permutation f from Problem 2, laboratory Study № 3, is normal in the group S_9?

Laboratory Study № 5 «Historical Cryptography»

Necessary Theoretical Data

The history of civilization shows that almost immediately after beginning of written languages various sorts of systems for protection information against unauthorized access were developed. Consider the most popular ones.

1. Caesar cipher (Caeser's cipher, Caesar's code, Caesar's shift). Its essence is that every plaintext letter (i.e., each letter in the encrypted message) is replaced by a letter some fixed number of positions further in the alphabet. This cipher was used by Julius Caesar in his business correspondence in the first century AD. Caesar replaced the first letter of the Latin alphabet (A) with the fourth (D), the second (B) – with the fifth (E), and the last one – with the third. In other words, the replacement was performed in accordance with the following table (see Figure 5.1):

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Figure. 5.1

Example 5.1. The famous Caeser's report to the Roman Senate describing his recent victory looked as follows:

YHQL YLGL YLFL

With fairly serious efforts to decrypt we can verify that the correct text is "Veni, vidi, vici" that means "I came, I saw, I conquered".

The Caesar cipher is referred to a class of ciphers called "simple substitution ciphers" or "substitution ciphers". These are ciphers in which every letter of the alphabet is replaced by a letter, number, symbol or any their combination.

2. Trithemius cipher. This encryption system was first published in 1518 in a treatise, written by religious abbot Trithemius (1462 - 1516). The Trithemius system represents a further improvement of the Caesar encryption system and is based on the idea of a motto. In this system the text of a motto (nowadays it is known as "key") is signed with reiteration under an encrypted text, then columnwise summation of the text and the motto letters is carried out. The obtained result is a ciphertext.

Example 5.2. Let encrypt the text «The sky is blue above Paris» with the motto «Rose». As stated above, we need to write down two lines – a line of the text and a string with the motto with reiteration. At the top and at the bottom we add a row with numbers of corresponding letters in the English alphabet. As a result we obtain the following table (see Figure. 5.3).

20	8	5	19	11	25	9	19	2	12	21	5	1	2	15	22	5	16	1	18	9	19
T	*H*	*E*	*S*	*K*	*Y*	*I*	*S*	*B*	*L*	*U*	*Å*	*A*	*B*	*O*	*V*	*E*	*P*	*A*	*R*	*I*	*S*
R	*Î*	*S*	*E*	*R*	*Î*	*S*	*E*	*R*	*Î*	*S*	*E*	*R*	*Î*	*S*	*E*	*R*	*Î*	*S*	*E*	*R*	*O*
18	15	19	5	18	15	19	5	18	15	19	5	18	15	19	5	18	15	19	5	18	15

Figure. 5.3

To obtain a ciphertext we sum numbers in each column of the table. If the sum is greater than 26 we subtract 26 from this sum. After these calculations we convert the derived number to a letter. So in the first column we get a number $20+18-26=12$, i.e., the letter «L». We continue this procedure until we get the following ciphertext:

L W X X Ñ N B X T A N J S Q H A W E T W A H

A french ambassador to Rome, Blaise de Vigenere (1523 - 1596), according to his service dealt with the problem of mail secrecy, wrote a large “Treatise on ciphers" (published in 1585). He made a practical improvement in the Trithemius cryptosystem that allowed to carry out the procedure of encryption - decryption almost automatically. In this system the role of the cipher machine is played by a square table with the alphabet. Its first line is filled with successive letters of the alphabet. The second line is the same alphabet, but shifted by one letter left – in this case it starts with the letter B and ends with the letter A. The third line starts with the letter C and ends with the letter B. And so on, up to 26 lines, inclusive. Now we revert to Example 5.2. At the intersection of the column with the first letter T and the row with the first letter R is the letter L – the first letter of the ciphertext. And so on.

In such form cryptosystems with mottoes were used for about 400 years as absolutely reliable and undecryptable, espessially in military affairs. The fact that the Trithemius system was successfully applied in the early twentieth century, is confirmed, in particular, by certain pages of the immortal book "The Good Soldier Švejk" by Jaroslav Hašek.

Practice of long usage of a cryptographic system pointed to the problem of keys. Usage of the same key over a long period of time can bring enemy to some regularity and subsequently cracking the cryptosystem. This problem has been overcome in two ways. The idea to use long keys came first. Ideally the key length coincides with the length of an encrypted text. Then, of course, the idea to change keys frequently appeared. Frequent key changes arise problems how to generate and to transfer a new key. The found solution was unexpected and brilliantly simple – a book. Participants use identical copies of the same edition of a particular book. The new key is reported by means of calling a page and a paragraph of the book. It is unlikely that two numbers sent by mail or published in the advertising section of a newspaper can give enemy meaningful information.

Vigenère table (1576 г.)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

3. Route cipher. There is a group of ciphers called "transposition ciphers". In these ciphers positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system. A "route cipher" is an example of a transposition cipher. An encrypted message is typed in the rows of a given $[n \times m]$ rectangular. A ciphertext is found if we write columns of the table.

The next example demonstrates a "router cipher".

Example 5.3. The text consisting of 30 letters is typed in the rows of a 5×6 matrix or table (Figure. 5.4):

W	*E*	*W*	*E*	*R*	*E*
D	*I*	*S*	*C*	*O*	*V*
E	*R*	*E*	*D*	*F*	*L*
E	*E*	*A*	*W*	*A*	*Y*
A	*T*	*O*	*N*	*C*	*E*

Figure. 5.4

To obtain a ciphertext it is necessary to write down matrix columns in a string starting with the first one:

WDEEA EIRET WSEAO ECDWN ROFAC EVLYE

Surely, there are other possible ways to type a message in a given table and to write down columns of the table.

We can increase complexity of encryptions discussed above if we use a motto. Namely, have written a message in the table we can rearrange columns of the table in some way.

Example 5.4. Let complicate the encrypted message from Example 5.3 by applying the motto "Matrix". According to the order of the motto's letters in the English alphabet we can assign the following numbers to them: 3,1,5,4,2,6. We write down the columns of the table from Example 5.3 in this order:

EIRET ROFAC WDEEA ECDWN WSEAO EVLYE

4. Cardan grille. Perhaps the most complicated variant of "router transposition" is a Cardano grill. Gerolamo Cardano (1501 – 1576) is a famous Italian mathematician, physician, mechanic, philosopher. As a mathematician he is renowned for being found formulas for roots of cubic equations. And as a mechanic he became famous primarily for the fact that his ideas are implemented in each car device called "cardan shaft" or "drive shaft". Finally, Cardano scored in cryptography.

Gerolamo Cardano invented the following encryption method. To send a secret message containing $4mk$ letters one make a square paper stencil containing $2m \times 2k$ squares. In the stencil one cut out mk squares so that when the stencil is applied to a blank sheet of paper in four possible ways its cuts completely cover the entire area of the sheet. The order of these four possible positions are determined in advance. Letters of a message are sequentially typed in the cuts of a stencil – the most natural variant – by rows, each row from left to right. The filled table is written sequentially – each column in a line (Figure. 5.6).

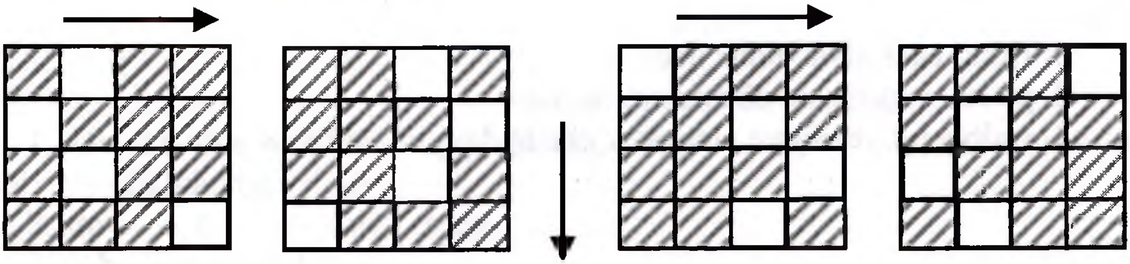

Figure. 5.6

Example 5.7. Read the message encrypted with the stencil and the procedure described above:

EGSC IINS RINB LASO

Problems for Classroom

Problem 5.1. Read the text encrypted by the Caesar cipher:
a) Pb prwkhu kdv d yhub qlfh fdu;
b) Uhdg wkh whaw hqfubswhg eb wkh Fdhvdu flskhu.

Problem 5.2. Decrypt the ciphertext created with the Vigenère table:
a) ehx pw ietzkns a zyiqn vit ;
b) pog'a hdigs cnp dkpzq am bje eafl xuxm.

Problem 5.3. Decrypt the message encrypted by a route cipher method:
a) ivyls micoe dnanv rgree imaar;
b) gkary antyg uehvo swveo smerd.

Problem 5.4. Decrypt the message encrypted with the Cardano grille:
wloteseea seielaifh hlasecces tomhoflsd

			x		
x					
x			x	x	
	x		x		
x				x	

Self Instructional Problems for Laboratory Study № 5 «Historical Cryptography»

1. Read the text encrypted by the Caesar cipher.
2. Decrypt the message encrypted by a route cipher method.
3. Decrypt the message with the motto "mathematica".
4. Decrypt the message encrypted with a Cardano grille.

Variant 1.

1. Grulv orrnhg durxqg wkh ehgurrp iru wkh odvw wlph wr pdnh fhuwdlq wkdw wkh sohdvdqw urrp, jurzq ghdu ryhu wkh sdvw wkluwb bhduv, zdv qhdw dqg wlgb
2. Hdhli eaelt slsfe olmrr ltaus
3. po rvy mgkmg od dbzesrxm?
4. wakyrernt ycwfinye plotmsvir eheihydew

x				x	
			x		x
	x		x		
				x	
		x	x		

Variant 2.

1. WKhu vnlq udq wkh jdpxw iurp d wudqvoxfhqw zklwh wr d ghhs urvh, ghshqglqj rq zkhwkhu vkh zdv dqjub, wluhg, ru haflwhg

2. Lyonr onmdo veena ewsed lhaws

3. ut bz e tizta ezttyxmigqpg detk

4. mlnieetks lielkosnd sadrlktce chltaseaa

	x			x	
x		x		x	
	x	x			
			x		x

Variant 3.

1. Zlwk wkh dgyhqw ri frpsxwhuv, wkh vlwxdwlrq kdg fkdqjhg gudpdwlfdoob, dqg hqruprxv dprxqwv ri prqhb frxog eh wudqvihuuhg lqvwdqwdqhrxvob

2. Asnpc ptwph erari dison eaaag

3. ut bz aqle eqrfh lliunz

4. httasyydi teroderan weeyvfsnd ehwarotwy

	x				
x				x	
	x				x
			x		
			x		
x		x			

Variant 4.

1. Dv vkh vhw wkh vfrufkhg phdw dqg ehdqv lq iurqw ri klp, vkh irujrw khu fduhixoob uhkhduvhg vshhfk

2. sroto oeohr rrdew csida etnoy

3. ut bz aqle eqrfh lliunz

4. seoipasse msrkolyoa ytenttptm idsolergs

		x			
x			x		
				x	
			x		x
	x				
x				x	

Variant 6.

1. Uhjxodu fxvwrphuv zhuh lvvxhg ghsrvlw volsv zlwk d shuvrqdo pdjqhwlchg frgh dw wkh erwwrp

2. iteic lomty iryec kiwbl edhie

3. ihr hvq wx lqizg mome?

4. uheueitiy hheosrdee eseabntnm toscntcbm

					x
		x			
x					
			x		
x		x		x	x
			x		

Variant 7.

1. Lq wkh rog prylhv wkh exwohu dozdbv fdph wr wkh uhvfxh zlwk d wudb ri gulqnv.

2. tyime hssoc ittsu sehtr smese

3. yy zyeznr'a paye bz oxompklpa

4.smbanoegh oohinlwhs ytahwimef edskestil

x		x		x	
			x		
			x		
	x				x
x				x	

Variant 8.

1. Wkhuhduhpdqblqwhuhvwlqjdqgqreohsurihvvlrqv

2. saiih hlkso elenu ryses elhwe

3. u lbzxqn mw napy zhkm eomtypar

4. ermnteeou teeheects reiaarida hxsvbnrft

		x			
	x		x		x
x					
		x			
			x		x
x					

Variant 9.

1. LzdqwwrvdbwkdwLfdqqrwlpdjlqhpbolihzlwkrxwwudyhoolqj
2. dowai ouwsn nkhve tnoir yowge
3. sanzw ial otemt fhxtefivioitu
4. eaaeealae ssdalnsto wxuthfeep ahehshdio

			x		x
				x	
		x			x
				x	
x			x		
	x				

Variant 10.

1. Brxwklvdyhublpsruwdqwshulrglqwkholihripdq
2. leleh issse tntas taatk lirty
3. pog'a hdigs cnp dkpzq!
4. tnyopiurt epeoducoy sdtmahess hoorsteda

					x
	x	x			
x					x
x			x	x	
	x				

Variant 11.

1. WkhfdslwdoriwkhXVDlvwkhflwbriZdvklqjwrq
2. from now you are the chosen one
3. u dhu'x wnhe yha il cmsegmte!
4.eseooohlw amtrbpyiw hxmwteano hanaruisg

	x			x	
	x				
x		x			x
				x	
			x		
					x

Variant 12

1. Lzrxogolnhwrwhoobrxderxwvkrsslqj
2. histe otiot wpbhh iolaa ssevt
3. u wtz junxl hod silipigo
4. satousose hyodoapsi idmssbsbl itatitoao

	x	x			
		x		x	
	x				
			x		x
	x				x

Variant 13

1. QhzBrunQhzBrundwwudfwshrsohiurpdooryhu
2. foaee rwrcn oyeho moton nuhse
3. u lbzxqn mw napy zhkm eomtypar
4. aiammaltf heaedoonn ncrbjueoc vneeryrae

	x				
x			x		
x		x			x
	x				
				x	
x					

Variant 14.

1. WkhHqjolvkshrsoholnhdqlpdovyhubpxfk
2. hvass eechd ymkou gemrd ibyte
3. ihta ede rww daign mz blckr?
4. berttwrwu yagdseito morbueagh aeyuihiey

			x		
				x	x
			x		
x	x				
		x			x
					x

Variant 15.

1. Pdqbuholjlrqvhalvwrqrxusodqhw
2. ohert bereu epoal yofth twgku
3. ehx pw ietzkns a zyiqn aiv
4. iensuyair lkwmasdns ieiianyum whtendnme

		x		x	
		x			
x					
			x		
x		x		x	
					x

Laboratory Study № 6 «Modern Cryptosystems»

Necessary Theoretical Data

Modern cryptography has the exact date of birth – 1976 when W. Diffie and M. Hellman published their article with the new fundamental revolutionary ideas. According to one of these ideas a good cryptosystem should be based on a one-way function. The characteristic feature of a one-way one-one function is that values of this function can be calculated easily but values of the inverse function is practically not computable without knowledge of additional information – keys. They suggested a candidate for the role of a one-way function – a function of two prime arguments $f(p,q)=p\cdot q$ for large p and q. Soon, in 1977, U.S. researchers R. Rivest, A. Shamir, and L. Adleman suggested a system of data encryption based on a one-way function. The proposed encryption system now is called the RSA cryptosystem.

1. RSA cryptosystem. The essence of the RSA cryptosystem is simple. First of all encrypted information is converted into digital format. For example, in the origin letters of the Latin alphabet were replaced by two-digits numbers: "a" = 01, «b» = 02, ..., etc. In any case, transmitted information is a natural number c. Then one choose two large prime numbers p and q, such that they do not divide c and $n=p\cdot q>c$. It is obvious that $\varphi(n)=(p-1)(q-1)$. At last one should choose a natural number e

such that $0 < e < n$ and $\text{GCD}(e, \varphi(n)) = 1$.

The encrypted message (or ciphertext) is the number $m = c^e (\text{mod}\, n)$. The pair of natural numbers (e, n) is the public key of the RSA cryptosystem.

Example 6.1. Let $p = 3$, $q = 11$. Then $n = pq = 33$, $\varphi(n) = 2\cdot 10 = 20$. Let take $e = 7$. It is easy to see that then $d = 3$. Let «S» = 19 be a message to transmit. Then the ciphertext is the number $m = c^e (\text{mod}\, n) = 19^7 (\text{mod}\, 33)$. This value we compute in several steps. $19^2 = 361 \equiv 31 (\text{mod}\, 33)$. $19^4 \equiv 31^2 (\text{mod}\, 33) = 961 \equiv 4 (\text{mod}\, 33)$. Then $19^7 \equiv 4\cdot 31\cdot 19 (\text{mod}\, 33) \equiv 13 (\text{mod}\, 33)$. Thus $m = 13$. An addressee is sent the message $(m, e, n) = (13, 7, 33)$.

The addressee receives the message (n, e, m). He like everybody knows n and e. He also need to know the secret key – such natural $d < n$ that $e\cdot d \equiv 1 (\text{mod}\, (\varphi(n)))$. Hence $e\cdot d = \varphi(n)\cdot k + 1$ for some integer k. Then by Euler's Theorem $m^d = c^{ed} = c\cdot (c^{e})^{\varphi(k)} \equiv c\cdot 1 = c\, (\text{mod}\, n)$. Thus in order to find c it is enough to find the remainder of m^d upon division by n.

It is possible to crack the RSA cryptotext only when solution d of the congruence $ex \equiv 1 (\text{mod}\, \varphi(n))$ is found. To do this an attacker need to know $\varphi(n)$. The properties of the function $\varphi(n)$ implies that the only reliable way to calculate $\varphi(n)$ is to factor n. But the problem of factorization is very labor-consuming. It is a base for the security of the RSA cryptosystem.

Example 6.2. Decrypt the RSA cryptotext $(m, e, n) = (13, 7, 33)$.

Solution. Here $d = 3$. Therefore the decryption of the message is done by the rule:

$$c = m^d (\text{mod}\, n) = 13^3 (\text{mod}\, 33) = 13^2 \cdot 13 (\text{mod}\, 33) \equiv 4\cdot 13 (\text{mod}\, 33) = 52 (\text{mod}\, 33) = 19.$$

The true message is defined completely and correctly.

2. Chinese Remainder Theorem (CRT). The Chinese Remainder Theorem (CRT) is formulated in the following way.

Theorem 6.1. *Let $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$ be the decomposition of a natural number m into a product of pairwise coprime factors. Let $b_1, b_2, \ldots, b_n$ be arbitrary fixed integers. Then the system of congruences* $\begin{cases} x \equiv b_1 (\text{mod}\, m_1), \\ \quad \ldots\ldots\ldots \\ x \equiv b_n (\text{mod}\, m_n) \end{cases}$ *always has a solution and all solutions of this system are congruent modulo m.*

Definition 6.1. In the conditions of Theorem 6.1 every integer x has n remainders b_i upon division by every divisor m_i of m. A set $(b_1, b_2, \ldots, b_n)$ is called a CRT representation of x modulo m.

The CRT-theorem states that there are infinitely many integers $\widetilde{x}$ with the same set $(b_1, b_2, \ldots, b_n)$ of remainders upon division by integers m_i. But all of them are congruent modulo m, i.e., the distance between them is a multiple of m:

$\widetilde{x} = x + mq$ for a suitable integer q. In particular it implies that the ring Z/mZ contains a unique number x with a given set $(b_1, b_2, ..., b_n)$. Thus, there is

Corollary 1. The CRT-theorem establishes one-to-one correspondence between the integers on the interval from zero up to $m-1$ inclusive and all possible sets of numbers $(b_1, b_2, ..., b_n)$ for integer b_i on the interval from zero up to $m_i - 1$ inclusive: $x \leftrightarrow (b_1, b_2, ..., b_n)$.

From the properties of relatively prime numbers and corollary 1 we obtain

Corollary 2. Under the conditions of Corollary 1 a class $\overline{x}$ is invertible in the ring Z/mZ iff every coordinate b_i from the set $(b_1, b_2, ..., b_n)$ corresponding to x generates an invertible class in Z/m_iZ.

The correspondence assigned by Corollary 1 preserves arithmetic operations on numbers due to the properties of congruences.

Corollary 3. If $x \leftrightarrow (b_1, b_2, ..., b_n)$, $y \leftrightarrow (c_1, c_2, ..., c_n)$ then

$$(x \pm y) \bmod m \leftrightarrow ((b_1 \pm c_1) \bmod m_1, (b_2 \pm c_2) \bmod m_2, ..., (b_n \pm c_n) \bmod m_n);$$

$$(x \cdot y) \bmod m \leftrightarrow ((b_1 \cdot c_1) \bmod m_1, (b_2 \cdot c_2) \bmod m_2, ..., (b_n \cdot c_n) \bmod m_n);$$

$$(x \cdot y^{-1}) \bmod m \leftrightarrow ((b_1 \cdot c_1^{-1}) \bmod m_1, (b_2 \cdot c_2^{-1}) \bmod m_2, ..., (b_n \cdot c^{-1}{}_n) \bmod m_n)$$

for an invertible element $\overline{y} \in Z/mZ$.

Further the set of all invertible classes $\overline{g}$ in the ring Z/mZ we will denote by Z/mZ^* or $U(m)$. From Euler's Theorem $\overline{g}^{\phi(m)} = \overline{1}$ for every $\overline{g} \in U(m)$ and Corollary 2 we obtain

Corollary 4. Let τ be the least common multiple of numbers $\varphi(\mathrm{m}_1)$, $\varphi(m_2), ..., \varphi(m_n)$ for $m_1, m_2, ..., m_n$ from Theorem 6.1. Then the equality $\overline{g}^{\tau} = 1$ holds for every element $\overline{g} \in U(m)$.

According to Corollary 3 of Theorem 6.1 arithmetic operations modulo m on numbers can be replaced by the same operations but on their CRT representations. At first glance such transition seems to be cumbersome. But it brings significant gain in number of operations for numbers which are clearly beyond capacity used in computers now. For example, if m is factorized into a product of two coprime factors then multiplication of their CRT representations gives approximately a twofold gain in number of operations and hence a twofold gain in time.

Even greater gain (three-fold and even fourfold) is obtained when numbers are raised to a power. Corollary 4 of Theorem 6.1 is applied to solve such problems.

Example 6.3. Let find $23^{17} (\bmod 35)$.

Solution. Traditional method

$$23^2 = 529 = 35 \cdot 15 + 4 \equiv 4 (\bmod 35);$$

$$23^4 \equiv 16 (\bmod 35);$$

$$23^8 \equiv 256 (\bmod 35) = (35 \cdot 7 + 11)(\bmod 35) \equiv 11 (\bmod 35);$$

$$23^{16} \equiv 121 (\bmod 35) \equiv 16 (\bmod 35).$$

Then $23^{17} = 23^{16} \cdot 23 \equiv 16 \cdot 23 (\mathrm{mod}\, 35) \equiv 18 (\mathrm{mod}\, 35)$.

Let try to solve the same problem through CRT representation. Since $35 = 5 \cdot 7$ and $23 \equiv 3 (\mathrm{mod}\, 5)$; $23 \equiv 2 (\mathrm{mod}\, 7)$, then the CRT representation of 23 is the pair $(3, 2)$. Here $\varphi(5) = 4$, $\varphi(7) = 6$. Therefore the least common multiple is $r = 12$. Consequently

$$3^{17} \equiv 3^5 (\mathrm{mod}\, 5) \equiv 3 (\mathrm{mod}\, 5);\ 2^{17} \equiv 2^5 (\mathrm{mod}\, 7) \equiv 4 (\mathrm{mod}\, 7).$$

Thus, the CRT representation of $23^{17} (\mathrm{mod}\, 35)$ is the pair which obviously represents the number 18.

If $n = 2; m_1 = p$ and $m_2 = q$ are prime numbers then to recover an element $x \in Z / mZ$ by its CRT representation $x \leftrightarrow (a, b)$ the following Garner's formulae are used: $x = (((b - a)(p^{-1} \bmod q)) \bmod q) p + a$ or $x = (((a - b)(q^{-1} \bmod p)) \bmod p) q + b$.

Example ***6.4.*** For the number 19 the pair $(8, 6)$ is the CRT representation modulo $143 = 11 \cdot 13$. Hence 19 is a solution of the system of congruences $\begin{cases} x \equiv 8 (\mathrm{mod} 11); \\ x \equiv 6 (\mathrm{mod} 13). \end{cases}$ We try to restore it by Garner's formulae.

Solution. Compute $13^{-1} (\mathrm{mod}\, 11)$ and $11^{-1} (\mathrm{mod}\, 13)$. Clearly, $13 (\mathrm{mod} 11) = 2$; $2 \cdot 6 = 12 \equiv (\mathrm{mod}\, 11)$, therefore $13^{-1} (\mathrm{mod}\, 11) = 6$. We find $11^{-1} (\mathrm{mod} 13)$ by the extended Euclidian algorithm for $\mathrm{GCD}(11, 13) = 1$: $13 = 11 \cdot 1 + 2$; $11 = 2 \cdot 5 + 1$. From here by down-sweep step we obtain the equality

$$1 = 11 \cdot 1 + 2 \cdot (-5) = 11 \cdot 1 + (13 \cdot 1 + 11 \cdot (-1))(-5) = 13 \cdot (-5) + 11 \cdot 6.$$

Hence $11^{-1} (\mathrm{mod} 13) = 6$. By the first Garner's formula we have $x = ((6 - 8) 6 \bmod 13) 11 + 8 = (-12 (\mathrm{mod}\, 13)) 11 + 8 = 11 + 8 = 19$. By the second Garner's formula we obtain $x = ((8 - 6)\, 6 \bmod 11)\, 13 + 6 = 13 + 6 = 19$.

Surely if one works with the real RSA cryptosystems, then the actual calculations are done by the Chinese Remainder Theorem.

3. Rabin cryptosystem. This cryptosystem was the result of rethinking of the RSA cryptosystem. M.Rabin became interested in the problem of key choice in the RSA cryptosystem where e is always coprime with $\varphi(n)$ and in particular is always odd. And what happens if we take an even e? And if we take the simplest case $e = 2$? As a result of detailed examination unexpectedly appeared the Rabin cryptosystem considered here.

Let p and q be two distinct prime numbers and $N = pq$. We fix a number B, $0 \leq B < N$. The pair $\{N, B\}$ is the public key of the Rabin cryptosystem. A transmitted message c is considered as an element of the ring Z / NZ and is encrypted by the formula: $m = c(c + B)(\mathrm{mod} N)$. Clearly this encryption method is implemented much faster than in the RSA cryptosystem. So, the Rabin cryptotext represents three numbers (N, B, m), where the latter is the ciphertext and the first two are public keys. In fact, the message c is one of the roots of the quadratic equation $x^2 + Bx - m = 0$ in the ring Z/NZ. In this ring 2 is an invertible element. Therefore we can use the standard formula $x = \left(\sqrt{\frac{B^2}{4} + m} - \frac{B}{2}\right) (\operatorname{mod} N)$ to solve the quadratic equation.

The major disadvantage of the Rabin cryptosystem is that there are four roots of every square in the ring Z/NZ.

***Example* 6.5.** Suppose $N = 3 \cdot 7 = 21$. Let take $B = 5$ and let the letter $s = 19$ be the transmitted information. The ciphertext is $m = c(c + B)(\operatorname{mod} N) = 19(19 + 5)(\operatorname{mod} 21) = 15$. An addressee is sent three numbers $(N, B, m) = (21, 5, 15)$.

The addressee computes the discriminant of the quadratic equation: $D = \frac{B^2}{4} + m = 25/4 + 15 \equiv (25 \cdot 16 + 15)(\operatorname{mod} 21) = 16$. This discriminant has the following CRT representation modulo 21: $16 \leftrightarrow (1, 2)$. In $Z/3Z$ there are two square roots of 1: 1 and 2. In $Z/7Z$ there are also two square roots of 2: 3 and 4. Therefore in $Z/21Z$ square roots of 16 have 4 different CRT representations: (1, 3); (1, 4); (2, 3); (2, 4). It means that in $Z/21Z$ there are 4 different roots of 16. Let find them by the first Garner's formula. 3^{-1} (mod 7) = 5. Therefore

$$d_1 = ((3-1)5) \bmod 7)3 + 1 = 10; \qquad d_2 = ((4-1)5) \bmod 7)3 + 1 = 4;$$
$$d_3 = ((3-2)5) \bmod 7)3 + 2 = 17; \qquad d_4 = ((4-2)5) \bmod 7)3 + 2 = 11.$$

In $Z/21Z$ $2^{-1} = 11$. Therefore in $Z/21Z$ the quadratic equation has 4 roots: $x_1 = 4 - 5 \cdot 11 \equiv 12(\operatorname{mod} 21)$; $x_2 = 10 - 55 \equiv 18(\operatorname{mod} 21)$; $x_3 = 11 - 55 \equiv 19(\operatorname{mod} 21)$; $x_4 = 17 - 55 \equiv 4(\operatorname{mod} 21)$. The authors of the problem know which answer is correct, but how to inform the addressee about it is an additional problem for the sender.

4. ElGamal cryptosystem appeared as a reaction on excessive complexity of the RSA cryptosystem. Its security is based on the other problem – the problem of discrete logarithm: to solve the equation $\bar{a}^x = \bar{b}$ in the ring Z/pZ with prime p one need to look sequentially through degrees $\bar{a}$ until the desired residue class $\bar{b}$ is obtained. The problem is to develop the other not enumerative method to determine the degree of x in this equation.

The base of the ElGamal cryptosystem is a large prime number P. For real, not academic cryptosystems it should contain from 150 to 300 decimal digits. It means that P lies in the range from 2^{512} to 2^{1024}. It is known that the residue class ring Z/PZ is a field because all its nonzero residue classes are invertible under multiplication. Moreover it is known that the multiplicative group Z/PZ^* of this field has order $P-1$ and is cyclic. It is also assumed that there is another large prime number $Q \approx 2^{160}$ among divisors of $P-1$. Let g be a generator of this multiplicative group. It is not very easy to find this generator. But this search is a preliminary task.

Developers of the cryptosystem face this problem during cryptosystem's construction. The parameters P and g are public keys of the system.

Any natural number x can be a secret key of the cryptosystem. It is known to both a sender and an addressee. The value $h = g^x (\mathrm{mod}\ P)$ is the third public key of the cryptosystem. Any natural number c interpreted as a nonzero element of the field Z/PZ is an informational message in this cryptosystem. To send a message c or multiple messages during short period of time the sender generates a session key k. The addressee does not know it. To encrypt a message c one need to multiply it by $K = h^k (\mathrm{mod} P)$ in the field Z/PZ. Thus the encrypted message is $m = cK (\mathrm{mod} P)$. The addressee is send a message of two numbers (m, O_{sk}), where $O_{sk} = g^k (\mathrm{mod} P)$ is a public session key.

The addressee knows three public keys (P, g, h). He also knows the secret key x. The addressee computes the value $O_{sk}^x (\mathrm{mod}\ P)$. Note, that $O_{sk}^x (\mathrm{mod}\ P) = g^{kx} (\mathrm{mod}\ P) = h^k (\mathrm{mod}\ P) = K$. It remains to find K^{-1} in the field Z/PZ. This is the same problem as finding d in the RSA cryptosystem. After this the addressee can find the true message by the formula: $c = m \cdot K^{-1} (\mathrm{mod} P)$.

Example 6.6. Let $P = 23$. Direct verification shows that $g = 5$ can be taken as a generator in $Z/23Z^*$. Let $x = 7$. Then

$$h = 5^7 (\mathrm{mod}\ 23) = 5^2 \cdot 5^2 \cdot 5^2 \cdot 5 (\mathrm{mod}\ 23) \equiv 2 \cdot 2 \cdot 2 \cdot 5 (\mathrm{mod}\ 23) =$$
$$= 40 (\mathrm{mod}\ 23) \equiv 17 (\mathrm{mod}\ 23).$$

So, $h = 17$. Let take $k = 3$. Then

$$K = h^k (\mathrm{mod}\ P) = 17^3 (\mathrm{mod}\ 23) \equiv 14 (\mathrm{mod}\ 23).$$

$O_{sk} = g^k (\mathrm{mod}\ P) = 5^3 (\mathrm{mod}\ 23) \equiv 10 (\mathrm{mod}\ 23)$. Let $c = 20$ be a message to encrypt. Then $m = cK (\mathrm{mod} P) = 20 \cdot 14 (\mathrm{mod} 23) \equiv 4 (\mathrm{mod} 23)$. A couple of numbers $(m, O_{sk}) = (4, 10)$ is sent to an addressee. The values $(P, g, h, x) = (23, 5, 17, 7)$ should be known to him in advance. The addressee computes $K = O_{sk}^x (\mathrm{mod}\ P) = 10^7 (\mathrm{mod}\ 23) = 14$. It is easy to see that $K^{-1} (\mathrm{mod}\ 23) = 5$. Then $c = m \cdot K^{-1} (\mathrm{mod} P) = 4 \cdot 5 (\mathrm{mod} 23) = 20$ – the letter «t».

Problems for Classroom

Problem 6.1. Use RSA to encrypt the message $c = 156$.

Solution. Choose $n = 209 = 11 \cdot 19, p = 11, q = 19$ such that $156 < 209$ and GCD(156, 209) = 1. Here $\varphi(209) = \varphi(11) \cdot \varphi(19) = 10 \cdot 18 = 180$. Choose $e = 7$ such that $\mathrm{GCD}(7, 180) = 1$. Then the ciphertext is $m \equiv c^e = 156^7 (\mathrm{mod} 209)$.

$e = 7_{10} = 111_2 = 2^2 + 2 + 1 = 4 + 2 + 1$; $156^7 \equiv 156^4 \cdot 156^2 \cdot 156 (\mathrm{mod}\ 209)$;

$156^2 = 24336 \equiv 92 (\mathrm{mod}\ 209)$; $156^4 \equiv 92^2 = 8464 \equiv 104 (\mathrm{mod}\ 209)$;

$156^7 \equiv 156 \cdot 92 \cdot 104 = 1492608 \equiv 139 (\mathrm{mod}\ 209)$.

The pair $(7, 209)$ is the public key. The message to send is $(n,e,m) = (209, 7, 139)$.

Problem 6.2. Use the Chinese Remainder Theorem to calculate 139^{103} (mod 209).

Solution. It is easy to see that $139 \leftrightarrow (7, 6)$ modulo $209 = 11 \cdot 19$. By Fermat's Little Theorem we have

$$7^{10} \equiv 1\,(\mathrm{mod}\,11);\ 6^{18} \equiv 1\,(\mathrm{mod}\,19).$$

Therefore $7^{103} \equiv 7^3 (\mathrm{mod}\,11) \equiv 2\,(\mathrm{mod}\,11)$. $6^{103} \equiv 6^{13} (\mathrm{mod}\,19) \equiv 4\,(\mathrm{mod}\,19)$. Thus, $139^{103} \leftrightarrow (2, 4)$. $11^{-1} (\mathrm{mod}\,19) = 7$. By Garner's formula we obtain $139^{103} (\mathrm{mod}\,209) = ((4-2)7 \bmod 19)11 + 2 = 156$.

Problem 6.3. Decrypt the RSA cryptotext $(n,e,m) = (209, 7, 139)$.

Solution. 1) we factor $n = 209$: $209 = p \cdot q = 11 \cdot 19$;

2) we compute $\varphi(209) = (p-1)(q-1) = 10 \cdot 18 = 180$;

3) we find the secret key d by the extended Euclidian algorithm:

$$180 = 25 \cdot 7 + 5;\ 7 = 1 \cdot 5 + 2;\ 5 = 2 \cdot 2 + 1.$$

Therefore

$$1 = 5 + (-2) \cdot 2 = 5 + (-2) \cdot (7 - 1 \cdot 5) = 5 + (-2) \cdot 7 + 2 \cdot 5 = (-2) \cdot 7 + 3 \cdot 5 =$$
$$= (-2) \cdot 7 + 3(180 - 25 \cdot 7) = 3 \cdot 180 + (-77) \cdot 7.$$

Hence $\overline{e^{-1}} = \overline{-77} = \overline{180-77} = \overline{103}$. Thus, $d = 103$;

4) we find $m^d (\mathrm{mod}\,n) = c$, i.e., 139^{103} (mod 209). From the solution of problem 6.2 it follows: the sent message is $c = 156$.

Problem 6.4. Use RSA and the Chinese Remainder Theorem to encrypt the message «as».

Solution is not unique. Naturally, we perform the transition from the word to a number as the authors of RSA did: $a \leftrightarrow 01$, $s \leftrightarrow 19$. Therefore $as \leftrightarrow 119$. So the message is $c = 119$. We choose prime numbers p and q so that their product $n = pq$ is greater than $c = 119$ and is coprime to it. Let take $p = 13$ and $q = 19$. Then $n = pq = 247$ satisfies the required conditions. Let take $e = 41$. It is necessary to calculate $m = c^e \bmod(n) = 119^{41} (\mathrm{mod} 247)$. We find the CRT-representation $c = 119 \leftrightarrow (2,5)$. $\varphi(n) = 12 \cdot 18 = 216$. LCM(12,18)=36. Hence by Corollary 4 for every $\overline{a} \in (Z/247Z)^*$ we have $\overline{a}^{36} = \overline{1}$. Therefore $119^{41} = 119^{36+5} = 119^5 (\mathrm{mod} 247)$. Let find the fifth degrees of the CRT representation of c.

$$2^5 \equiv 6 (\mathrm{mod} 13).$$

$$5^5 = 25 \cdot 25 \cdot 5 = 6 \cdot 6 \cdot 5 (\mathrm{mod} 19) = 36 \cdot 5 (\mathrm{mod} 19) = 17 \cdot 5 (\mathrm{mod} 19) = 9 (\mathrm{mod} 19).$$

Thus, $m \leftrightarrow (6,9)$. To restore m we use the following Garner's formulae: $m = (((b-a)(p^{-1} \bmod q)) \bmod q)p + a$. Here $p^{-1} \bmod q = 13^{-1} \bmod 19 = 3 \bmod 19 = 3$. Then $m = (((9-6)3) \bmod 19)13 + 6 = (9 \bmod 19)13 + 6 = 9 \cdot 13 + 2 = 123$. So, by the RSA scheme we have the message $(n,e,m) = (247,41,123)$.

Problem 6.5. Decrypt the message $(n,e,m)=(247,41,123)$ using the Chinese Remainder Theorem.

Solution. The basis of strength of the RSA cryptosystem (the complexity of factorization) for $n=247$ can be easily overcome: $247=13\cdot19$. Then $\varphi(247)=12\cdot18=216=2^3\cdot3^3$ and $\mathrm{GCD}(\varphi(13),\varphi(19))=6$. It is necessary to find $d=e^{-1}=41^{-1}$ in the ring $Z/216Z$. $\varphi(216)=\varphi(2^3)\cdot\varphi(3^3)=4\cdot18=72$ and $\mathrm{LCM}(\varphi(2^3),\varphi(3^3))=36$. Hence for every $a\in(Z/216Z)^*$ we have $\bar{a}^{36}=\bar{1}$, in particular $41^{36}=1$. Therefore in the ring $Z/216Z$ we have $41^{-1}=41^{35}$. Let compute this value.

$$41^2=1681\equiv169(\mathrm{mod}216);\, 41^4\equiv169^2\equiv49(\mathrm{mod}216);$$

$$41^8\equiv49^2\equiv25(\mathrm{mod}216);\, 41^{16}\equiv25^2\equiv193(\mathrm{mod}216);\; 41^{32}\equiv193^2\equiv97(\mathrm{mod}216).$$

Hence $41^{35}=41^{32}\cdot41^2\cdot41\equiv97\cdot169\cdot41(\mathrm{mod}216)\equiv137(\mathrm{mod}216)$. So in the ring $Z/216Z$ we have $41^{-1}=137$.

To decrypt the message we should calculate $c=m^d(\mathrm{mod}n)=123^{137}(\mathrm{mod}247)$. While solving the previous problem we noted that for every $\bar{a}\in(Z/247Z)^*$ the equality $\bar{a}^{36}=\bar{1}$ holds. Therefore $123^{137}=123^{3\cdot36+29}\equiv123^{29}(\mathrm{mod}247)$. Let turn to the CRT representation: $123^{29}\leftrightarrow(6^{29},9^{29})$. By the little Fermat's theorem we have $6^{12}\equiv1(\mathrm{mod}13)$ and $9^{18}\equiv1(\mathrm{mod}19)$. Therefore $6^{29}\equiv6^5(\mathrm{mod}13)\equiv6^2\cdot6^2\cdot6(\mathrm{mod}13)\equiv10\cdot10\cdot6(\mathrm{mod}13)\equiv2(\mathrm{mod}13)$; $9^{29}\equiv9^{11}(\mathrm{mod}19)$. Since $9^2\equiv5(\mathrm{mod}19)$, $9^4\equiv5^2(\mathrm{mod}19)\equiv6(\mathrm{mod}19)$, then $9^{11}=9^{4\cdot2+2+1}\equiv6^2\cdot5\cdot9(\mathrm{mod}19)\equiv17\cdot7(\mathrm{mod}19)\equiv5(\mathrm{mod}19)$.

Thus $c\leftrightarrow(2,5)$. To restore c by its CRT representation we use Garner's formula

$$c=(((a-b)(q^{-1}\bmod p))\bmod p)q+b\,.$$

Here

$$q^{-1}(\mathrm{mod}\,p)=19^{-1}(\mathrm{mod}13)=6^{-1}(\mathrm{mod}13)=11(\mathrm{mod}13).$$

Then $c=(((2-5)11)\mathrm{mod}13)19+5=(-33\mathrm{mod}13)19+5=119$. Consequently the sent message is "as". The problem is completely solved.

Problem 6.6. Use the Rabin cryptosystem to encrypt the message "be".

Solution. Standard transition from the word into digital form proposed by R. Rivest, A. Shamir, and L. Adleman gives the number $c=205$. We choose $N=19\cdot29=551$, $B=43$. Then the encrypted message is

$$m=c(c+B)(\mathrm{mod}N)=205(205+43)(\mathrm{mod}551)=148.$$

Problem 6.7. Find all square roots of 237 in the ring $Z/551Z$.

Solution. The number $237\leftrightarrow(9,5)$ modulo $551=19\cdot29$. In the field $Z/19Z$ there exist two square roots of 9: 3 and 19–3 = 16. To find square roots of 5 in the field $Z/29Z$ we use the enumerative technique. Namely, we look through elements of the set $Z/29Z$ until we find an element $a\in Z/29Z$ such that $a^2\,\mathrm{mod}29\equiv5$. It is easy to see that $11^2\,\mathrm{mod}29\equiv5$. Therefore there exist two square roots of 5: 11 and

$29-11=18$. Hence in the ring $Z/551Z$ one can extract four square roots of 237. Let denote them by d_1, d_2, d_3, d_4. These numbers have the following CRT representations: $d_1=(3,11)$; $d_2=(16,11)$; $d_3=(3,18)$; $d_4=(16,18)$. We can find the roots by the first Garner's formula

$$x=(((b-a)(p^{-1} \bmod q)) \bmod q)p+a.$$

In this case $p^{-1}(\bmod q)=19^{-1}(\bmod 29)$. Let find this value by the extended Euclidian algorithm. $29=19\cdot 1+10$; $19=10\cdot 1+9$; $10=9\cdot 1+1$. Hence $1=10+9\cdot(-1)=10+(-1)\cdot(19+10\cdot(-1))=10\cdot 2+19\cdot(-1)=(29+19\cdot(-1))\cdot 2+19\cdot(-1)=$ $=29\cdot 2+19\cdot(-3)$. From this Bezout's identity it follows that in the ring $Z/29Z$ the equality $19^{-1}=29-3=26$ holds. Now we can easily obtain the desired roots:

$$d_1=((11-3)26(\bmod 29))\cdot 19+3=5\cdot 19+3=98;$$
$$d_2=((11-16)26(\bmod 29))\cdot 19+16=15\cdot 19+16=301;$$
$$d_3=((18-3)26(\bmod 29))\cdot 19+3=15\cdot 19+3=250;$$
$$d_4=((18-16)26(\bmod 29))\cdot 19+16=23\cdot 19+16=453.$$

Problem 6.8. Decrypt a two-letters message from the Rabin cryptotext: $(N,B,m)=(551,43,148)$.

Solution. According to the theory the desired message c is one of the roots of the quadratic equation $x^2+Bx-m=0$ in the ring Z/NZ. In this case we should solve the equation $x^2+43x-148=0$ in the ring $Z/551Z$. It can be rewritten in another form: $x^2+43x+403=0$. The roots of the equation we find by the standard formula: $x=\left(\dfrac{-43+\sqrt{43^2-4\cdot 403}}{2}\right)(\bmod 551)=\left(\dfrac{-43+\sqrt{237}}{2}\right)(\bmod 551)$. Taking into account the results of the previous problem we obtain four variants of the message: $c_1=\dfrac{98-43}{2}=\dfrac{55}{2}=\dfrac{55+551}{2}=303$; $c_2=\dfrac{301-43}{2}=\dfrac{258}{2}=129$; $c_3=\dfrac{250-43}{2}=\dfrac{207}{2}=\dfrac{207+551}{2}=379$; $c_4=\dfrac{453-43}{2}=205$. The first message is “cc”, the second, and the third does not have verbal decryption, and the fourth is decrypted as “be” and is the desired message.

Problem 6.9. Use the ElGamal cryptosystem to encrypt the message “be”.

Solution. $c=205$. Choose $P=509$. Then we can take $g=2$. Let $x=400$. Then $h=g^x(\bmod P)=2^{400}(\bmod 509)=2^{256+128+16}(\bmod 509)$; here

$$2^4=16;\ 2^8=256;\ 2^{16}=256^2\equiv 384(\bmod 509);$$
$$2^{32}\equiv 384^2(\bmod 509)\equiv 355;\ 2^{64}\equiv 355^2(\bmod 509)\equiv 302;$$
$$2^{128}\equiv 302^2(\bmod 509)\equiv 93; 2^{256}\equiv 93^2(\bmod 509)\equiv 505.$$

Hence $h=2^{400}(\bmod 509)=505\cdot 93\cdot 384(\bmod 509)=181$. Let $k=279$. Then

$$K=h^k(\bmod P)=181^{279}(\bmod 509)=181^{256+26+4+2+1}(\bmod 509)$$

Here

$$181^2 \equiv 185(\bmod 509);\ 181^4 \equiv 185^2(\bmod 509) \equiv 122;$$
$$181^8 \equiv 122^2(\bmod 509) \equiv 123;\ 181^{16} \equiv 123^2(\bmod 509) = 368;$$
$$181^{32} \equiv 356^2(\bmod 509) \equiv 30;\ 181^{64} \equiv 30^2(\bmod 509) \equiv 391;$$
$$181^{128} \equiv 391^2(\bmod 509) \equiv 181;\ 181^{256} \equiv 181^2(\bmod 509) \equiv 185.$$

Hence,

$$K = 181^{256+16+4+2+1}(\bmod 509) = 185 \cdot 368 \cdot 122 \cdot 185 \cdot 181(\bmod 509) \equiv 429.$$

At last we obtain the encrypted message:

$$m = cK(\bmod P) = 205 \cdot 429(\bmod 509) \equiv 397.$$

In addition to the encrypted message one compute the public session key $O_{sk} = g^k(\bmod P) = 2^{279}(\bmod 509) = 2^{256+16+4+2+1}(\bmod 509)$. Taking into account the above calculations we have $O_{sk} = 375$. Thus, an addressee is sent the message:

$$(P, g, h, m, O_{sk}) = (509, 2, 181, 397, 375).$$

Problem 6.10. Decrypt the ElGamal cryptotext $(P, g, h, m, O_{sk}) = (509, 2, 181, 397, 375)$ if the addressee knows the secret key $x = 400$.

Solution. The addressee computes $K = O_{sk}^x(\bmod P) = 375^{400}(\bmod 509) = 429$. Then using the extended Euclidian algorithm he calculates $K^{-1}(\bmod P) = 429^{-1}(\bmod 509) = 439$. Then

$$c = m \cdot K^{-1}(\bmod P) = 397 \cdot 439(\bmod 509) = 205 - \text{the word “be”}.$$

Problem 6.11. In the role of an unauthorized user not knowing the secret key x try to «hack» – decrypt – the message $(P, g, h, m, O_{sk}) = (509, 2, 340, 233, 375)$.

Solution. We construct a fragment of the cyclic group

$$< g > = < 2 > = \{2, 2^2 = 4, ...\}$$

until we obtain the equality $2^x = 340$ and find x. Then we repeat the calculations carried out in the solution of the previous problem.

Self Instructional Problems for Laboratory Study № 6 «Modern Cryptosystems»

1 – 2. Decrypt an RSA cryptotext (m, e, n).

3 – 4. Decrypt a Rabin cryptotext (n, B, m).

5 – 6. Decrypt an ElGamal cryptotext (P, g, h, x, m, O_{sk}).

Variant 1.

1. (899,3,101671). 2. (102020525,1,102030101).
3. (150419,15,90244). 4. (205916939,666,39843864).
5. (47,11,19,13,42,18). 6. (17,6,14,7,13,3).

Variant 2.

1. (201505,1,202451). 2. (1015081425,1,1015123177).

3. (155357,1001,9700). 4. (319372663,1024866,234853376).
5. (19,10,7,12,5,17). 6. (37,13,25,14,34,24).

Variant 3.

1. (10305,1,10349). 2. (205121225,1,205278781).
3. (101617,49,24873). 4. (1614612973, 260740, 455160832).
5. (43,18,40,8,19,13). 6. (29,8,23,16,3,15).

Variant 4.

1. (40169,3,82933). 2. (112090305,1,112100657).
3. (72329,252,23494). 4. (201043727,987654,40098000).
5. (61,10,58,12,38,22). 6. (59,6,40,7,26,51).

Variant 5.

1. (17243,3,20737). 2. (205011419,1,205145103).
3. (51959,26,27841). 4. (1003621907,1485,149729920).
5. (47,5,10,19,43,43). 6. (67,11,58,3,20,56).

Variant 6.

1. (90305,1,91709). 2. (116161205,1,116259959).
3. (200623,573,145601). 4. (719026801,322180, 521161600).
5. (67,12,33,4,61,39). 6. (11,8,3,6,10,6).

Variant 7.

1. (1650,3,12091). 2. (201040705,1,201043727).
3. (91709,398,36789). 4. (1828776151, 14789255, 876149760).
5. (17,6,8,6,8,15). 6. (17,10,5,7,6,12).

Variant 8.

1. (71515,1,72329). 2. (318050113,1,319372663).
3. (183641,26,91364). 4. (1106091083,5678,524381440).
5. (17,5,12,9,9,3). 6. (17,7,2,10,14,8).

Variant 9

1. (161523,1,162521). 2. (308051919,1,308880049).
3. (111101,448,73728). 4. (827010683,643345, 369698560).
5. (23,19,11,5,22,15). 6. (23,18,1,11,18,13).

Variant 10.

1. (121523,1,123463). 2. (1801140705,1, 1828776151).
3. (101671,800,6187). 4. (722603899,621040, 491328320).
5. (43,18,4,12,5,16). 6. (67,11,12,13,62,25).

Variant 11.

1. (100123,1,101617). 2. (1601160518,1, 1614612973).
3. (162521,1000,160525). 4. (1527869719, 376660, 1146343936).
5. (61,26,24,9,15,8). 6. (53,21,35,7,37,29).

Variant 12.

1. (39665,3,101671). 2. (1524090405,1, 1527869719).
3. (12091,50,157). 4. (116259959,157861,92205230).
5. (47,30,28,10,40,42). 6. (47,45,16,4,5,17).

Variant 13.

1. (200501,1,200623). 2. (718152312,1, 719026801).
3. (152051,128,5721). 4. (9643325473, 35665346, 4092805818).
5. (47,41,26,5,16,4). 6. (43,33,37,7,2,20).

Variant 14.

1. (110525,1,111101). 2. (815140525,1, 827010683).
3. (123463,333,31005). 4. (308880049,2924785,220730336).
5. (43,33,2,9,23,27). 6. (31,17,26,5,12,24).

Variant 15.

1. (152312,1,155357). 1. (718081404,1, 722603899).
3. (182731,48976,243087488). 4. (1671731863,52746,1364142592).
5. (31,24,23,9,4,15). 6. (31,24,4,6,3,16).

Laboratory Study № 7 «Ideals of Rings»

Necessary Theoretical Data

Definition 7.1. A ring is a nonempty set K equipped with two binary operations called addition $(+)$ and multiplication $(\cdot)$; K is required to be an abelian group under addition; multiplication and addition are linked by the distributive laws:

$$(a+b)\cdot c = a\cdot c + b\cdot c; \quad a\cdot(b+c) = a\cdot b + a\cdot c$$

for all $a, b, c \in K$.

The rings are distinguished by number of elements (finite or infinite) and properties of multiplication (associative and nonassociative, commutative and noncommutative, with a unity and without unity, with zero divisors and without divisors of zero, etc.).

Definition 7.2. A subring of a ring K is a subgroup of the additive group $(K,+)$ that is the ring itself, i.e., it is closed under multiplication in the ring K.

Definition 7.3. A subring J of a ring K is said to be a left ideal of K if for all $k \in K$ and for every $j \in J$ it holds $jk \in J$, i.e., $Jk \subseteq J$. If $kJ \subseteq J$ for all elements

$k \in K$ then J is called a right ideal. An ideal that is both left and right is said to be a two-sided ideal.

In any ring K the sets $\{0\}$ and K are formally the ideals of K. They are called *improper* ideals unlike the rest *proper* ideals.

Theorem 7.1. *For every element a of a ring K the sets $aK = \{ak \mid k \in K\}$ and $Ka = \{ka \mid k \in K\}$ are respectively a left and a right ideals of K.*

Definition 7.4. The left and the right ideals from Theorem 7.1 are called, respectively, a left principal ideal $<a>$ and a right principal ideal $<a>$ of a ring K, i.e., left and right principal ideals are subrings of a ring K, that consist of all elements $ak, k \in K$ or $ka, k \in K$ accordingly.

Theorem 7.2. *In the ring of integers, Z, every ideal J is principal.*

In every ring $\{0\}$ is a principal ideal.

Definition 7.5. An ideal M (left, right, two-sided) of a ring K is called maximal if there exists no other proper ideal J such that $M \subset J$.

Theorem 7.3. *In the ring of integers an ideal $J = <p>$ is maximal iff p is a prime number.*

Definition 7.5. A polynomial $f \in P[x]$ is said to be irreducible over P if f has positive degree and $f(x) = bc$ with $b, c \in P$ implies either b or c is a constant polynomial.

Theorem 7.4. *In the ring of polynomials $P[x]$ with coefficients in a field P every ideal J is principal. The ideal $J = <m(x)>$ generated by a polynomial $m(x)$ is maximal ıff $m(x)$ is irreducible over P.*

Problems for Classroom

Problem 7.1. Give the definition of a ring.

Problem 7.2. Give ten examples of rings.

Problem 7.3. Do there exist finite noncommutative rings?

Problem 7.4. Do there exist rings without 1?

Problem 7.5. Give examples of subrings in Z. Are your subrings ideals? Does the set I of integers with the remainder of 1 when divided by 5 form an ideal in the ring Z?

Solution. Suppose $f \in I, g \in I$. Since f and g give remainder of 1 when divided by 5 then $f + g$ give the remainder of 2 when divided by 5. Hence $f + g \notin I$. Therefore I is not closed under addition. Thus, I is not a subring and moreover is not an ideal.

Problem 7.6. The same questions for the polynomial ring. Does the set I of polynomials with even free terms form an ideal in the ring $Z[x]$ of polynomials with integer coefficients?

Solution. Determine whether I is a subring.

Suppose $f(x) \in I, g(x) \in I$. Then

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,\ g(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0,$$