MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
SUMY STATE UNIVERSITY

"ELEMENTARY NUMBER THEORY"

lecture notes with tests

for students of specialties
"Informatics" and "Applied Mathematics"

Sumy
Sumy State University
2016

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
SUMY STATE UNIVERSITY

"ELEMENTARY NUMBER THEORY"
lecture notes with tests

for students of specialties
"Informatics" and "Applied Mathematics"

Approved at meeting of
Department of Applied and Computational Mathematics
as the abstract of lecture notes
for the discipline ”Elementary number theory”
Record № 10 from 19.05.2015

Sumy
Sumy State University
2016

“Elementary Number Theory" lecture notes with tests / Yu.V. Shramko, E.I. Ogloblina. – Sumy : Sumy State University, 2016. – 72 p.

Department of Applied and Computational Mathematics

CONTENT

P.

1. DIVISIBILITY 4

Problems for Unit 1 8

2. PRIME NUMBERS 9

3. DIVISION 10

Problems for Unit 3 15

4. GREATEST COMMON DIVISOR (GCD) 16

5. THE EUCLIDEAN ALGORITHM 18

6. LOWEST (LEAST) COMMON MULTIPLE (LCM) 21

Problems for Unit 6 22

7. CONTINUED FRACTIONS 24

Problems for Unit 7 31

8. ARITHMETIC FUNCTIONS 32

Problems for Unit 8 37

9. MODULAR ARITHMETIC 39

9.1. CLASSES OF CONGRUENCE 39
9.2. PROPERTIES OF CONGRUENCES THAT CHANGE MODULUS 47
9.3. FERMAT'S LITTLE THEOREM AND EULER'S THEOREM ON THE EXISTENCE OF THE UNIT ELEMENT MODULO m 48
Problems for Unit 9 53

10. LINEAR CONGRUENCES WITH ONE UNKNOWN 54

10.1. CONGRUENCES OF THE FIRST ORDER. SOLVING CONGRUENCES .. 54
10.1.1. Application of Congruence's Properties 55
10.1.2. Application of Convergents 57
10.2. MULTIPLICATIVE INVERSE 59
10.3. SYSTEM OF LINEAR CONGRUENCES WITH ONE UNKNOWN 61
Problems for Unit 10 66

REFERENCES 71

1. DIVISIBILITY

In this course all numbers are integers unless otherwise specified. Thus, in the following definition d, n, and k are integers.

Definition 1.1

The number d divides the number n if there exists k such that $n=d\cdot k$.

Alternate terms are:

d is a divisor of n,

d is a factor of n,

n is a multiple of d.

This relationship between d and n is symbolized as $d \mid n$. The symbol $d \nmid n$ means that d does not divide n. The integer k is called the **quotient** from division n by d.

Note that the symbol $d \mid n$ is different from the fraction symbol d/n. It is also different from n/d because $d \mid n$ is either true or false, while n/d is a rational number.

All factors of n that are unequal 1 or n are called **proper (nontrivial) factors**; 1 and n are called **trivial** factors of integer n**.**

Theorem 1.1: Divisibility Properties

For any n, m, d, and c the following properties hold:

1. $\forall d \mid 0$.
2. if $0 \mid n \Rightarrow n = 0$.
3. $1 \mid n$.
4. *(Reflexivity property)* $n \mid n$.
5. $n \mid 1 \Rightarrow n = 1$ or $n = -1$.
6. *(Transitivity property)* $d \mid n$ and $n \mid m \Rightarrow d \mid m$.
7. *(Multiplication property)* $d \mid n \Rightarrow$ for any $a \in Z$: $d \mid a\cdot n$.
8. *(Linearity property)* $d \mid n$ and $d \mid m \Rightarrow d \mid a\cdot n + b\cdot m$ for all a and b.
9. *(Comparison property)* If d and n are positive and $d \mid n$, then $d \leq n$.
10. *(Integration property)* If $d \mid a$, $d \mid b$ and $a = b + c \Rightarrow d \mid c$.

Definition 1.1

If n is divisible by 2, then we say that it is **even** (or has **even parity**). Otherwise, a number is **odd** (or has **odd parity**).

Lemma 1.1

Recall that $|a|$ equals a if $a > 0$ and equals $-a$ if $a < 0$.

1. If $d \mid a$, then $-d \mid a$ and $d \mid -a$.
2. If $d \mid a$, then $d \mid |a|$.
3. The largest positive integer that divides a nonzero number a is $|a|$.

Examples

Example 1.1

Let x and y be integers. Prove that $2x + 3y$ is divisible by 17 if and only if (iff) $9x + 5y$ is divisible by 17.

Solution

Suppose that $17 \mid (2x + 3y)$. Then, according to *multiplication property* in theorem 1.1, we get $17 \mid [13(2x + 3y)]$ or
$17 \mid (26x + 39y)$.

Further, we decompose the right side into sum as follows:
$17 \mid (17x + 34y + 9x + 5y) \Rightarrow 17 \mid 17 \cdot (x + 2y) + (9x + 5y)$.

Finally, according to i*ntegration property* in theorem 1.1, we have $17 \mid (9x + 5y)$.

And conversely, producing the similar set of operations, we obtain
$17 \mid (9x + 5y) \Rightarrow 17 \mid [4(9x + 5y)]$,
or $17 \mid (36x + 20y) \Rightarrow 17 \mid (34x + 17y + 2x + 3y) \Rightarrow$
$17 \mid 17(2x + y) + 2x + 3y$.

Thus we have proved that $17 \mid 2x + 3y$.

Example 1.2

Prove that for any integer m, p, q, n such that $(m-p)|(mn+pq)$ is an integer, $(m-p)|(mq+np)$ is also the integer.

Solution

Let $(m-p)\,|\,(mq+np)$ be an integer. We can denote this in similar way: $\frac{mn+pq}{m-p}=t_1\in Z$.

It is necessary to prove that $\frac{mq+np}{m-p}=t_2\in Z$ or $t_1-t_2\in Z$. Let us show this. We obviously obtain:

$$\frac{mn+pq}{m-p}-\frac{mq+np}{m-p}=\frac{m(n-q)-p(n-q)}{m-p}=\frac{(m-p)(n-q)}{m-p}=n-q\in Z.$$

Therefore $t_1-t_2\in Z$ and, finally, $\frac{mq+np}{m-q}=t_2\in Z$.

Example 1.3

N is a five-digit number $N=\overline{a_4a_3a_2a_1a_0}$, $0\le a_i\le 9$. It is known that the number *N* is divisible by 41.

Prove if we shift digits of the number in a circular manner, then we will get new numbers divisible by 41 too.

Solution

$N=10^4a_4+10^3a_3+10^2a_2+10a_1+a_0$.

Let us shift the last digit a_0 to the first position, as follows: $N_1=10^4a_0+10^3a_4+10^2a_3+10a_2+a_1$. It is the new number. Prove that it is multiple of 41.

Let us try to separate the number *N* out from the right side of the expression for N_1. Multiplying by 10, we get

$10N_1=10^5a_0+10^4a_4+10^3a_3+10^2a_2+10a_1$.

Then add and subtract a_0. It yields: $10N_1=10^5a_0+10^4a_4+10^3a_3+10^2a_2+10a_1+a_0-a_0$.

By combining the first and last terms of expression, we obtain the number *N* as a summand: $10N_1=a_0(10^5-1)+N=99999a_0+N$.

Further, taking into account that

$41 \mid N, \quad 99999 = 9 \cdot 11111, \ \frac{11111}{41} = 271 \Rightarrow 41 \mid 99999,$

we come to conclusion that in the right side both terms are multiples of 41. Thus $41 \mid 10N_1 \Rightarrow 41 \mid N_1$

Example 1.4

Prove that $30 \mid \left(m^5 - m\right)$.

Solution

First, let us factorize 30:

$30 = 5 \cdot 6 = 5 \cdot 3!$.

Hence it is necessary to prove that $\left(m^5 - m\right)$ will be the multiple of 5 and $3!$, simultaneously.

Secondly, we introduce the number of combinations for *n* by *k*.

$C_n^{\ k} = \frac{n(n-1)(n-2)\cdot \ldots \cdot (n-k+1)}{k!} \in Z$.

It follows that the product of *k* consecutive integers divided by $k!$ is an integer.

Therefore, we need to represent $\left(m^5 - m\right)$ via the product of 5 consecutive integers, for such product is divisible by 5!=30*4. All the more, considering term will be divisible by 30. Also, we can show that $\left(m^5 - m\right)$ is the product of 3 consecutive integers and factor 5.

Thus we have for the first case:

$$\left(m^5 - m\right) = m\left(m^4 - 1\right) = m\left(m^2 - 1\right)\left(m^2 + 1\right) =$$

$$= (m-1)m(m+1)\left(m^2 - 4 + 5\right) = (m-1)m(m+1)\left(m^2 - 4\right) +$$

$$+5(m-1)m(m+1) = (m-2)(m-1)m(m+1)(\mathrm{m}+2) + 5(m-1)m(m+1).$$

$$\frac{(m-2)(m-1)m(m+1)(m+2)}{5!} \in Z \Rightarrow 30 \mid (m-2)(m-1)m(m+1)(m+2)$$

And finally, for the second case, we obtain

$$\frac{(m-1)m(m+1)}{3!}=\frac{(m-1)m(m+1)}{6}\in \mathrm{Z}\Rightarrow$$

$$\Rightarrow 6|(m-1)m(m+1)\Rightarrow 30\,|\,5(m-1)m(m+1).$$

This completes the proof.

PROBLEMS FOR UNIT 1

Problem 1.1

Find all positive integers d such that d divides both $n^2 + 1$ and $(n + 1)^2 + 1$ for some integer n.

Problem 1.2

N is a six-digit number. $N=\overline{a_5a_4a_3a_2a_1a_0}$, $0\le a_i\le 9$, $a_0=5$. If we rearrange last digit a_0=5 to the first place, we will get $N_1=4N$. Find this number N.

Problem 1.3

Prove that

1. $6\,|\,n(n+1)(2n+1)$.
2. $30\,|\,mn(m^4-n^4)$.

Problem 1.4

Prove that

$2^n\,|\,(n+1)(n+2)\cdot\ldots\cdot(n+n)$

Problem 1.5

Prove that the last digit of number $N=2^{2^n}+1$ is 7.

2. PRIME NUMBERS

Definition 2.1

An integer $p \geq 2$ is prime if it has only trivial divisors. An integer greater than or equal to 2 that is not prime is **composite.**

Note that 1 is neither prime nor composite.

Lemma 2.1

An integer $n \geq 2$ is composite iff it has factors a and b such that $1 < a < n$ and $1 < b < n$.

Lemma 2.2

If $n > 1$**,** then there is a prime p such that $p \mid n$.

Definition 2.2

Let p be a prime. If you know that $p^{\alpha} \mid a$ and $p^{\alpha+1} \nmid a$, then α is the highest power of occurrence of the prime p to an integer a.

Theorem 2.1: The Fundamental Theorem of Arithmetic

Every integer a greater than 1 can be written uniquely in the following form:

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_k^{\alpha_k},$$

where p_i are distinct primes and α_i are positive integers – the highest power of occurrence of prime p_i to an integer a.

Theorem 2.2: Euclid's Theorem

There are infinitely many primes.

Proof.

Suppose there exist only a finite number of primes, say $p_1, p_2, \ldots, p_n$.

Let $N = p_1 p_2 \cdot \cdot p_n + 1$. By the fundamental theorem of arithmetic, N is divisible by some prime p. That prime must be one of $p_1, \ldots, p_n$ since that list is assumed to be exhaustive. But it is seen that N is not divisible by any of the p_i. This is a contradiction; it

follows that the assumption that there are only finitely many primes is not true.

We shall use the following notations:

The set of divisors of an integer $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_k^{\alpha_k}$ is $D = \{ p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_3^{\beta_3} \cdot \ldots \cdot p_k^{\beta_k}, 0 \le \beta_i \le \alpha_i, i = \overline{1,k} \}$.

The number of divisors of an integer $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_k^{\alpha_k}$ equals

$$\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \cdot \ldots \cdot (\alpha_k + 1).$$

Theorem 2.3

If $a > 1$ is composite, then a has the least prime divisor $p \le \sqrt{n}$

Example 2.1

Consider the number 97. Note that $\sqrt{97} < \sqrt{100} = 10$. The primes less than 10 are 2, 3, 5, and 7. None of them divides 97, and so 97 is prime.

Useful Facts

Bertrand's Postulate. For every positive integer n, there exists prime p such that

$$n \le p \le 2n.$$

3. DIVISION

Let a, b be any integers. Without loss of generality by Lemma 1.1, we can assume that $a > 0$, $b > 0$.

Theorem 3.1

The pair of integers a, b $(a > b)$ can be uniquely submitted with pair of integers q, r, satisfying these two conditions:

1. $a = b \cdot q + r$.

2. $0 \le r < b$.

The integer r is called the **remainder** in division of a by b. If $r = 0$, then q is called the **quotient**, other wise it is called the **partial quotient**.

Corollary 3.1

The number *d* divides the number *n* iff in division of *n* by *d* the remainder is *r = 0.*

Criteria for number divisibility

Criteria for number divisibility are important in factorization of large integers.

To obtain criteria for divisibility, we will apply the method of remainders. Any non-negative integer can be represented in decimal form as follows:

$$N = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^3 a_3 + 10^2 a_2 + 10a_1 + a_0 .$$

We don't know digits $a_n, a_{n-1}, ..., a_3, a_2, a_1, a_0$, but we can analyze remainders of the division of 10^i (i=0,1,…, n) by some numbers.

1. Criteria for divisibility of *N* by 2^k

– Divisibility by 2

Obviously, the number $10^n a_n + 10^{n-1} a_{n-1} + \ldots + 10a_1$ is divisible by 2. **If a_0 is divisible by 2, then *N* will be divisible by 2.**

– Divisibility by $4=2^2$

Since the number $10^n a_n + 10^{n-1} a_{n-1} + \ldots + 10^2 a_2$ is divisible by 4, then ***N* will be divisible by 4 if $10a_1 + a_0$ is divided by 4.**

– Divisibility by $8=2^3$

Number $10^n a_n + 10^{n-1} a_{n-1} + \ldots + 10^3 a_3$ is divisible by 8. So, **if $10^2 a_2 + 10a_1 + a_0$ is divisible by 8, then *N* will be divisible by 8, and so on.**

– Generalization for 2^k

If the last *k* digits of the number *N* are divisible by 2^k, then *N* will be divisible by 2^k.

2. Criteria for divisibility of *N* by 3 and 9

We can rewrite number *N* as follows:

$$N = \underbrace{\underbrace{999...9}_{n} a_n + \underbrace{999...9}_{n-1} a_{n-1} + ... + 99a_2 + 9a_1}_{N_1} + a_n + a_{n-1} + ... + a_1 + a_0 =$$

$$= N_1 + \sum_{i=1}^{n} a_i .$$

It is evident that $9|N_1$, $3|N_1$

So, **if the sum of digits of the number *N* is divisible by 3 or 9, then *N* is divisible by 3 or 9.**

3. Criteria for divisibility of *N* by 5^k

$$N = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^3 a_3 + 10^2 a_2 + 10a_1 + a_0 .$$

If the number composed of the *k* last digits of the number *N* is divisible by 5^k, then *N* is divisible by 5^k. The proof is the same as for divisibility of *N* by 2^k

4. Criteria for divisibility of *N* by 7

$$N = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^3 a_3 + 10^2 a_2 + 10a_1 + a_0 .$$

Consider remainders of division of ten's powers by 7. We have

10: 10=1·7+3, the remainder is 3

10^2: 100=14·7+2, the remainder is 2

10^3: 1000=142·7+6=**143·7 - 1**, the remainder is 6 or **-1**

10^4: 10000=1428·7+4, the remainder is 4

10^5: 100000=14285·7+5, the remainder is 5

10^6: 1000000=142857·7+1, the remainder is **1**

We have obtained all type of division remainders by seven. If we continue process of division, then we will get the remainders from **considered above set.** Now we can formulate criterion for divisibility by 7.

a. Criteria for three-digit numbers

$N = 100a_2 + 10a_1 + a_0 = 98a_2 + 2a_2 + 7a_1 + 3a_1 + a_0 = 98a_2 + 7a_1 + 2a_2 + 3a_1 + a_0 = 7(14a_2 + a_1) + 2a_2 + 3a_1 + a_0$.

If $2a_2 + 3a_1 + a_0$ is divisible by 7, then *N* is divisible by 7 too.

Example 3.1

Check whether numbers 581 and 163 are divisible by 7 or not.

Solution

5·2 + 8·3 + 1 = 35. It is divisible by 7, so 581 is divisible by 7 too.

1) 1·2 + 6·3 + 3 = 23. It isn't divisible by seven. Since 23 has the remainder 2, then 163 has the same remainder.

b. Criteria for *n*-digit numbers

Note that 10^3 has the remainder -1 and 10^6 has the remainder 1.

Represent the considering number via the sum of three-digit numbers:

$$N = a_2a_1a_0 + 10^3 a_5a_4a_3 + 10^6 a_8a_7a_6 + ... =$$

$$= a_2a_1a_0 + 143\cdot 7a_5a_4a_3 - a_5a_4a_3 + 142857\cdot 7a_8a_7a_6 + a_8a_7a_6 + ... =$$

$$\underbrace{143\cdot 7a_5a_4a_3 + 142857\cdot 7a_8a_7a_6 + ...}_{N_1 \vdots 7} + \underbrace{a_2a_1a_0 - a_5a_4a_3 + a_8a_7a_6 - ...}_{N_2}$$

$$N = \overline{a_n ... \underbrace{a_8a_7a_6}_{+}\ \underbrace{a_5a_4a_3}_{-}\ \underbrace{a_2a_1a_0}_{+}}, \quad N_2 = a_2a_1a_0 - a_5a_4a_3 + a_8a_7a_6 - ...$$

If N_2 is divisible by 7, then N is divisible by 7 too.

Example 3.2

Check if the number N=23 161 320 is divisible by 7.

Solution

N_2=320 – 161 + 23 = 182. 182:7=26. So, N=23 161 320 is divided by 7. We have 23 161 320:7 = 3 308 760.

5. Criteria for divisibility of *N* by 11

$$N = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^3 a_3 + 10^2 a_2 + 10a_1 + a_0 .$$

Consider the remainders of the division of ten's powers by 11.

10: 10=0·11+10 = **1·11 – 1**, the remainder is 10 or **-1**

10^2: 100=9·11+1, the remainder is **1**

10^3: 1000=90·11+10=**91·11 - 1**, the remainder is 10 or **-1**

10^4: 10000=901·11+1, the remainder is **1**

$$N = \overline{a_n ... a_5\ a_4\ a_3\ a_2\ a_1\ a_0}, \qquad N_2 = a_0 - a_1 + a_2 - a_3 + ...$$

$$+\ -\ +\ -\ +$$

If N_2 is divisible by 11, then N will be divisible by 11 too.

Example 3.3

Check if the numbers N=23 161 320 and N=1 186 680 are divisible by 11.

Solution

1) N_2= 0 – 2 + 3 – 1 + 6 – 1 + 3 – 2 = 6. It isn't divisible by 11. So, N=23 161 320 isn't divisible too.

2) N_2= 0 – 8 + 6 – 6 + 8 – 1 + 1 = 0. It is divisible by 11, therefore N=1 186 680 is divisible by 11 too.

6. Criteria for divisibility of *N* by 13

Criterion for divisibility by 13 matches the criterion of divisibility by 7.

Example 3.4

Check that N = 3 040 232 is divisible by 13.

Solution

232 – 40 + 3 = 195. 195:13=15. Then 3 040 232 is divisible by 13.

7. Criteria for divisibility of *N* by *d* = 10*k* + 1 (31, 41, 61,…)

$$N = \overline{\underbrace{a_n \ldots a_3 a_2 a_1}_{A} a_0} = 10A + a_0 .$$

Multiply N by k: $kN = 10kA + ka_0 + A - A = A(10k+1) - (A - ka_0)$.

Since k isn't divisible by $10k + 1$, we see that ***N* will be divisible by 10*k* + 1 if $N_2 = A - ka_0$ is a multiple of $10k + 1$.**

This criterion can be applied until the divisibility or lack of it become apparent.

8. Criteria for divisibility of *N* by *d* = 10*k* – 1 (19, 29, 59,…)

$$N = \overline{\underbrace{a_n \ldots a_3 a_2 a_1}_{A} a_0} = 10A + a_0 .$$

Multiply N by k:

$$kN = 10kA + ka_0 + A - A = A(10k-1) + (A + ka_0).$$

Since k isn't divisible by $10k - 1$, it follows that ***N* will be divisible by 10*k* – 1 if $N_2 = A + ka_0$ is a multiple of $10k + 1$.**

This criterion can be applied until the divisibility or lack of it become apparent.

Example 3.5

Check that N = 3 040 232 is divisible by 31.

Solution

Here, the divisor is 31, then it is necessary to use the eighth criteria. We get

31 = 10·3+1, k = 3, A=304 023, a_0 = 2.

If $N_2 = A - 3a_0$ is divisible by 31, then N is divisible by 31:

1. N_2 =304 023 – 3·2 = 304 017.

2. A = 30 401, a_0 = 7, 30 401 – 3·7 = 30 380.

3. A=3 038, a_0 = 0, 3 038 – 3·0 = 3 038.

4. A=303, a_0 = 8, 303 – 3·8 = 279.

5. A=17, a_0 = 9, 27 – 3·9 = 0.

It is clear that 0 is divisible by 31, so N = 3 040 232 is divisible by 31 too. 3 040 232:31 = 98072.

PROBLEMS FOR UNIT 3

3.1. Check that a is divisible by m

***m*=35**		***m*=39**		***m*=55**	
1.	a=351645	6.	a =437931	11.	a =747615
2.	a=236215	7.	a =294177	12.	a =502205
3.	a =590835	8.	a =735813	13.	a =1256145
4.	a =236810	9.	a =294918	14.	a =503470
5.	a =564655	10.	a =703209	15.	a =1200485
***m*=31**		***m*=91**		***m*=29**	
16.	a =238173	21.	a =1559649	26.	a =394197
17.	a =159991	22.	a =1047683	27.	a =264799
18.	a =400179	23.	a =2620527	28.	a =662331
19.	a =160394	24.	a =1050322	29.	a =265466
20.	a =382447	25.	a =2504411	30.	a =632983

4. GREATEST COMMON DIVISOR (GCD)

Without loss of generality (see Lemma 1.1), we can assume that all factors of integers are positive.

Definition 4.1

An integer is a common divisor of n others if it divides all of them.

We denote the set of numbers that are common divisors of $a_1, a_2, \ldots, a_n$ by $C(a_1, a_2, \ldots, a_n)$.

Example 4.1

1. The set of common divisors of 18 and 30 is

$C(18, 30) = \{-1, 1, -2, 2, -3, 3, -6, 6\}$.

2. The set of common divisors of 10, 30, 100 and 130 is

$C(10, 30, 100, 130) = \{-1, 1, -2, 2, -5, 5, -10, 10\}$.

Definition 4.2

The greatest common divisor of n nonzero integers $a_1, a_2, \ldots, a_n$ is the largest integer from the set $C(a_1, a_2, \ldots, a_n)$, except that $\gcd(0, 0) = 0$.

Denotation of the greatest common divisor for integers $a_1, a_2, \ldots, a_n$ is

$$\gcd(a_1, \ldots, a_n).$$

Example 4.2

For results obtained in Example 4.1, we have

1. $\gcd(18, 30)$ is the largest integer from the set $C(18, 30) = \{-1, 1, -2, 2, -3, 3, -6, 6\}$. Then $\gcd(18, 30) = 6$.

2. $\gcd(10, 30, 100, 130)$ is the largest integer from the set $C(10, 30, 100, 130) = \{-1, 1, -2, 2, -5, 5, -10, 10\}$. Then $\gcd(10, 30, 100, 130) = 10$.

Definition 4.3

If $\gcd(a_1, a_2, \ldots, a_n) = 1$, then integers $a_1, a_2, \ldots, a_n$ are called **coprime** numbers **(relative primes).**

Definition 4.4

If **the greatest common divisors of all pairs** $(a_i, a_j)\,(i, j = 1, 2, ..., n)$ from integers a_1, a_2, …, a_n are equal 1, then a_1, a_2, …, a_n are called pairwise prime numbers**. Pairwise prime numbers** are **coprime numbers, but not conversely.**

Example 4.3

Numbers (5, 15, 21, 31) are **coprime numbers,** because gcd (5, 15, 21, 31) = 1. But gcd (5,15) = 5 ≠ 1, gcd (15,21) = 3 ≠ 1.

Gcd (3, 7, 11, 13) =1, then numbers (3, 7, 11, 13) are **coprime,** and gcd (3,7) =1, gcd (3,11) =1, gcd (3,13) =1, gcd (7,11) =1, gcd (7,13) = 1, gcd (11,13) =1. Thus, the numbers are **pairwise prime numbers.**

Lemma 4.1

$$\gcd(a, b) = \gcd(b, a).$$

Lemma 4.2

$$\gcd(a, b) = \gcd(|a|, |b|).$$

Lemma 4.3

If $a \neq 0$ or $b \neq 0$, then gcd(a, b) exists and satisfies condition

$$0 < \gcd(a, b) \leq \min\{|a|, |b|\}.$$

Example 4.4

It follows from considered lemmas that gcd(48, 732) = = gcd(−48, 732) = gcd(−48,−732) = gcd(48,−732). We also know that 0 < gcd(48, 732) ≤ 48. If d = gcd(48, 732), then $d \mid 48$. To find d, we just need to check all positive divisors of 48 that also divide 732.

If two numbers have the greatest common divisor equal 1, then they have only trivial common factors.

Lemma 4.4

If g = gcd(a, b), then gcd(a/g, b/g) = 1.

Examples 4.5

g = gcd(15,21) = 3, gcd(15/3, 21/3) = gcd(5,7) = 1.

Lemma 4.5 (Bezout's Lemma)

The greatest common divisor of two numbers is a linear combination of those two: for all integers a and b there exist integers s and t such that

$$\gcd(a, b) = sa + tb.$$

5. THE EUCLIDEAN ALGORITHM

We can efficiently compute the greatest common divisor of two numbers.

First we simplify the problem. Since $\gcd(a, b) = \gcd(|a|, |b|)$ (and $\gcd(0, 0) = 0$), we just need to obtain a method for computing the $\gcd(a, b)$ of nonnegative a and b. And, since $\gcd(a, b) = \gcd(b, a)$, we will consider the case $a > b > 0$.

Lemma 5.1

If $a > 0$, then $\gcd(a, 0) = a$.

Lemma 5.2

If $a > 0$, then $\gcd(a, a) = a$.

Lemma 5.3

Let $a > b > 0$. If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

Proof.

If we show that the two sets of common divisors $C(a, b)$ and $C(b, r)$ are equal, then this will suffice to prove the whole lemma, because there will be the same greatest element in both sets. Recall, the sets are equal iff they possess the same elements. Let us prove the last statement.

First, suppose that there exist $d \in C(a, b)$ such that $d \mid a$ and $d \mid b$. Let us note that $r = a - bq$.·Therefore, according to Theorem 1.1(10), we make a conclusion that $d \mid r$. Thus, $d \mid b$ and $d \mid r$, and so d belongs to $C(b, r)$.

We have shown that any element of $C(a, b)$ is an element of $C(b, r)$, so it implies

$C(a, b) \subseteq C(b, r)$.

On the other hand, let us assume that there exist $d \in C(b, r)$ such that $d \mid b$ and $d \mid r$. Since $a = bq + r$, we again apply Theorem 1.1 (10) to show that $d \mid a$. So $d \mid a$ and $d \mid b$, and, therefore, $d \in C(a, b)$. That is, then $d \in C(a, b)$.

QED

The Euclidean algorithm uses Lemma 5.3 to compute the greatest common divisor of two numbers. Let us consider the algorithm.

Choose $a, b \in Z$ such that $a > b$. Construct a chain of a division with the remainders as follows:

Step 1: $a = b \cdot q_0 + r_1$, $0 < r_1 < b$, $\gcd(a, b) = \gcd(b, r_1)$;

Step 2: $b = r_1 \cdot q_1 + r_2$, $0 < r_2 < r_1$, $\gcd(b, r_1) = \gcd(r_1, r_2) \Rightarrow$
$\Rightarrow \gcd(a, b) = \gcd(r_1, r_2)$;

Step 3: $r_1 = r_2 \cdot q_2 + r_3$, $0 < r_3 < r_2$, $\gcd(r_1, r_2) = \gcd(r_2, r_3) \Rightarrow$
$\Rightarrow \gcd(a, b) = \gcd(r_2, r_3)$

……

Step n: $r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n$, $0 < r_n < r_{n-1}$, $\gcd(r_{n-2}, r_{n-1}) =$
$= \gcd(r_{n-1}, r_n) \Rightarrow \gcd(a, b) = \gcd(r_{n-1}, r_n)$;

Step n+1: $r_{n-1} = r_n \cdot q_n$

Since there is no remainder in the last division, we get $\gcd(r_{n-1}, r_n) =$
$= r_n \Rightarrow$ **$\gcd(a, b) = r_n$.**

One can say that for any numbers ***a*** and ***b*** **the last nonzero remainder** in a chain of division with the remainders **is gsd(*a*, *b*).**

Example 5.1

Compute gcd(803, 154), $a = 803$, $b = 154$

Step 1: gcd(803, 154) = gcd(154, 33), since $803 = 154 \cdot 5 + 33$, $a = bq_0 + r_1$, $q_0 = 5$, $r_1 = 33$, $0 < 33 < 154$.

Step 2: gcd(154, 33) = gcd(33, 22), since $154 = 33 \cdot 4 + 22$, $b = r_1 q_1 + r_2$, $q_1 = 4$, $r_2 = 22$, $0 < 22 < 33$.

Step 3: gcd(33, 22) = gcd(22, 11) since $33 = 22 \cdot 1 + 11$, $r_1 = r_2 q_2 + r_3$, $q_2 = 1$, $r_3 = 11$, $0 < 11 < 22$.

Step 4: gcd(22, 11) = 11 since $22 = 11 \cdot 2$, $r_2 = r_3 q_3$, $q_3 = 2$, $r_4 = 0$.

Hence, gcd(803, 154) = gcd(22, 11) = 11.

Recall that Bezout's lemma asserts that for given a and b, there exist two numbers s and t such that gcd(a, b) = $s \cdot a + t \cdot b$. We can use Euclidean algorithm to find s and t by tracing the steps of division in reverse order.

Example 5.2

Express gcd(803, 154) as a linear combination of 803 and 154. We will use the considered above Example 5.1.

From step 3: $11 = 33 - 22 \cdot 1$;

From step 2: $22 = b - 33 \cdot 4$, or $11 = 33 - (b - 33 \cdot 4)\, 1 = = - b \cdot 1 + 33 \cdot 5$;

From step 1: $33 = a - b \cdot 5$, or $11 = - b \cdot 1 + (a - b \cdot 5) \cdot 5 = =- 26 \cdot b + a \cdot 5$.

Hence, we can express gcd(803, 154) = 11 as a linear combination of 803 and 154 as follows below:

$11 = 803 \cdot 5 + (-26) \cdot 154, s = 5, t = -26$ or $g = a \cdot 5 + b \cdot (-26)$.

Lemma 5.4 (Generalization)

Let

$$a_0 = cq_0 + r_0, \quad a_1 = cq_1 + r_1, ..., \; a_n = cq_n + r_n \Rightarrow$$

$$\Rightarrow \gcd(a_0, a_1, ..., a_n, c) = \gcd(c, r_0, r_1, ..., r_n).$$

Example 5.3

Compute gcd(261, 135, 48).

Step 1: Divide a_0 =261 and a_1 =135 by c= 48. We get: $261 = 48 \cdot 5 + + 21$, r_{10}=21; $135 = 48 \cdot 2 + 39$, $r_{11} = 39$.

Step 2: Find gcd(48, 39, 21). Divide c = 48 and r_{11}= 39 by r_{10} = 21. We obtain $48 = 21 \cdot 2 + 6$, $r_{20} = 6$, $39 = 21 \cdot 1 + 18$, $r_{21} = 18$

Step 3: Find gcd(21, 18, 6). Divide r_{10} = 21 and r_{21}= 18 by r_{20} = 6. It yields: $21 = 6 \cdot 3 + 3$, $r_{30} = 3$, $18 = 6 \cdot 3 + 0$, $r_{21} = 0$. Zero is divided by any numbers. Gcd(18,6) = 6.

Step 4: Find gcd(6, 3): gcd(6, 3) = 3.

Hence, gcd(261, 135, 48) = 3.

6. LOWEST (LEAST) COMMON MULTIPLE (LCM)

Definition 6.1

An integer is a common multiple of n others if it is divided by all of them.

We denote by $\boldsymbol{M(a_1, a_2, \ldots, a_n)}$ the set of numbers that are common multiples of $\boldsymbol{a_1, a_2, \ldots, a_n}$. The set M is infinite.

Definition 6.2

The lowest common multiple of n nonzero integers $a_1, a_2, \ldots, a_n$ is the least integer from the set $M(a_1, a_2, \ldots, a_n)$.

Designation of the lowest common multiple for integers $a_1, a_2, \ldots, a_n$ is $\mathbf{lcm(a_1, \ldots, a_n)}$.

Lemma 6.1

$$Lcm(a,b) = \frac{a \cdot b}{gcd(a,b)}.$$

Proof

Let $d = gcd(a, b)$, then $a = a_1 \cdot d$, and $b = b_1 \cdot d$, $gcd(a_1, b_1) = 1$ (according to lemma 4.4). M denotes any common multiple of a and b. Then $M = k \cdot a$. The number M/b is an integer, because M is multiple of b. We will get after the series of transformations

$$\frac{M}{b} = \frac{ka}{b} = \frac{ka_1 d}{b_1 d} = \frac{ka_1}{b_1}.$$

Since $gcd(a_1, b_1) = 1$, we see that k is divisible by b_1 and $k = b_1 \cdot t$, $t \in Z$.

$$\frac{M}{b} = \frac{ka_1}{b_1} = \frac{b_1 t a_1}{b_1} = ta_1,\ M = a_1 \cdot b \cdot t = \frac{a_1 \cdot b \cdot d}{d} t = \frac{a \cdot b}{d} t,\ t \in Z.$$

Hence, we can express the set of common multiples of $\boldsymbol{a}$ and $\boldsymbol{b}$ by the formula

$$M = \frac{a \cdot b}{gcd(a,b)} \cdot t,\ \ t \in Z.$$

If $t = 1$, then we obtain the lowest common multiple of a and b as follows:

$$Lcm(a,b) = \frac{a \cdot b}{gcd(a,b)}.$$ **QED.**

PROBLEMS FOR UNIT 6

6.1. Compute $gcd(a,b)$ with Euclidean algorithm and $lcm(a,b)$ with Lemma 6.1

1. a = 1232, b = 1672	2. a = 1 329, b = 2 136	3. a = 1 359, b = 8 211
4. a = 5 427, b = 32 877	5. a = 5 894, b = 3 437	6. a =12 606, b = 6494
7. a =29 719, b = 76 501	8. a =162 891, b = 32 176	9. a =469 459, b = 579 203
10. a =738 089, b = 3 082 607	11. a =179 370 199, b = 4 345 121	12. a =3 327 449, b = 6 314 153
13. a =12 870, b = 7 650	14. a =41 382, b = 103 818	15. a =3 640, b = 14 300
16. a =24 700, b = 33 250	17. a =7 650, b = 25 245	18. a =56 595, b = 82 467
19. a =35 574, b = 192 423	20. a =25 245, b = 129 591	21. a =10 140, b = 92 274
22. a =36 372, b = 147 220	23. a =46 550, b = 37 730	24. a =1 403, b = 1 058
25. a =213 239, b = 512 525	26. a =138 285, b = 356 405	27. a =72 348, b = 5 632
28. a =354 295, b = 543 440	29. a =24 789, b = 35 286	30. a =32 893, b = 72 568

6.2. Compute gcd(a, b, c) with Lemma 5.4

1. a = 529, b = 1541, c = 1817	2. a = 67 283, b = 122 433, c = 221 703
3. a = 549 493, b =863 489, c = 133 125	4. a = 738089, b = 3082607, c = 28 303 937
5. a = 1767, b =2223, c = 11 913	6. a = 476, b = 1258, c = 21 114
7. a = 3445, b =4225, c = 5915	8. a = 572, b = 5746, c = 1118
9. a = 19 074, b =13 566, c = 8211	10. a = 1073, b = 3683, c = 34 481
11. a = 1012, b = 1474, c = 4598	12. a = 988, b = 2014, c = 42 598
13. a = 2585, b = 7975, c = 13 915	14. a = 874, b = 1518, c = 20 142
15. a = 2227, b = 9911, c = 952	16. a = 1253, b = 252, c = 406
17. a = 2743, b = 3587, c = 6963	18. a = 4345, b = 6523, c = 10967
19. a = 7683, b = 5161, c = 12 909	20. a = 5174, b = 12 337, c = 13 403
21. a = 10 047, b = 6749, c = 16 881	22. a = 6766, b = 16 133, c = 17 527
23. a = 11 229, b = 7543, c = 18 867	24. a = 7562, b = 18 031, c = 19 589
25. a = 13 593, b = 9131, c = 22 839	26. a = 9154, b = 21 827, c = 23 713
27. a = 17 139, b = 11 513, c = 28 797	28. a = 11 542, b = 27 521, c = 29 899
29. a = 18 321, b = 12 307, c = 30 783	30. a = 12 338, b = 29 419, c = 31 961

7. CONTINUED FRACTIONS

Theorem 7.1. General Form

A continued fraction is an expression of the form

$$\alpha = q_1 + \cfrac{b_1}{q_2 + \cfrac{b_2}{q_3 + \ldots.}} \\ \vdots \\ \ldots\ldots + \cfrac{b_{s-2}}{q_{s-1} + \cfrac{1}{\alpha_s}}$$

where α, q_i and b_i are either rational numbers, real numbers, or complex numbers.

If $b_i = 1$ for all i, then the expression is called a simple continued fraction. If the expression contains **finitely many terms**, then it is called a **finite continued fraction**; otherwise, it is called an **infinite continued fraction**. The numbers $\boldsymbol{q_i}$ are called the **partial quotients.**

Theorem 7.2

The continued fraction expression of a real number is finite iff the real number is rational.

Every rational number $\frac{a}{b}$ can be represented by the **simple continued fraction** as follows:

$$\frac{a}{b} = q_1 + \frac{r_1}{b} = q_1 + \frac{1}{\frac{b}{r_1}} = q_1 + \frac{1}{q_2 + \frac{r_2}{r_1}} = q_1 + \frac{1}{q_2 + \frac{1}{\frac{r_1}{r_2}}} =$$

$$= q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{r_3}{r_2}}} = \ldots = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ldots \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}.$$

We can obtain all q_i and r_i by Euclidean algorithm. The continued fraction has as many terms, as many steps are in this algorithm.

Simple continued fractions $\frac{a}{b}$, $\gcd(a,b)=1$ can be written in a compact form using a **chain of partial quotients:**

$$\frac{a}{b} = [q_1, q_2, \ldots, q_n].$$

Example 7.1

Represent rational number $Q = \frac{151}{13}$ by a continued fraction.

Solution

Gcd(151,13) = 1.

$$Q = \frac{151}{13} = 11 + \frac{8}{13} = 11 + \cfrac{1}{\cfrac{13}{8}} = 11 + \cfrac{1}{1 + \cfrac{5}{8}} = 11 + \cfrac{1}{1 + \cfrac{1}{\cfrac{8}{5}}} =$$

$$= 11 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{3}{5}}} = 11 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\cfrac{5}{3}}}} =$$

$$= 11 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{2}{3}}}} = 11 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{3}{2}}}} = 11 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2}}}}.$$

The chain of partial quotients is $\frac{151}{13} = [11, 1, 1, 1, 1, 2]$.

Rational numbers obtained from only a limited number of terms in a continued fraction are called **convergents**. For example, in the simple continued fraction

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ldots \\ q_{n-1} + \cfrac{1}{q_n}}}}$$

the convergents are

$$\delta_1 = q_1; \quad \delta_2 = q_1 + \frac{1}{q_2}; \quad \delta_3 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}}; \ldots;$$

$$\delta_n = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ldots \\ \vdots \\ \ldots\ldots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}} = \frac{a}{b}.$$

A sequence of convergents is approximation of a rational number.

Convergent properties

Property 7.1

An approximated rational number lies between two neighboring convergents closer to the right.

The method of the convergent computation

Let us denote the i[th] convergent by $\delta_i = \frac{P_i}{Q_i}$. Then, $\delta_1 = q_1 = \frac{q_1}{1} = \frac{P_1}{Q_1}$,

and $\delta_2 = q_1 + \frac{1}{q_2} = \frac{q_1 q_2 + 1}{q_2} = \frac{q_1 q_2 + 1}{1 \cdot q_2 + 0} = \frac{P_2}{Q_2}$.

We assign $P_0 = 1,\ Q_0 = 0$. Then $\delta_2 = \frac{q_1 q_2 + 1}{1 \cdot q_2 + 0} = \frac{P_2}{Q_2} = \frac{P_1 q_2 + P_0}{Q_1 q_2 + Q_0}$,

For convergent δ_3, we have

$$\delta_3 = \frac{P_1\left(q_2 + \frac{1}{q_3}\right) + P_0}{Q_1\left(q_2 + \frac{1}{q_3}\right) + Q_0} = \frac{q_3(P_1 q_2 + P_0) + P_1}{q_3(Q_1 q_2 + Q_0) + Q_1} = \frac{q_3 P_2 + P_1}{q_3 Q_2 + Q_1} = \frac{P_3}{Q_3}.$$

For any convergent δ_i we get $\delta_i = \frac{q_i P_{i-1} + P_{i-2}}{q_i Q_{i-1} + Q_{i-2}} = \frac{P_i}{Q_i}$.

Thus we have deduced the recursion formula for calculation of the i[th] convergent.

The results of convergent computations can be placed into the table.

Table 7.1 – The results of convergent computations

i	**0**	**1**	**2**	....
q_i		q_1	q_2	....
P_i	1	$P_1 = q_1$	$P_2 = q_2P_1 + P_0$	....
Q_i	0	$Q_1 = 1$	$Q_2 = q_2Q_1 + Q_0$	....

j	**...**	***n***
q_j	....	q_n
$P_j = q_jP_{j-1} + P_{j-2}$	....	$a = P_n = q_nP_{n-1} + P_{n-2}$
$Q_j = q_jQ_{j-1} + Q_{j-2}$	....	$b = Q_n = q_nQ_{n-1} + Q_{n-2}$

Property 7.2

For any $i > 0$, the following formula takes place: $P_iQ_{i-1} - Q_iP_{i-1} = (-1)^i$.

Property 7.3

For any $i > 1$, the following formula takes place: $\delta_i - \delta_{i-1} = \dfrac{(-1)^i}{Q_iQ_{i-1}}$.

Property 7.2 is used for solving the Diophantine equation $ax + by = 1$**.**

We write down property 7.2 for the last two columns of the table 7.1:

$P_nQ_{n-1} - Q_nP_{n-1} = (-1)^n$, $P_n = a$, $Q_n = b$, then $aQ_{n-1} - bP_{n-1} = (-1)^n$.

1. If *n* is even, then $aQ_{n-1} - bP_{n-1} = 1$, $a \cdot Q_{n-1} + b \cdot (-P_{n-1}) = 1$.

We have got a solution to the Diophantine equation: $x = Q_{n-1}$, $y = -P_{n-1}$.

2. If *n* is odd, then $aQ_{n-1} - bP_{n-1} = -1$, *or* $-a \cdot Q_{n-1} + b \cdot P_{n-1} = 1$.

Therefore, we have obtained a solution to the Diophantine equation: $x = -Q_{n-1}$, $y = P_{n-1}$.

Example 7.1

Compute all convergents for the number $\frac{151}{13}$ and solve the Diophantine equation $151x+13y=1$.

Solution

We will use Example 7.1. Number $Q=\frac{151}{13}$ can be written as the chain of partial quotients: $\frac{151}{13}=[11, 1, 1, 1, 1, 2]$. Construct the table.

$$P_0=1,\ Q_o=0,\ P_1=q_1=11,\ Q_1=1,\ \delta_1=\frac{P_1}{Q_1}=\frac{11}{1}=11,$$

$$P_2=q_2P_1+P_0=1\cdot 11+1=12,\ Q_2=q_2Q_1+Q_0=1\cdot 1+0=1,$$

$$\delta_2=\frac{P_2}{Q_2}=\frac{12}{1}=12,$$

$$P_3=q_3P_2+P_1=1\cdot 12+11=23,\ Q_3=q_3Q_2+Q_1=1\cdot 1+1=2,$$

$$\delta_3=\frac{P_3}{Q_3}=\frac{23}{2}=11.5,$$

$$P_4=q_4P_3+P_2=1\cdot 23+12=35,\ Q_4=q_4Q_3+Q_2=1\cdot 2+1=3,$$

$$\delta_4=\frac{P_4}{Q_4}=\frac{35}{3}\approx 11.667,$$

$$P_5=q_5P_4+P_3=1\cdot 35+23=58,\ Q_5=q_5Q_4+Q_3=1\cdot 3+2=5,$$

$$\delta_5=\frac{P_5}{Q_5}=\frac{58}{5}=11.6,$$

$$P_6=q_6P_5+P_4=2\cdot 58+35=151,\ Q_6=q_6Q_5+Q_4=2\cdot 5+3=13,$$

$$\delta_6=\frac{P_6}{Q_6}=\frac{151}{13}\approx 11.615=\frac{a}{b}.$$

i	0	1	2	3	4	5	6
q_i		11	1	1	1	1	2
P_i	1	11	12	23	35	58	151
Q_i	0	1	1	2	3	5	13

Verify property 7.1

Number $\frac{151}{13} \approx 11.615$ is between $\delta_1 = 11$ and $\delta_2 = 12$ closer to $\delta_2 = 12$, because $|11.615 - 11| = 0.615 > |11.615 - 12| = 0.385$.

Number $\frac{151}{13} \approx 11.615$ is between $\delta_2 = 12$ and $\delta_3 = 11.5$ closer to $\delta_3 = 11.5$, because $|11.615 - 12| = 0.385 > |11.615 - 11.5| = 0.115$.

Number $\frac{151}{13} \approx 11.615$ is between $\delta_3 = 11.5$ and $\delta_4 = 11.667$ closer to $\delta_4 = 11.667$, because $|11.615 - 11.5| = 0.115 > |11.615 - 11.667| = 0.052$.

Number $\frac{151}{13} \approx 11.615$ is between $\delta_4 = 11.667$ and $\delta_5 = 11.6$ closer to $\delta_5 = 11.6$, because $|11.615 - 11.667| = 0.052 > |11.615 - 11.6| = 0.015$.

Number $\frac{151}{13} \approx 11.615$ is between $\delta_4 = 11.667$ and $\delta_5 = 11.6$ closer to $\delta_5 = 11.6$, because $|11.615 - 11.667| = 0.052 > |11.615 - 11.6| = 0.015$.

Number $\frac{151}{13} \approx 11.615$ is equal to the last convergent $\delta_6 = \frac{153}{13}$.

Now, we can solve the Diophantine equation $151x + 13y = 1$ using property 7.2.

$P_6 Q_5 - Q_6 P_5 = (-1)^6$ or $a \cdot 5 - b \cdot 58 = 1$ or $a \cdot 5 + b \cdot (-58) = 1$.

The solution to equation is $x = 5,\ \ y = -58$.

PROBLEMS FOR UNIT 7

7.1. The rational number $\frac{a}{b}$ is represented via the chain of partial quotients. Compute all convergents for the number $\frac{a}{b}$, find a and b from the table of convergents and solve a Diophantine equation $ax + by = 1$.

1. $\frac{a}{b} = [2,1,3,4,1,2]$	2. $\frac{a}{b} = [2,1,1,6,8]$	3. $\frac{a}{b} = [0,3,1,2,7,1]$
4. $\frac{a}{b} = [1,1,2,4,5]$	5. $\frac{a}{b} = [0,3,4,3,2,3]$	6. $\frac{a}{b} = [3,1,1,1,5]$
7. $\frac{a}{b} = [2,1,3,4,2,9]$	8. $\frac{a}{b} = [13,1,4,2,5]$	9. $\frac{a}{b} = [0,4,1,3,2,5]$
10. $\frac{a}{b} = [22,3,1,4,7]$	11. $\frac{a}{b} = [2,1,30,2,3]$	12. $\frac{a}{b} = [1,24,3,4,5]$
13. $\frac{a}{b} = [1,25,1,2,3,1,1]$	14. $\frac{a}{b} = [11,2,3,5,1,1]$	15. $\frac{a}{b} = [31,5,2,3,1,5]$
16. $\frac{a}{b} = [1,25,1,2,3,1,1]$	17. $\frac{a}{b} = [1,13,1,2,5,1,1]$	18. $\frac{a}{b} = [2,8,1,2,3,1,2]$
19. $\frac{a}{b} = [2,7,2,1,1,1,4]$	20. $\frac{a}{b} = [3,7,2,5,1,1,2]$	21. $\frac{a}{b} = [2,41,2,3,1]$
22. $\frac{a}{b} = [2,17,1,5,1]$	23. $\frac{a}{b} = [3,19,1,1,3]$	24. $\frac{a}{b} = [2,1,1,3,5,1,1]$
25. $\frac{a}{b} = [2,11,3,19,1,1,3]$	26. $\frac{a}{b} = [5,9,3,11,1,1,2]$	27. $\frac{a}{b} = [21,1,37,1,1,3]$
28. $\frac{a}{b} = [2,23,1,2,3,1,2]$	29. $\frac{a}{b} = [3,29,1,1,2,2]$	30. $\frac{a}{b} = [1,47,1,1,2,1,2]$

8. ARITHMETIC FUNCTIONS

In this section we shall consider several important arithmetic functions.

8.1. The floor function (The integer part function)

Every real number ***x*** can be written uniquely as $x = n + \alpha$, where $n \in Z$ and $0 \le \alpha < 1$. We call *n* the **integer part** or the **floor of *x*** and denote it by [*x*] or $\lfloor x \rfloor$; and α is called the **fractional part of *x*** and is denoted by {*x*}. Thus, for $x \in R$, [*x*] is the greatest integer not exceeding *x*.

The fractional part of ***x*** is commonly thought of as the part after the decimal point, but this notion is correct only for positive ***x***. We define the **fractional part** by

$$\{x\} = x - [x] \text{ for } x \in R.$$

Example 8.1

Find integer and fractional parts for numbers 123.45; 0.83; -0.01; -10.56.

Solution

1. [123.45] = 123; {123.45} = 123.45 – [123.45] = 123.45 – – 123 = 0.45.
2. [0.83] = 0; {0.83} = 0.83 - [0.83] = 0.83 – 0 = 0.83.
3. [–0.01] = –1; {–0.01} = –0.01 – [–0.01] = –0.01 – (–1) = 0.9.
4. [–10.56] = –11; {–10.56} = –10.56 – [–10.56] = –10.56 – – (–11) = 0.44.

An integer part function is used for prime factorization of n! We can find the highest power of prime *p* occurring in the prime decomposition of an integer *a* by this function.

Example 8.2

Find the exponent of the highest power of prime 2 in the prime decomposition of the integer 13!

Solution

13! = 1·2·3·4·5·6·7·8·9·10·11·12·13.

From this product write down the set of numbers that will be multiples of 2. Denote this set by S_2:

$S_2 = \{2, 4, 6, 8, 10, 12\}$;

The number of members of S_2 (the cardinality $|S_2|$ of S_2) is 6. This operation corresponds to the computation of the integer part of the number $\left[\frac{13}{2}\right] = 6$.

From S_2 write down the set of numbers that will be multiples of 2^2. Denote this set by S_4:

$S_4 = \{4, 8, 12\}$. The cardinality of S_4 equals $\left[\frac{13}{2^2}\right] = 3$.

From S_4 write down the set of numbers that will be multiples of 2^3. Denote this set by S_8:

$S_8 = \{8\}$. The cardinality $|S_8|$ is $\left[\frac{13}{2^3}\right] = 1$.

From S_8 write down the set of numbers that will be multiples of 2^4. Denote this set by S_{16}:

$S_{16} = \{\varnothing\}$; $|S_{16}| = \left[\frac{13}{2^4}\right] = 0$.

The total power of prime 2 in prime factorization of 13! is

$$6 + 3 + 1 = 10.$$

The integer 2^{10} is the factor of 13!, and 2^{11} does not divide it.

Hence, **the exponent of the highest power of a prime p occurring in the prime decomposition of an integer n! is given by**

$$\alpha = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^k}\right], \quad p^k \le n, \; p^{k+1} > n.$$

Example 8.3

The number of positive divisors of an integer n – $\tau(n)$, the sum of positive divisors of an integer n – $\sigma(n)$, the Euler's totient function – $\phi(n)$.

If the prime factorization of n > 1 is $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, then **the number of positive divisors (factors)** of this number is

$$\tau(n) = \tau\left(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}\right) = (\alpha_1 + 1)(\alpha_2 + 1) \cdot \ldots \cdot (\alpha_k + 1), \qquad (8.4.1)$$

if $n = p^{\alpha}$, then $\tau(n) = \tau\left(p^{\alpha}\right) = (\alpha + 1)$;

and **the sum of positive divisors (factors)** of this number is

$$\sigma\left(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}\right) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}, \qquad (8.4.2)$$

if $n = p^{\alpha}$, then $\sigma(n) = \sigma\left(p^{\alpha}\right) = \frac{p^{\alpha+1} - 1}{p - 1}$.

Example 8.4

Compute the number and the sum of factors for the integer 18.

Solution

The prime factorization of 18 is $18 = 2 \cdot 3^2$. The integer 18 has positive divisors: 1, 2, 3, 6, 9, 18. The number of these divisors is 6, $\tau(18) = 6$.

In the prime factorization of 18 the prime number 2 has power 1 and the prime number 3 has power 2. We can compute $\tau(18)$ using formula (8.41):

$$\tau(18) = \tau\left(2 \cdot 3^2\right) = (1+1)(2+1) = 2 \cdot 3 = 6.$$

Both results coincide.

The sum of factors is $\sigma(18) = 1 + 2 + 3 + 6 + 9 + 18 = 39$.

By formula (8.4.2), we get

$$\sigma(18)=\sigma\left(2\cdot 3^2\right)=\frac{2^2-1}{2-1}\cdot\frac{3^3-1}{3-1}=3\cdot\frac{(3-1)\left(3^2+3+1\right)}{(3-1)}=3\cdot 13=39^{1}.$$

Both results are correct.

Definition 8.1

The Euler's totient function (phi-function) for an integer n counts the number of positive integers less than n and relatively prime to it.

Designation of the Euler's totient function for an integer n is $\phi(n)$.

Example 8.5

The integer 7 has six positive numbers less than 7 and relatively prime to it: 1, 2, 3, 4, 5, 6. The integer 2 has one such number – 1. The integer 6 has two such numbers – 1 and 5.

8.2. Computation of a value of Euler's function

If the number p is prime, then

$$\phi(p)=p-1; \qquad (8.7.1)$$

If $n=p^{\alpha}$, then

$$\phi\left(p^{\alpha}\right)=p^{\alpha}-p^{\alpha-1}=p^{\alpha-1}(p-1)=p^{\alpha}\left(1-\frac{1}{p}\right); \qquad (8.7.2)$$

If $n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}$, then

$$\phi(n)=\phi\left(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}\right)=\phi\left(p_1^{\alpha_1}\right)\phi\left(p_2^{\alpha_2}\right)\cdot\ldots\cdot\phi\left(p_k^{\alpha_k}\right)=$$
$$=\left(p_1^{\alpha_1}-p_1^{\alpha_1-1}\right)\left(p_2^{\alpha_2}-p_2^{\alpha_2-1}\right)\cdot\ldots\cdot\left(p_k^{\alpha_k}-p_k^{\alpha_k-1}\right)=$$
$$=p_1^{\alpha_1-1}p_2^{\alpha_2-1}\cdot\ldots\cdot p_k^{\alpha_k-1}(p_1-1)(p_2-1)\cdot\ldots\cdot(p_k-1)=$$
$$=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right). \qquad (8.7.3)$$

---

[1] $\left(a^{2k+1}-1\right)=(a-1)\left(a^{2k}+a^{2k-1}+\ldots+a+1\right),\ k\geq 1$

Example 8.6

Compute phi-function for integers 13, 25, 10, 100, 1000.

Solutions

1) 13 is prime, therefore from formula (8.7.1)

$\phi(13) = 13 - 1 = 12$;

2) $25 = 5^2$, then from formula (8.7.2)

$\phi(25) = \phi(5^2) = 5^2 - 5 = 5(5-1) = 20$;

3) $10 = 2 \cdot 5$, then from formula (8.7.3)

$\phi(10) = \phi(2 \cdot 5) = \phi(2)\phi(5) = (2-1)(5-1) = 4$, they are 1, 3, 7, 9;

4) $100 = 2^2 \cdot 5^2$, then from formula (8.7.3)

$$\phi(100) = \phi\left(2^2 \cdot 5^2\right) = \phi\left(2^2\right)\phi\left(5^2\right) = \left(2^2 - 2\right)\left(5^2 - 5\right) =$$

$$= 2 \cdot 5 \cdot (2-1)(5-1) = 10 \cdot 4 = 40;$$

5) $1000 = 2^3 \cdot 5^3$, then from formula (8.7.3)

$$\phi(1000) = \phi\left(2^3 \cdot 5^3\right) = \phi\left(2^3\right)\phi\left(5^3\right) = \left(2^3 - 2^2\right)\left(5^3 - 5^2\right) =$$

$$= 2^2 \cdot 5^2 \cdot (2-1)(5-1) = 100 \cdot 4 = 400.$$

Definition 8.2

$\tau(1)$, $\sigma(1)$, and $\phi(1)$ are defined to be 1.

Definition 8.3

We say that function *f* is multiplicative if $f(m \times n) = f(m) \times f(n)$ for all relatively prime positive integers *m*, and *n*, when *f*(1) = 1.

Theorem 8.1

Functions $\tau(n)$, $\sigma(n)$, and $\phi(n)$ are multiplicative.

PROBLEMS FOR UNIT 8

8.1

a. Find the exponents of the highest powers of primes *a* and *b*, occurring in the prime factorization of an integer *n*!

1. $a=3,\ b=5,$ $N=337!$!	6. $a=2,\ b=13,$ $N=271!$	11. $a=2,\ b=11,$ $N=745!$
2. $a=2,\ b=7,$ $N=234!$	7. $a=5,\ b=13,$ $N=234!$	12. $a=5,\ b=11,$ $N=652!$
3. $a=2,\ b=11,$ $N=381!$	8. $a=3,\ b=5,$ $N=931!$	13. $a=7,\ b=11,$ $N=734!$
4. $a=3,\ b=11,$ $N=534!$	9. $a=2,\ b=7,$ $N=491!$	14. $a=3,\ b=7,$ $N=439!$
5. $a=5,\ b=7,$ $N=625!$	10. $a=3,\ b=11,$ $N=834!$	

b Calculate how many zeros the factorial of *a* number *n*! ends with (the number of trailing zeros)

15. $N=356!$	21. $N=534!$	27. $N=399!$
16. $N=428!$	22. $N=749!$	28. $N=923!$
17. $N=295!$	23. $N=957!$	29. $N=847!$
18. $N=345!$	24. $N=367!$	30. $N=537!$
19. $N=650!$	25. $N=841!$	
20. $N=728!$	26. $N=791!$	

8.2

Compute $\tau(n)$, $\sigma(n)$, and $\phi(n)$ for an integer *n*. The prime factorization of *n* > 1 is $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$

1. $a = 2^8 \cdot 3^3 \cdot 13 \cdot 17$	2. $a = 3^5 \cdot 5^3 \cdot 11 \cdot 13$	3. $a = 3^7 \cdot 7^3 \cdot 17 \cdot 19$
4. $a = 5^4 \cdot 7^2 \cdot 19$	5. $a = 2^9 \cdot 3^7 \cdot 5^2 \cdot 29$	6. $a = 2^6 \cdot 3^5 \cdot 5 \cdot 17$
7. $a = 2^3 \cdot 3^4 \cdot 5^3 \cdot 31$	8. $a = 3^5 \cdot 7^2 \cdot 37 \cdot 41$	9. $a = 5^2 \cdot 7^3 \cdot 29$
10. $a = 2^3 \cdot 3^7 \cdot 7^2 \cdot 59$	11. $a = 5^5 \cdot 7^2 \cdot 13 \cdot 43$	12. $a = 3^3 \cdot 7^6 \cdot 17 \cdot 23$
13. $a = 2^5 \cdot 5^2 \cdot 31 \cdot 43$	14. $a = 2^8 \cdot 7^2 \cdot 23 \cdot 53$	15. $a = 3^8 \cdot 11^2 \cdot 19 \cdot 23$
16. $a = 5^4 \cdot 7^3 \cdot 19 \cdot 41$	17. $a = 2^5 5^2 \cdot 7 \cdot 61$	18. $a = 2^6 \cdot 7^2 \cdot 11^2 \cdot 37$
19. $a = 3^2 \cdot 5^2 \cdot 11^2 \cdot 23$	20. $a = 3^5 \cdot 7^2 \cdot 11^2 \cdot 79$	21. $a = 3^7 \cdot 5^2 \cdot 7 \cdot 71$
22. $a = 2^6 \cdot 3^4 \cdot 5^3 \cdot 41$	23. $a = 2^6 \cdot 3^4 \cdot 5^3 \cdot 41$	24. $a = 2^6 \cdot 5^3 \cdot 101$
25. $a = 3^7 \cdot 5^2 \cdot 103$	26. $a = 2^7 \cdot 3^2 \cdot 7^2 \cdot 97$	27. $a = 3^3 \cdot 7^2 \cdot 101$
28. $a = 2^5 \cdot 3^4 \cdot 7^2 \cdot 71$	29. $a = 2^9 \cdot 3^4 \cdot 11^2 \cdot 41$	30. $a = 2^9 \cdot 3^4 \cdot 5^3 \cdot 53$

9. MODULAR ARITHMETIC

9.1. CLASSES OF CONGRUENCE

Let us consider the example of distribution of the set of integers into a finite number of classes with some relationships among these numbers.

Let us take the number $p = 7$. This number has 7 different remainders – 0, 1, 2, 3, 4, 5, 6, and there are not any other remainders of the division of any integers by 7. So, we can form a table of the distribution of integers into the classes corresponding to such seven remainders.

Table 9.1 – The distribution of integers into classes by remainders from division by 7

Remainders→ Quotient ↓	0	1	2	3	4	5	6
1	7	7+1=8	7+2=9	7+3=10	7+4=11	7+5=12	7+6=13
2	14	15	16	17	18	19	20
3	21	22	23	24	25	26	27
…	…	…	…	…	…	…	…
20	140	141	142	143	144	145	146
…	…	…	…	…	…	…	…
33	231	232	233	234	235	236	237
…	…	…	…	…	…	…	…
q	**7q**	**7q+1**	**7q+2**	**7q+3**	**7q+4**	**7q+5**	**7q+6**
…	…	…	…	…	…	…	…

This table has 7 columns with integers and infinite numbers of rows because infinite set of integers is distributed into 7 classes.

All numbers from class 0 have common property such that they are divided by 7. We can denote this class as 7q. All numbers of class 1 have the remainder r=1 from division by 7 and we denote this class as 7q+1. We denote classes 2, 3, 4, 5, 6 as 7q + 2, 7q + 3, 7q + +4, 7q + 5, 7q + 6 respectively.

In number theory the devisor 7 is called **modulus,** and all numbers of one class are called **congruent modulo 7.** We say that 141 is congruent to 15 modulo 7 because these numbers are in the same class 7q + 1. We denote this fact as: $141 \equiv 15 (\mathrm{mod}\, 7)$.

Numbers of different classes are not congruent modulo 7. 233 is not congruent to 25 modulo 7 because 233 belongs to the class 7q + 2 and 25 belongs to the class 7q + 4. We denote this fact as $233 \not\equiv 25 (\mathrm{mod}\, 7)$.

Generalizing the consideration, we can make a conclusion.

For every integer ***m*** called **modulus,** we can consider the set of ***m* remainders {0, 1, 2, …, r_i, …, *m*-1}**. Each remainder r_i of this set forms a corresponding **number class**. This class is denoted as $m \times q + r_i$, $q \in Z$, $r_i < m$. All numbers from the class $m \times q + r_i$ are **congruent to each other** modulo *m*. This fact is denoted as $\forall a, b \in mq + r_i \Rightarrow a \equiv b (mod\, m)$. Another notation is $a = b + mq$.

Definition 9.1.1

The relationship $a \equiv b (\mathrm{mod}\, m)$ is called congruence modulo *m*.

Numbers from **different** classes are not congruent modulo *m*. This fact is denoted as

$$\forall a \in mq + r_i \;\&\; \forall b \in mt + r_j, i \neq j,\ a \not\equiv b (mod\, m).$$

Definition 9.1.2

Each number of the class is called **residue** with respect to other numbers from the same class**.**

Definition 9.1.3

A system that includes **one residue from each class** is called **a complete residue system modulo *m*.** In particular, {0, 1, . . . , m−1} is **the set of the least nonnegative residue modulo *m*.**

For example, the set of numbers {7, 15, 142, 234, 144, 26, 13} forms a complete residue system modulo 7, because the residue of each classes belongs to it. The set of the least nonnegative residue modulo 6 is the set {0, 1, 2, 3, 4, 5, 6}.

Each residue of the class $m \times q$ is congruent to 0 modulo m $mq \equiv 0 (mod\, m),\ \forall q \in Z$. If we add/ subtract a residue of this class to (from) any side of an arbitrary congruence modulo *m*, then the congruence will not be altered.

For example, let us consider a congruence modulo 7. We have:

$$41 \equiv 6 (mod\, 7),\ \ 41 \equiv 6 - 7 (mod\, 7) \Rightarrow 41 \equiv -1 (mod\, 7).$$

Really, 41 = 7·5 + 6, $7 \cdot 5 \in 7 \cdot q$, then $7 \cdot 5 \equiv 0 (mod\, 7)$ and $41 \equiv 6 (mod\, 7)$. On the other hand,

41 = 7·6 – 1, $7 \cdot 6 \in 7 \cdot q$, then $7 \cdot 6 \equiv 0 (mod\, 7)$ and $41 \equiv -1 (mod\, 7)$. Thus, $6 \equiv 6 - 7 = -1 (mod\, 7)$.

This example shows that we can consider a negative residue as well as a nonnegative one.

Lemma 9.1.1

For any a, b >0 and positive *m*, the following statement holds. If $a \equiv b (mod\, m)$**, then** $a \equiv b - m (mod\, m)$ **and** $a - m \equiv b (mod\, m)$.

Let us consider the complete system of the least nonnegative residue modulo *m*. This system can be separated into two subsystems as specified out below.

1. First, if *m* is **odd,** then the residues 0, 1, 2, …, $\frac{m-1}{2}$ will remain the same, and from the residues $\frac{m-1}{2} + 1$, $\frac{m-1}{2} + 2 \ldots$, $m - 1$ we will subtract modulo *m*. As a result, we will obtain the system of the residues $\{0, \pm 1, \pm 2, \ ..., \ \pm \frac{m-1}{2}\}$.

2. Secondly, if *m* is **even,** then the residues 0, 1, 2, …, $\frac{m}{2}$ will not be altered, and from the residues $\frac{m}{2} + 1$, $\frac{m-1}{2} + 2 \ldots$, $m - 1$ we

will subtract modulus *m*. Thus, we will obtain the system of residues $\{-\frac{m}{2}+1,...,-2,-1,0,1,2,...,\frac{m}{2}\}$.

Definition 9.1.4

The complete system of the least nonnegative residues modulo *m* can be split into two subsystems**.** There are *m* residues in both subsystems. Each subsystem is called **the least absolute residue system modulo *m*.**

Example 9.1.1

Construct the least absolute residue system: 1) modulo 7; 2) modulo 8.

Solution

1) The least nonnegative residues modulo 7 are $\{0,1,2,3,4,5,6\}$. $\frac{7-1}{2}=3$, so **the least absolute residue system modulo 7** is $\{0,1,2,3,4-7,5-7,6-7\}$ =(0, ±1, ±2, ±3} or $\{-3,-2,-1,0,1,2,3\}$;

2) The least nonnegative residues modulo 8 are $\{0,1,2,3,4,5,6,7\}$. $\frac{8}{2}=4$, so **the least absolute residue system modulo 8** is $\{0,1,2,3,4,5-8,6-8,7-8\}=\{-3,-2,-1,0,1,2,3,4\}$.

Properties of congruences modulo *m*

Theorem 9.1.1

For any integers a, b, c, and m > 0 the following properties hold:

1. Reflexivity property $a \equiv a \pmod m$

This property means that any integer can be uniquely represented as $a = m \cdot q + r,\ 0 \le r < m$ for arbitrary positive divisor *m* (Theorem 3.1).

2. Symmetry property $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$

This property signifies that both numbers have the same remainder in division by *m*.

For example: $24 \equiv 38 \pmod{7} \Rightarrow 38 \equiv 24 \pmod{7}$. Indeed, $24 = 3 \cdot 7 + 3$ *and* $38 = 5 \cdot 7 + 3$. So, both numbers have the same remainder 3 in division by 7.

3. Transitivity property

If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

For transitivity, assume that *a* leaves the same remainder as *b* on division by *m*, and that *b* leaves the same remainder as *c*. The all three leave the same remainder as each other, and in particular *a* leaves the same remainder as *c*.

For example: $24 \equiv 38 \pmod{7}$, $38 \equiv 150 \pmod{7} \Rightarrow 24 \equiv 150 \pmod{7}$**.**

The all three have the same remainder of 3 on division by 7.

Actually, $24 = 3 \cdot 7 + 3$, $38 = 5 \cdot 7 + 3$, $150 = 21 \cdot 7 + 3$.

Theorem 9.1.2

For any *a, b*$\in$*Z* and positive *m*>1, *m*$\in$*Z,* $a \equiv b \pmod{m}$ iff $m \mid (a - b)$.

Proof

Clearly if $m \mid (a - b)$, then

$a - b = mq \Rightarrow a = b + mq \Rightarrow a \equiv b (mod\ m)$.

On the other hand,

$a \equiv b (mod\ m) \Rightarrow a = b + mt \Rightarrow a - b = mt \Rightarrow m \mid (a - b)$.

So, the **difference of any two numbers from the same class belongs to class 0,**

$a - b \equiv 0 (mod\ m)$.

Theorem 9.1.3

If $a \equiv b \pmod{m}$ and $c \equiv d (mod\ m)$, then

1) $a+c \equiv b+d(mod\, m)$ and $a-c \equiv b-d(mod\, m)$ – **algebraic addition**.

Consequence: $a+c \equiv b(mod\, m) \Rightarrow a \equiv b-c(mod\, m)$;

2) $ac \equiv bd(mod\, m)$ – **multiplication;**

3) $a^n \equiv b^n(mod\, m)$ for all $n \geq 1$ – **powering;**

4) $\forall k \in Z \;\; ka \equiv kb(mod\, m)$ – **multiplication by number;**

5) $\forall a, b, a_1, b_1, \; k \in Z, \; \gcd(m,k) = 1,$

$a = k \cdot a_1, \;\; b = k \cdot b_1 : \;\; a \equiv b(\mathrm{mod}\, m) \Rightarrow a_1 \equiv b_1(\mathrm{mod}\, m)$;

6) **If** $a_i \equiv b_i(mod\, m), \; i = \overline{1,n}$ *and* $x \equiv y(mod\, m)$, **then**

$\sum_{i=0}^{n} a_{n-i} x^{n-i} \equiv \sum_{i=0}^{n} b_{n-i} y^{n-i}(mod\, m)$ **for all polynomials with integer coefficients.**

Proof

1) $a \equiv b(mod\, m)$ implies that $a = m \cdot t + b, \; t \in Z$; $c \equiv d(mod\, m)$ means that $c = m \cdot q + d, \; q \in Z$.

The addition of both equations produces

$a + c = m \cdot t + b + m \cdot q + d = m \cdot (t+q) + b + d;$

$t + q = s \in Z; \;\; m \cdot s \equiv 0(mod\, m) \Rightarrow a + c \equiv b + d(mod\, m).$

Similarly, if we add two congruences such that $a + c \equiv b(mod\, m)$, and $-c \equiv -c(mod\, m)$, then we will get

$a \equiv b - c(mod\, m)$.

2) $a \equiv b(mod\, m)$ means that $a = m \cdot t + b, \; t \in Z$; $c \equiv d(mod\, m)$ signifies that $c = m \cdot q + d, \; q \in Z$. Product of both equations yields

$a \cdot c = (mt + b)(mq + d) = mtmq + mtd + bmq + bd =$

$= m(mtq + td + bq) + bd;$

$mtq + td + bq = \mathrm{s} \in \mathrm{Z}; \; \mathrm{ms} \equiv 0(\mathrm{modm}) \Rightarrow ac \equiv bd(\mathrm{mod}\, m).$

3) $a^n \equiv b^n(mod\, m)$ is got by successive multiplication of congruences by themselves. Hence, property (3) is indeed true.

4) $a \equiv b(mod\, m) \Leftrightarrow a = b + mq$, we multiply the last expression by *k*:

$$ka = kb + mkq,\ kq = q_1 \in Z \Rightarrow ka = kb + mq_1 \Rightarrow ka \equiv kb(mod\, m).$$

5) $a = k \cdot a_1,\ b = k \cdot b_1:\ a \equiv b \pmod m \Rightarrow$

$\Rightarrow ka_1 \equiv kb_1 \pmod m$ *or* $ka_1 = kb_1 + mq$. According to *Integration property* in Theorem 1.2, we can write $k \mid mq$. Since $gcd(m,k) = 1$, it follows that $k \mid q,\ q = kq_1$. So, we have $ka_1 = kb_1 + mkq_1$. Finally, by dividing the last expression by *k*, we will get $a_1 = b_1 + mq_1 \Rightarrow a_1 \equiv b_1(mod\, m)$.

6) Let us consider a congruence

$$a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = \sum_{i=0}^{n} a_{n-i}x^{n-i} \equiv 0(mod\, m).$$

Taking into account that $a_i \equiv b_i \pmod m$, $i = \overline{1,n}$ *and* $x \equiv y \pmod m$, or $a_i = b_i + mq_i;\ x = y + mt$, we obtain

$$\sum_{i=0}^{n} a_{n-i}x^{n-i} = \sum_{i=0}^{n} (b_{n-i} + \boldsymbol{mq_{n-i}})x^{n-i} = \sum_{i=0}^{n} b_{n-i}x^{n-i} + \boldsymbol{m}\sum_{\boldsymbol{i=0}}^{\boldsymbol{n}} \boldsymbol{q_{n-1}} \equiv$$

$$\equiv \sum_{i=0}^{n} b_{n-i}x^{n-i} \pmod m.$$

Further, the right side of obtained congruence can be rewritten as follows:

$$\sum_{i=0}^{n} b_{n-i}x^{n-i} = \sum_{i=0}^{n} b_{n-i}\left(\boldsymbol{y}+\boldsymbol{mt}\right)^{n-i} =$$

$$= \sum_{i=0}^{n} b_{n-i}\left(y^{n-i} + C_{\mathbf{n-i}}^{\ 1} y^{n-i-1}mt + ... + C_{\mathbf{n-i}}^{\ \mathbf{n-i-1}} y(mt)^{n-i-1} + (mt)^{n-i}\right).$$

By denoting

$q = C_{n-i}^{\ 1} y^{n-i-1}t + ... + C_{n-i}^{\ n-i-1} ym^{n-i-2}t^{n-i-1} + m^{n-i-1}t^{n-i} \in Z$, we have

$$\sum_{i=0}^{n} b_{n-i}\left(\boldsymbol{y} + \boldsymbol{mt}\right)^{n-i} = \sum_{i=0}^{n} b_{n-i}\left(y^{n-i} + mq\right) = \sum_{i=0}^{n} b_{n-i}y^{n-i} + \sum_{i=0}^{n} b_{n-i}\boldsymbol{mq} =$$

$$= \sum_{i=0}^{n} b_{n-i} y^{n-i} + m \sum_{i=0}^{n} b_{n-i} \boldsymbol{q} .$$

By introducing $q_1 = \sum_{i=0}^{n} b_{n-i} q \in Z$, we get

$$\sum_{i=0}^{n} b_{n-i} x^{n-i} = \sum_{i=0}^{n} b_{n-i} y^{n-i} + m \sum_{i=0}^{n} b_{n-i} \boldsymbol{q} = \sum_{i=0}^{n} b_{n-i} y^{n-i} + m q_1 \equiv$$

$$\equiv \sum_{i=0}^{n} b_{n-i} y^{n-i} \pmod{m}.$$

As a result, we deduce $\sum_{i=0}^{n} a_{n-i} x^{n-i} \equiv \sum_{i=0}^{n} b_{n-i} y^{n-i} (mod\ m)$.

Examples 9.1.2

Take two congruences $3 \equiv 52 (mod\, 7)$ and $5 \equiv 40 (mod\, 7)$.

1) The sum of $3 \equiv 52 (mod\, 7)$ and $5 \equiv 40 (mod\, 7)$ is $8 \equiv 92 (mod\, 7)$. The obtained congruence is true because $8 \equiv 1 (mod\, 7)$ and $92 \equiv 1 (mod\, 7)$. The difference between them is $-2 \equiv 12 (mod\, 7)$. Such congruence is correct, because $-2 \equiv 5 (mod\, 7)$ and $12 \equiv 5 (mod\, 7)$.

2) The product of given congruences is $15 \equiv 2080 (mod\, 7)$. One can see that $15 \equiv 1 (mod\, 7)$ and $2080 = 7 \cdot 297 + 1 \Rightarrow 2080 \equiv 1 (mod\, 7)$. Hence, this congruence is correct.

3) Raise the first congruence to the second power:

$$\left(3 \equiv 52 \pmod 7\right)^2 \Rightarrow 3^2 \equiv 52^2 \pmod 7 \Rightarrow 9 \equiv 2704 \pmod 7;$$

$$9 \equiv 2 \pmod 7;\ 2704 = 7 \cdot 386 + 2 \Rightarrow 2704 \equiv 2 \pmod 7.$$

So, if $3 \equiv 52 \pmod 7$ is true, then $3^2 \equiv 52^2 \pmod 7$ is indeed true.

4) Multiply through the congruence $3 \equiv 52 \pmod 7$ by 10. We obtain $30 \equiv 520 \pmod 7$; $30 = 7 \cdot 4 + 2$; $520 = 7 \cdot 74 + 2$. Both numbers 30

and 520 leave the same remainder 2 when divided by 7; hence $3\cdot 10 \equiv 52\cdot 10 \pmod 7$ is true.

5) Take the congruence $5 \equiv 40 (mod\, 7)$. Both integers of this congruence are divided by 5. The greatest common divisor of 5 and 7 is 1. Divide the congruence by 5: 5/5=1; 40/5=8. The congruence $1 \equiv 8 (mod\, 7)$ is correct.

6) Find the remainder of the division 1348^{26} by 13 without calculator.

Solution

To solve this problem means to find the least positive residue of the residue class modulo 13 with the representative 1348^{26}

$1348 = 13\cdot 103 + 9 \Rightarrow 1348 \equiv 9 (mod\, 13);\ 9 < 13;\ gcd(9,13) = 1$. The integer 9 is the least positive residue for the integer 1348 modulo 13. Then using property **(6),** we can write $1348^{26} \equiv 9^{26} (mod\, 13)$.

Similarly, we will reduce the integer 9^{26} taking into account property **(6).**

$$9^{24} = \left(9^2\right)^{13} = 81^{13} = (13\cdot 6 + 3)^{13} \equiv 3^{13} (mod\, 13);$$

$$3^{13} = 3^{12}\cdot 3 = \left(3^4\right)^3 \cdot 3 = 81^3 \cdot 3 \equiv 3^3 \cdot 3 \pmod{13};$$

$$3^3 \cdot 3 = 27\cdot 3 = (13\cdot 2 + 1)\cdot 3 \equiv 3 \pmod{13};\ \mathbf{3 < 13}.$$

Thus we have obtained that the remainder of the division 1348^{26} by 13 is 3.

9.2. PROPERTIES OF CONGRUENCES THAT CHANGE MODULUS

Theorem 9.2.1

If $a \equiv b \pmod m$, then

1) for $\forall a,b,a_1,b_1,m,m_1,k \in Z,\ a = k\cdot a_1,\ b = k\cdot b_1,\ m = k\cdot m_1$: the following congruence holds:

$$\left(\frac{a}{k}\right) \equiv \left(\frac{b}{k}\right) \left(\bmod \frac{m}{k}\right) \ or\ \ a_1 \equiv b_1 \pmod{m_1}.$$

For example, we have

$155 \equiv 85 (mod\ 35);\quad \frac{155}{5} = 31;\ \frac{85}{5} = 17;\ \frac{35}{5} = 7 \Rightarrow 31 \equiv 17 (mod\ 7);$

2) $\forall k \in Z\ \ ka \equiv kb (mod\ km)$ – **multiplication by number.**

For example, multiply the congruence $31 \equiv -2 (mod\ 11)$ by 5. We obtain $155 \equiv -10 (mod\ 55)$. This congruence holds because both integers belong to the same residue class modulo 55 with the least positive residue 45;

3) $\forall d \geq 1,\ \ d \in Z:\ if\ \ d \mid m$ and $d \mid a \Rightarrow$

$\Rightarrow d \mid b$ ($if\ \ d \mid m$ and $d \mid \boldsymbol{b} \Rightarrow d \mid a$).

For example, $x \equiv 93 (mod\ 144);\ \ gcd(93,144) = 3 \Rightarrow 3 \mid x;$

4) if $a \equiv b (\mathrm{mod}\, m_1)$, and $a \equiv b (\mathrm{mod}\, m_2)$, and....., and

$a \equiv b (\mathrm{mod}\, m_k) \Leftrightarrow$ then $a \equiv b (\mathrm{mod}\, Lcm(m_1, m_2, ..., m_k))$. **Moreover, if** $\gcd(m_1, m_2, ..., m_k) = 1$, **then** $a \equiv b (mod\ m_1 m_2 ... m_k)$.

For example,

a) Suppose $x \equiv 3 (\mathrm{mod}\, 5)$, $x \equiv 3 (\mathrm{mod}\, 11)$, $x \equiv 3 (\mathrm{mod}\, 7)$, we get $x \equiv 3 (\mathrm{mod}\, 5 \cdot 11 \cdot 7)$.

b) Assume that $x \equiv 3 (\mathrm{mod}\, 5)$, $x \equiv 3 (\mathrm{mod}\, 35)$, $x \equiv 3 (\mathrm{mod}\, 21)$, $lcm(5, 35, 21) = 105$, then $x \equiv 3 (\mathrm{mod}\, 105)$.

9.3. FERMAT'S LITTLE THEOREM AND EULER'S THEOREM ON THE EXISTENCE OF THE UNIT ELEMENT MODULO *m*

Theorem 9.3.1. (Fermat's little theorem) If p is a prime and a is a coprime to p (gcd(a,p)=1), then

$p \mid (a^p - a)$.

This is the same as

$a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.

Theorem 9.3.2. (Euler's theorem) If m > 0 and a is a coprime to m

(gcd(a,m)=1), then

$$a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m).$$

Example 9.3.1. Check, if $167^{10} \equiv 1(mod\ 11)$

Solution

Consider the following congruence:

$167 \equiv 2(mod\ 11) \Rightarrow gcd(167,11) = 1$.

Hence, with **Fermat's little theorem 9.3.1,**

$167^{10} \equiv 2^{10}(mod\ 11)$,

$2^{10} = (2^5)^2 = 32^2 \equiv (32 - 3 \cdot 11)^2 = (-1)^2 = 1(mod\ 11)$.

Then $167^{10} \equiv 1(mod\ 11)$ **and Fermat's little theorem holds.**

Example 9.3.2. Find the remainder from the division of 23^{1443} ***by 13.***

Solution

We have

$23^{1443} \equiv x(mod\ 13);\ 23 \equiv -3(mod\ 13) \Rightarrow 23^{1443} \equiv (-3)^{1443}(mod\ 13)$.

Taking into account that gcd(3,13)=1, then with **Fermat's little theorem we can write** $(-3)^{12} \equiv 1(mod\ 13)$**.**

Further, raising the congruence to the 120th power, we get

$((-3)^{12})^{120} \equiv 1^{120}(mod\ 13) \Rightarrow (-3)^{1440} \equiv 1(mod\ 13)$.

Obviously, 1443 = 1440+3, so we have

$$(-3)^{1443} = (-3)^{1440+3} = \underbrace{(-3)^{1440}}_{\equiv 1(\mathrm{mod}13)}(-3)^3 \equiv (-3)^3 \equiv -27 \equiv$$

$$\equiv -27 + 3 \cdot 13 \equiv 12 (\mathrm{mod} 13).$$

Hence, the remainder from the division 23^{1443} by 13 is equal 12.

Example 9.3.3. Find the last three digits of the integer 13^{1599}**.**

Solution

Let us rephrase this problem as follows: **find the remainder from the division of** 13^{1599} **by 1000.**

A solution to the problem will be the congruence: $13^{1599} \equiv x(mod\,1000)$.

Obviously, $gcd(13,1000)=1$. As 1000 is composite, then $1000=2^3\cdot 5^3$. Hence, **Euler's theorem** is correct for this number: $13^{\varphi(1000)} \equiv 1(mod\,1000)$,

$$\varphi(1000)=\varphi(2^3\cdot 5^3)=(2^3-2^2)(5^3-5^2)=4\cdot 100=400\,.$$

We have $13^{400} \equiv 1(1000)$ – **Euler's theorem.**

The exponent 1599 is not divisible by 400, but $1600=400\cdot 4$. Multiplying the congruence by 13, we obtain $13^{1600} \equiv 13x(mod\,1000)$. Using property (3) in Theorem 9.1.10, we can write down that $13^{1600}=(13^{400})^4 \equiv 1(mod\,1000)$. So, $13x \equiv 1(mod\,1000)$. Then, taking into account property (1) in Theorem 9.1, we add the modulus 1000 to the right side of the congruence:

$13x \equiv 1001(mod\,1000);\ 1001=13\cdot 77;\ \ gsd(13,1000)=1\,.$

Finally, we divide the last congruence by 13 using the property (5) in Theorem 9.1:

$x \equiv 77(mod\,1000)$.

The answer for the task is that the remainder from the division of 13^{1599} by 1000 equals 77, and the last three digits of the integer 13^{1599} are 077.

Example 9.3.4. Find the remainder from the division of 348^{128} by 21.

Solution

Let us write the congruence for the solution of this task: $348^{128} \equiv x(mod\,21)$.

It should be noted that gcd(348,21) = 3. Then, according to the property (3) in Theorem 9.2.1, we can conclude that $3 \mid x$.

By introducing new variable $x = 3y$, we obtain that $348^{128} \equiv 3y(mod\ 21)$.

Let us divide the congruence by 3 using the property (1) in Theorem 9.2.1:

$$348^{128} = 348^{127} \cdot 348 \equiv 3y \pmod{21} \Rightarrow 348^{127} \cdot 116 \equiv y \pmod 7,$$

$$348 = 7^3 + 5;\ 116 = 7 \cdot 16 + 4 \Rightarrow 348 \equiv 5 \pmod 7,$$

$$116 \equiv 4 \pmod 7 \overset{prop\ (6)}{\Rightarrow} (5)^{127} \cdot 4 \equiv y \pmod 7.$$

Obviously, $gcd(5,7) = 1$, then, according to **Fermat's little theorem,** we get $5^6 \equiv 1(mod\ 7)$.

$$127 = 6 \cdot 21 + 1 \Rightarrow 5^{127} = 5^{6 \cdot 21 + 1} = \left(5^6\right)^{21} \cdot 5.$$

Since $5^6 \equiv 1(mod\ 7) \Rightarrow \left(5^6\right)^{21} \equiv 1(mod\ 7)$ (the property (3) in Theorem 9.1.10), and $5^{127} \cdot 4 = \left(5^6\right)^{21} \cdot 5 \cdot 4 \equiv 20 \pmod 7$, $20 \equiv 6 \pmod 7 \Rightarrow y \equiv 6 \pmod 7$.

Finally, using back substitution for $x = 3y$, we obtain $y \equiv 6(mod\ 7) \Rightarrow x \equiv 3 \cdot 6(mod\ 21)$.

The answer for the task is that the remainder from the division of 348^{128} by 21 equals 18.

Example 9.3.5. Find the remainder from the division of $143^{50} + 343^{50}$ by 17.

Solution

Let us write the congruence for the solution of the given task: $143^{50} + 343^{50} \equiv x(mod\ 17)$.

First, according to property (1) in Theorem 9.1.3, we see that stated above problem splits into two congruences:

$$143^{50} \equiv x_1(mod\ 17);\ \ 343^{50} \equiv x_2(mod\ 17).$$

Obviously, $x = x_1 + x_2$.

So, we shall solve each problem separately and then find the sum of the solutions. Let us start with the first one. We have

1. $143^{50} \equiv x_1 (mod\, 17)$.

$\gcd(143,17) = 1;\ 17\ is\ prime \overset{Th 9.3.1}{\Rightarrow} 143^{16} \equiv 1 (\mathrm{mod} 17)$,

$50 = 16 \cdot 3 + 2 \Rightarrow 143^{50} = \underbrace{\left(143^{16}\right)^3}_{\equiv 1 (mod\, 17)} \cdot 143^2 \equiv 143^2 (mod\, 17)$,

$143 = 17 \cdot 8 + 7 \Rightarrow 143 \equiv 7 (\mathrm{mod} 17) \Rightarrow 143^2 \equiv 7^2 (\mathrm{mod} 17)$,

$7^2 = 49 = 17 \cdot 2 + 15 = 17 \cdot 3 - 2 \Rightarrow 7^2 \equiv -2 (mod\, 17)$.

Thus $x_1 \equiv -2 (mod\, 17)$ is a solution to the first congruence.

2. Now, we will consider the second congruence. We get $343^{50} \equiv x_2 (mod\, 17)$.

$\gcd(343,17) = 1;\ 17\ is\ prime \overset{Th 9.3.1}{\Rightarrow} 343^{16} \equiv 1 (\mathrm{mod} 17)$,

$50 = 16 \cdot 3 + 2 \Rightarrow 341^{50} = \underbrace{\left(343^{16}\right)^3}_{\equiv 1 (mod\, 17)} \cdot 343^2 \equiv 343^2 (mod\, 17)$,

$343 = 17 \cdot 20 + 3 \Rightarrow 343 \equiv 3 (\mathrm{mod} 17) \Rightarrow 343^2 \equiv 3^2 (\mathrm{mod} 17)$,

$3^2 = 9 < 17$.

Thus we have obtained $x_2 \equiv 9 (mod\, 17)$.

3. Finally, the total solution to the given problem is $x = x_1 + x_2 \equiv -2 + 9 = 7 (mod\, 17)$.

The answer for the task is that the remainder from the division of $143^{50} + 343^{50}$ by 17 equals 7.

PROBLEMS FOR UNIT 9

9.1. Find the remainder from the division

1. 6617 by 7	2. 2100+3100 by 5	3. 11802 by 1000	4. 172001 by 1000
5. 192402 by 100	6. 17852 by 11	7. 19671968 by 11	8. 383175 by 45
9. 109345 by 14	10. 439291 by 60	11. 293275 by 48	12. 6617 by 7
13. 11753 by 11	14. 570+750 by 12	15. 580+7100 by 13	16. 550+13100 by 18
17. 111841 by 7	15. 580+7100 by 13	16. 550+13100 by 18	20. 122751 by 10
21. 343741 by 26	22. 1782741 by 22	23. 111201 by 1000	24. 71199 by 1000
25. 3157 by 100	26. 1778 by 100	27. 1979 by 100	28. 7114 by 100
29. 11203 by 100	30. 7332 by 100		

10. LINEAR CONGRUENCES WITH ONE UNKNOWN

10.1. CONGRUENCES OF THE FIRST ORDER. SOLVING CONGRUENCES

Definition 10.1.1

An expression of the form

$ax + b \equiv 0 (\mathrm{mod}\, m)$ or $ax \equiv b (\mathrm{mod}\, m)$

is called a congruence of the first order or a linear congruence with one unknown.

Definition 10.1.2

A solution of the first order congruence modulo m is a class of numbers $x_1 + mt,\ t \in Z$ such that substitution of each residue into the congruence yields the equivalent congruence $b \equiv b (\mathrm{mod}\, m)$.

As a rule, the number x_1 belongs to the least absolute residue system modulo n or the least nonnegative residue system modulo *n.*

To study existence of solutions of such congruence, we shall consider several situations:

First, we introduce case $(a, m) = 1$.

If x ranges over a complete residue system modulo m, then the number ax also takes on values from such system with the precision to a sequence order. Thus, there exists only one x congruent to b.

Conclusion

If condition $(a, m) = 1$ takes place, then the congruence $ax \equiv b (\mathrm{mod}\, m)$ has a unique solution.

Secondly, let us consider the congruence $ax \equiv b (\mathrm{mod}\, m)$ and assume that $(a, m) = d > 1$:

$ax \equiv b (\mathrm{mod}\, m) \Rightarrow ax = b + mt$.

If $d \mid a,\ d \mid m \Rightarrow d \mid b$, then the congruence's terms can be written as follows:

$a = a_1 d,\ b = b_1 d,\ m = m_1 d,\ (a_1, m_1) = (b_1, m_1) = 1.$

Hence, according to a property of congruences, such congruence can be divided by d. Finally, we get

$a_1 x \equiv b_1 (\mathrm{mod}\, m_1)$.

From the above, it has a unique solution $x \equiv x_1 (\mathrm{mod}\, m_1)$ or $x = m_1 t + x_1$. On the other hand, if we consider the complete system of incongruent residues to modulus $m = dm_1$, then we will be able to see that there will be solutions in the interval $[0, m]$ as follows:

$x_1,\ x_1 + m_1,\ x_1 + 2m_1, ..., x_1 + (d-1)m_1$.

Here, the total number of solutions is d. The solutions are incongruent modulo m and, consequently, each of them forms their own class of residues.

Conclusion

In the case condition $(a, m) = d > 1$ holds, then the congruence will possess at least one solution if $d \mid b$. There will be exactly d solutions (d classes of solutions). The first of them could be obtained from the given congruence divided by d, the rest are calculated as follows:

$x_2 = x_1 + m_1, ..., x_d = x_1 + (d-1)m_1$.

A linear congruence can be solved by several methods.

10.1.1. Application of Congruence's Properties

Examples

a) Solve the congruence: $15x \equiv 25 (\mathrm{mod} 17)$.

Solution

First, let us consider gcd of 15 and 17. Since $(15,17) = 1$, then the congruence possesses a unique solution. Further, using properties

of congruence, we can simplify it. Here, both 25 and 15 have common multiplier 5 that is coprime to modulo 17. Hence, by applying the properties of congruence, we can divide equation by 5: $3x \equiv 5(\mathrm{mod}17)$. The number 5 corresponds to the least absolute residue – 12, which is multiple of 3. Finely, we cancel off equation $3x \equiv -12(\mathrm{mod}17)$ by 3, this yields: $x \equiv -4(\mathrm{mod}17)$. Thus, the congruence has a unique solution from the least absolute residue system modulo 17 or from the least nonnegative residue system modulo 17: $x = -4 + 17 = 13$.

b) Solve the congruence $10x \equiv 35(\mathrm{mod}\,55)$.

Solution

We get $(10,55) = 5 > 1,\ 5 \mid 35$.

Hence, the congruence has just five solutions.

Then cancellation by $d = 5$ produces

$2x \equiv 7(\mathrm{mod}11)$.

Taking into account $(2,11) = 1$, we can make a conclusion that such congruence possesses a unique solution

$2x \equiv 7 + 11(\mathrm{mod}11) \Rightarrow 2x \equiv 18(\mathrm{mod}11) \Rightarrow x \equiv 9(\mathrm{mod}11)$.

In the same way, the given congruence $10x \equiv 35(\mathrm{mod}\,55)$ will have five solutions of the obtained above form as follows:

$x_0 \equiv 9(\mathrm{mod}\,55)$, $x_1 \equiv 9 + 11 \cdot 1 = 18(\mathrm{mod}\,55)$,

$x_2 \equiv 9 + 11 \cdot 2 = 31(\mathrm{mod}\,55)$,

$x_3 \equiv 9 + 11 \cdot 3 = 42(\mathrm{mod}\,55)$, $x_4 \equiv 9 + 11 \cdot 4 = 53(\mathrm{mod}\,55)$.

If we again add extra modulus 11, then we will get $x_5 \equiv 9 + 5 \cdot 11 = 64 \equiv 9(\mathrm{mod}\,55)$.

Thus solutions x_0, x_1, x_2, x_3, x_4 are incongruent modulo 55 and $x_5 \equiv x_0\,(\mathrm{mod}\,55)$.

Finely, we have obtained five incongruent classes that are solutions of given congruence. In a general form, solution may be written as follows:

$$x \equiv 9 + 11t \pmod{55}, \quad t = [0,...,d-1] = [0,...,4].$$

c) Solve the congruence $10x \equiv 33 \pmod{55}$.

Solution

We obtain that $(10,55) = 5 > 1$, but 33 is not multiple of 5, thus the congruence has no solutions.

10.1.2. APPLICATION OF CONVERGENTS

Consider the case $ax \equiv b \pmod{m}$, $(a,m) = 1$.

Let us expand the given below ratio into continued fraction

$$\frac{m}{a} = q_{1`} + \cfrac{1}{q_2 + ... \\ \qquad + \cfrac{1}{q_n}}.$$

We shall get a set of partial quotients $q_1, q_2, ..., q_n$. According to a well-known scheme, we will built continued fractions: $\delta_i = \frac{P_i}{Q_i}$. Let us consider the last two terms from the set: $\delta_{n-1} = \frac{P_{n-1}}{Q_{n-1}}$, $\delta_n = \frac{P_n}{Q_n} = \frac{m}{a}$.

It follows from properties of continued fractions that $P_n Q_{n-1} - Q_n P_{n-1} = (-1)^n$. Hence, $mQ_{n-1} - aP_{n-1} = (-1)^n$. Since Q_{n-1} is an integer, we may suppose that mQ_{n-1} is a modular period which can be truncated. This leads to $aP_{n-1} = (-1)^{n-1} \bmod(m)$. Multiplying both parts of the expression by number $(-1)^n b$, we obtain

$$a(-1)^{n-1} b P_{n-1} \equiv b \pmod{m}.$$

Thus the solution of the congruence will be $x \equiv (-1)^n P_{n-1} b (\mathrm{mod}\, m)$.

Example

Solve the congruence $256x \equiv 179 (\mathrm{mod}\, 337)$.

Solution

We have

$(256,337) = 1$.

Therefore, the congruence possesses a unique solution. Let us expand fraction $\frac{337}{256}$ into continued one as follows:

$\frac{337}{256} = 1 + \frac{81}{256}, \quad q_1 = 1;$ $\qquad$ $\frac{256}{81} = 3 + \frac{13}{81}, \; q_2 = 3;$

$\frac{81}{13} = 6 + \frac{3}{13}, \; q_3 = 6;$ $\qquad$ $\frac{13}{3} = 4 + \frac{1}{3}, \; q_4 = 4;$

$\frac{3}{1} = 3, \; q_5 = 3.$

Form the table.

i	0	1	2	3	4	5
q_i		1	3	6	4	3
P_i	1	1	4	25	104	337
Q_i	0	1	3	19	79	256

It follows from the obtained above data that

$n = 5, \; P_{n-1} = P_4 = 104, \; b = 179 \Rightarrow$

$\Rightarrow x = (-1)^4 104 \cdot 179 (\mathrm{mod}\, 337); \quad \frac{104 \cdot 179}{337} = 55 + \frac{81}{337}.$

Thus the solution is $x \equiv 81 (\mathrm{mod}\, 337)$.

10.2. MULTIPLICATIVE INVERSE

Definition 10.2.1

If a' is a solution of the congruence $ax \equiv 1 (\mathrm{mod}\, m)$, then a' is called a (multiplicative) inverse of a modulo m, and we say that a is invertible modulo m. We shall denote $a' = a^{-1}$.

Since we know methods of solutions of linear congruences involving one unknown, we may find an answer to the question:

Does there exist any element from the complete residue system modulo m having multiplicative inverse?

First, let us consider the congruence

$ax \equiv 1 (\mathrm{mod}\, m)$.

As the right side of the congruence equals 1 then, according to a condition of the solution's existence, we deduce $(a, m) = 1$. If values of a were elements from the least nonnegative system modulo m – such system is the base for all class of numbers – then, obviously, the congruence could be nonsolvable. For example, $m = 15,\ a = 5$. Hence, from the system under consideration it is necessary to throw away all multiples of modulus. So, we will get the reduced residue system containing $\varphi(m)$ elements. Finally, for any element from the reduced residue system modulo m the inverse of a will be a solution of the congruence $ax \equiv 1 (\mathrm{mod}\, m)$:

$x \equiv a^{\varphi(m)-1} (\mathrm{mod}\, m)$.

Therefore, if the modulus m is composite, then the inverse element exists just for **the reduced residue system modulo** m. Thus, for an arbitrary a from mentioned above class the inverse is defined by formula as follows:

$a^{-1} \equiv a^{\varphi(m)-1} (\mathrm{mod}\, m)$.

However, if the modulus is a prime number p then **the reduced residue system modulo** p will coincide with the complete residue

system.

We have come to a conclusion that for any element from **the complete residue system modulo** p the inverse **exists and is a unique:**

$$a^{-1} \equiv a^{p-2} (\mathrm{mod}\, p).$$

Using continued fractions, it will be easy to find the inverse as follows:

$$a^{-1} = (-1)^{n-1} P_{n-1}.$$

Example

Obtain the multiplicative inverse for number $a = 131$ modulo $m = 437$.

Solution

Let us consider the fraction $\frac{a}{m} = \frac{437}{131}$. We are going to expand the fraction via chain of partial quotients. This produces

$$\frac{437}{131} = 3\frac{44}{131}, \quad q_1 = 3; \quad \frac{131}{44} = 2\frac{43}{44}, \quad q_2 = 2; \quad \frac{44}{43} = 1\frac{1}{43}, \quad q_3 = 1;$$

$$\frac{43}{1} = 43, \quad q_4 = 43.$$

Thus $\frac{437}{131} = [3, 2, 1, 43]$.

Then we build a table of convergents.

i	0	1	2	3	4	
q_i		3	2	1	43	
P_i	1	3	7	10	437	m
Q_i	0	1	2	3	131	a

Using their properties, one can write the following:

$$P_4 \cdot Q_3 - P_3 \cdot Q_4 = (-1)^4 \text{ or } \underbrace{437 \cdot 3}_{\equiv 0 (\mathrm{mod}\, 437)} - 10 \cdot 131 = 1.$$

Therefore, we come to a conclusion that

$(-10)\cdot 131 \equiv 1 (\mathrm{mod}\, 437)$.

Finely, we have $131^{-1} \equiv -10 (\mathrm{mod}\, 437)$ or $131^{-1} \equiv 427 (\mathrm{mod}\, 437)$.

Answer

The multiplicative inverse of $a = 131$ modulo $m = 437$ equals $a^{-1} = -10$ (in the absolute least residue system) and corresponds to $a^{-1} = 427$ in the least nonnegative residue system.

10.3. SYSTEM OF LINEAR CONGRUENCES WITH ONE UNKNOWN

Consider a system of congruences involving one unknown with respect to different modulus

$$\begin{cases} a_1 x \equiv b_1 (\mathrm{mod}\, m_1), & (a_1, m_1) = 1, \\ a_2 x \equiv b_2 (\mathrm{mod}\, m_2), & (a_2, m_2) = 1, \\ \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ a_k x \equiv b_k (\mathrm{mod}\, m_k), & (a_k, m_k) = 1. \end{cases} \qquad (1)$$

Let us assume that $m_1, m_2, ..., m_k$ are pairwise prime numbers such that $(m_i, m_j) = 1,\ i = \overline{1,k};\ j = \overline{1,k};\ i \neq j$.

Definition 10.3.1

A solution of the system of congruences with one unknown is an integer α that satisfies all congruences simultaneously.

First, we simplify this system. Since $(a_i, m_i) = 1,\ i = \overline{1,k}$, then there exists the inverse a_i^{-1} for a_i such that $a_i^{-1}:\ a_i \cdot a_i^{-1} \equiv 1 (\mathrm{mod}\, m_i)$. Further, multiplying every system's equation by its own inverse, we obtain the equivalent system

$$\begin{cases} x \equiv c_1 (\mathrm{mod}\, m_1), \\ x \equiv c_2 (\mathrm{mod}\, m_2), \\ \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ x \equiv c_k (\mathrm{mod}\, m_k). \end{cases} \qquad (2)$$

Thus, if we solve the system (2), then we will thereby know the solution to the system (1).

To answer the questions about the existence and structure of the solution of the system (2), we introduce **the Chinese remainder theorem:**

Let $m_1, m_2, ..., m_k$ be pairwise coprime positive integers and let $c_1, c_2, ..., c_k$ be integers satisfying the inequalities $0 \le c_i \le m_i - 1, \quad i = \overline{1,k}$. Then, there exists a unique integer α such that c_i will be the remainder on dividing α by m_i, i. e., $\alpha \equiv c_i \pmod{m_i}$.

Proof

We shall prove the theorem by constructing a number α. Denote by M the gcd of all moduli. Since they are pairwise coprime, then $M = m_1 m_2 ... m_k$. Further, we build a system of numbers as follows:

$$M_i = \frac{M}{m_i} = \frac{m_1 m_2 ... m_i ... m_k}{m_i} = m_1 m_2 ... m_{i-1} m_{i+1} ... m_k, \quad i = \overline{1,k}.$$

Being pairwise coprime with m_i, each M_i has an inverse

$$M_i^{-1} \equiv M_i^{\varphi(m_i)-1} \bmod(m_i).$$

Let us construct the integer $\alpha = \sum_{i=1}^{k} M_i M_i^{-1} c_i$.

It is obvious that the solution to the system (2) is a residue class that satisfies a congruence

$$x \equiv \alpha \pmod{M}.$$

Indeed, let us substitute α to the first congruence of the system (2):

$$M_1 M_1^{-1} c_1 + M_2 M_2^{-1} c_2 + ... + M_k M_k^{-1} c_k \equiv c_1 \pmod{m_1}.$$

Here all terms, starting from the second one, are divided by m_1, since m_1 is a factor of M_i, $i = \overline{2,k}$. Therefore, all of them are

congruent to 0 modulo m_1. As stated above, $M_1 M_1^{-1} \equiv 1 (\mathrm{mod}\, m_1)$ and, consequently, $(M_1, m_1) = 1$. Finally, there will remain only equivalent congruence $c_1 \equiv c_1 (\mathrm{mod}\, m_1)$.

In the second equation, the only term incongruent to 0 modulo m_2 is $M_2 M_2^{-1} c_2$. Thus, α is the solution for the second congruence, etc.

Clearly, the solution, according to its structure, satisfies every congruence in the system.

Conclusion

The solution to the system (2) exists and it is a class of integers $x = \alpha + Mt, \quad t \in Z$.

Consider an example for the solution of the system with several congruences.

Example

Solve a system of congruences

$$\begin{cases} 743x \equiv 16 (\mathrm{mod}\, 13), \\ 59x \equiv 128 (\mathrm{mod}\, 5), \\ 136x \equiv 82 (\mathrm{mod}\, 3). \end{cases}$$

Solution

There is the system of three congruences modulo prime numbers.

STEP 1. Let us simplify the system. We substitute the least residues of appropriate moduli for numbers in each of congruences.

$$\begin{cases} 2x \equiv 3 (\mathrm{mod}\, 13), \\ 4x \equiv 3 (\mathrm{mod}\, 5), \\ x \equiv 1 (\mathrm{mod}\, 3). \end{cases}$$

We bring the system to the type (2):

$$\begin{cases} 2x \equiv 3 + 13 (\mathrm{mod}\, 13) \Rightarrow 2x \equiv 16 (\mathrm{mod}\, 13) \underset{(2,13)=1}{\Rightarrow} x \equiv 8 (\mathrm{mod}\, 13), \\ 4x \equiv 3 + 5 (\mathrm{mod}\, 5) \Rightarrow 4x \equiv 8 (\mathrm{mod}\, 5) \underset{(4,5)=1}{\Rightarrow} x \equiv 2 (\mathrm{mod}\, 5), \\ x \equiv 1 (\mathrm{mod}\, 3). \end{cases}$$

This yields the reduced system as follows:

$$\begin{cases} x \equiv 8 \pmod{13}, \\ x \equiv 2 \pmod{5}, \\ x \equiv 1 \pmod{3}. \end{cases}$$

According to the Chinese remainder theorem, a solution to such system exists, and it is a unique.

STEP 2. Let us consider the first congruence $x \equiv 8 \pmod{13}$. We can rewrite it via such equality:

$$x = 8 + 13t_1. \qquad (*)$$

Since x is a solution for every congruences, we substitute it into the second congruence and deduce value for unknown t_1:

$$8 + 13t_1 = 2 \pmod 5 \Rightarrow 13t_1 \equiv -6 \pmod 5 \Rightarrow$$

$$\Rightarrow 3t_1 \equiv -6 + 5 \cdot 3 \pmod 5 \Rightarrow 3t_1 \equiv 9 \pmod 5.$$

Taking into account that $(3,5) = 1$, we divide both parts of the congruence by 3:

$t_1 \equiv 3 \pmod 5$, this yields $t_1 = 3 + 5t_2$.

Then we substitute t_1 into formula (*); this produces

$$x = 8 + 13(3 + 5t_2) = 8 + 39 + 13 \cdot 5t_2 = 47 + 13 \cdot 5t_2,$$

$$x \equiv 47 \pmod{13 \cdot 5}.$$

We get

$$x = 47 + 13 \cdot 5t_2. \qquad (**)$$

STEP 3. Further, we substitute the obtained above expression for x into the third congruence:

$$47 + 13 \cdot 5t_2 \equiv 1 \pmod 3 \Rightarrow 65t_2 \equiv -46 \pmod 3 \Rightarrow$$

$$\Rightarrow -t_2 \equiv -1 \pmod 3 \Rightarrow t_2 \equiv 1 \pmod 3 \Rightarrow t_2 = 1 + 3t_3.$$

If we replace t_2 by its expression in (**), we obtain

$$x = 47 + 13 \cdot 5(1 + 3t_3) = 47 + 65 + 13 \cdot 5 \cdot 3t_3 = 112 + 13 \cdot 5 \cdot 3t_3 .$$

Thus we have

$$x \equiv 112 \pmod{13 \cdot 5 \cdot 3} \text{ or } x \equiv 112 \pmod{195}.$$

Answer

$$x \equiv 112 \pmod{195}.$$

Solution check

$$\begin{cases} 2 \cdot 112 = 224 = 13 \cdot 17 + 3 \Rightarrow 2 \cdot 112 \equiv 3 \pmod{13}, \\ 4 \cdot 112 = 448 \equiv 3 \pmod{5}, \\ 112 = 3 \cdot 37 + 1 \Rightarrow 112 \equiv 1 \pmod{3}. \end{cases}$$

Solution is correct.

Remark

1. If in the system (1) there is a congruence $a_i x \equiv b_i \pmod{m_i}$ possessing properties $(a_i, m_i) = d > 1$, $d \mid b_i$, then, by dividing it by d, we get an expression $\frac{a_i}{d} x \equiv \frac{b_i}{d} \left(\bmod \frac{m_i}{d} \right)$ and, further, we will substitute the obtained congruence into the system.

If in the new deduced system moduli are still pairwise coprimes, then, according to the Chinese remainder theorem, such system possesses a unique solution. But in this case an i-th congruence has just d solutions: $x \equiv c_i + t_j \frac{m_i}{d} \pmod{m_i}$, $t_j = \overline{0,(d-1)}$. Therefore, it is necessary to consider d systems, having an appropriate solution of congruence in the system's *i*-th position.

2. A system of two equations

$$\begin{cases} x \equiv c_1 \pmod{m_1}, \\ x \equiv c_2 \pmod{m_2} \end{cases}$$

is solvable iff two conditions hold $(m_1, m_2) = d > 1$ and $d \mid c_2 - c_1$. Otherwise, the system has no solutions. In the case conditions are

met and a solution exists, then it will be found by modulo gcd of m_1 and m_2.

3. If a system contains more than two congruences **(**$k > 2$) with modules having gcd greater than 1, then we must check its solution step-by-step. When at least one of obtained congruences is nonsolvable, then such system is inconsistent at all. If the solution exists, then it will be congruent modulo gcd of all moduli.

PROBLEMS FOR UNIT 10

Problem 1

Obtain inverse for a **modulo** m**.**

1. $a = 142,$ $m = 439$	2. $a = 137,$ $m = 932$	3. $a = 95,$ $m = 308$	4. $a = 37,$ $m = 107$	5. $a = 37,$ $m = 217$	6. $a = 113,$ $m = 311$
7. $a = 221,$ $m = 367$	8. $a = 41,$ $m = 101$	9. $a = 31,$ $m = 142$	10. $a = 93,$ $m = 133$	11. $a = 23,$ $m = 691$	12. $a = 137,$ $m = 323$
13. $a = 97,$ $m = 323$	14. $a = 101,$ $m = 931$	15. $a = 103,$ $m = 1031$	16. $a = 91,$ $m = 323$	17. $a = 137,$ $m = 837$	18. $a = 59,$ $m = 311$
19. $a = 97,$ $m = 433$	20. $a = 113,$ $m = 923$	21. $a = 89,$ $m = 323$	22. $a = 47,$ $m = 311$	23. $a = 67,$ $m = 691$	24. $a = 64,$ $m = 531$
25. $a = 64,$ $m = 743$	26. $a = 71,$ $m = 531$	27. $a = 83,$ $m = 323$	28. $a = 93,$ $m = 531$	29. $a = 128,$ $m = 1025$	30. $a = 29,$ $m = 531$

Problem 2

Solve the system of congruences, simplifying it first.

1. $\begin{cases} 913x \equiv 132 \pmod{17}, \\ 138x \equiv 245 \pmod{19}, \\ 457x \equiv 623 \pmod{13}. \end{cases}$

2. $\begin{cases} 913x \equiv 132 \pmod{23}, \\ 138x \equiv 245 \pmod{11}, \\ 457x \equiv 623 \pmod{17}. \end{cases}$

3. $\begin{cases} 913x \equiv 132 \pmod{29}, \\ 138x \equiv 245 \pmod{17}, \\ 457x \equiv 623 \pmod{23}. \end{cases}$

4. $\begin{cases} 253x \equiv 429 \pmod{17}, \\ 338x \equiv 545 \pmod{19}, \\ 579x \equiv 741 \pmod{13}. \end{cases}$

5. $\begin{cases} 253x \equiv 429 \pmod{31}, \\ 338x \equiv 545 \pmod{23}, \\ 579x \equiv 741 \pmod{19}. \end{cases}$

6. $\begin{cases} 253x \equiv 429 \pmod{37}, \\ 338x \equiv 545 \pmod{29}, \\ 579x \equiv 741 \pmod{23}. \end{cases}$

7. $\begin{cases} 353x \equiv 529 \pmod{17}, \\ 138x \equiv 945 \pmod{19}, \\ 279x \equiv 241 \pmod{13}. \end{cases}$

8. $\begin{cases} 353x \equiv 529 (mod\ 31), \\ 137x \equiv 945 (mod\ 23), \\ 279x \equiv 241 (mod\ 17). \end{cases}$

9. $\begin{cases} 353x \equiv 529 (mod\ 37), \\ 137x \equiv 945 (mod\ 17), \\ 279x \equiv 241 (mod\ 23). \end{cases}$

10. $\begin{cases} 347x \equiv 519 (mod\ 17), \\ 438x \equiv 345 (mod\ 29), \\ 271x \equiv 541 (mod\ 37). \end{cases}$

11. $\begin{cases} 347x \equiv 519 (mod\ 31), \\ 438x \equiv 327 (mod\ 23), \\ 271x \equiv 541 (mod\ 19). \end{cases}$

12. $\begin{cases} 347x \equiv 519 (mod\ 37), \\ 438x \equiv 327 (mod\ 17), \\ 271x \equiv 541 (mod\ 23). \end{cases}$

13. $\begin{cases} 547x \equiv 219 (mod\ 17), \\ 639x \equiv 175 (mod\ 29), \\ 371x \equiv 341 (mod\ 37). \end{cases}$

14. $\begin{cases} 547x \equiv 219 (mod\ 31), \\ 638x \equiv 145 (mod\ 23), \\ 371x \equiv 341 (mod\ 19). \end{cases}$

15. $\begin{cases} 547x \equiv 219 (mod\ 37), \\ 638x \equiv 145 (mod\ 17), \\ 371x \equiv 341 (mod\ 23). \end{cases}$

16. $\begin{cases} 747x \equiv 319 \pmod{17}, \\ 838x \equiv 195 \pmod{29}, \\ 571x \equiv 241 \pmod{37}. \end{cases}$

17. $\begin{cases} 747x \equiv 319 \pmod{31}, \\ 838x \equiv 195 \pmod{23}, \\ 571x \equiv 241 \pmod{19}. \end{cases}$

18. $\begin{cases} 747x \equiv 319 \pmod{37}, \\ 838x \equiv 195 \pmod{17}, \\ 571x \equiv 241 \pmod{23}. \end{cases}$

19. $\begin{cases} 437x \equiv 719 \pmod{17}, \\ 925x \equiv 395 \pmod{29}, \\ 771x \equiv 225 \pmod{37}. \end{cases}$

20. $\begin{cases} 437x \equiv 719 \pmod{31}, \\ 925x \equiv 395 \pmod{23}, \\ 771x \equiv 225 \pmod{41}. \end{cases}$

21. $\begin{cases} 437x \equiv 719 \pmod{37}, \\ 925x \equiv 395 \pmod{17}, \\ 771x \equiv 225 \pmod{23}. \end{cases}$

22. $\begin{cases} 333x \equiv 579 \pmod{17}, \\ 1025x \equiv 495 \pmod{29}, \\ 797x \equiv 245 \pmod{37}. \end{cases}$

23. $\begin{cases} 333x \equiv 579 \pmod{31}, \\ 1025x \equiv 495 \pmod{23}, \\ 797x \equiv 245 \pmod{41}. \end{cases}$

24. $\begin{cases} 337x \equiv 525 (mod\ 37), \\ 1025x \equiv 495 (mod\ 17), \\ 797x \equiv 245 (mod\ 23). \end{cases}$

25. $\begin{cases} 733x \equiv 571 (mod\ 17), \\ 625x \equiv 405 (mod\ 29), \\ 707x \equiv 295 (mod\ 37). \end{cases}$

26. $\begin{cases} 733x \equiv 571 (mod\ 31), \\ 625x \equiv 405 (mod\ 23), \\ 707x \equiv 295 (mod\ 19). \end{cases}$

27. $\begin{cases} 733x \equiv 571 (mod\ 37), \\ 625x \equiv 405 (mod\ 17), \\ 707x \equiv 295 (mod\ 23). \end{cases}$

28. $\begin{cases} 398x \equiv 171 (mod\ 17), \\ 925x \equiv 605 (mod\ 29), \\ 507x \equiv 395 (mod\ 37). \end{cases}$

29. $\begin{cases} 398x \equiv 171 (mod\ 31), \\ 925x \equiv 605 (mod\ 19), \\ 507x \equiv 395 (mod\ 11). \end{cases}$

30. $\begin{cases} 398x \equiv 171 (mod\ 11), \\ 925x \equiv 605 (mod\ 13), \\ 507x \equiv 395 (mod\ 41). \end{cases}$

REFERENCES

1. Clark W. Edwin. Elementary Number Themory / W. Edwin Clark. – University of South Florida, 2002. – Dec.

2. Stein W. Elementary Number Theory / W. Stein. – Harvard University, 2004 – Sept.

3. Sato Naoki. Number Theory – Naoki Sato [Електронний ресурс]. – Режим доступу : safo@problemsolvings.com.

4. Collins Darren C. Continued Fraction / Darren C. Collins // MIT Undegraduate Journal of Mathematics.

Навчальне видання

Елементи теорії чисел
Конспект лекцій та контрольні завдання
для студентів напрямів підготовки
6.04030101 „Прикладна математика”
та 6.040302 „Інформатика”
усіх форм навчання

(Англомовний курс)

Відповідальний за випуск Л. А. Фильштинський
Редактор С. В. Чечоткіна
Комп’ютерне верстання Ю. В. Шрамко

Формат 60×84/16. Ум. друк. арк. 4,19. Обл.-вид. арк. 4,78.

Видавець і виготовлювач
Сумський державний університет,
вул. Римського-Корсакова, 2, м. Суми, 40007
Свідоцтво суб’єкта видавничої справи ДК № 3062 від 17.12.2007.