

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE SUMY STATE UNIVERSITY

## "ELEMENTARY NUMBER THEORY" lecture notes with tests <br> for students of specialties "Informatics" and "Applied Mathematics"

## 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<br>Department of Applied and<br>Computational Mathematics<br>as the abstract of lecture notes<br>for the discipline "Elementary<br>number theory"<br>Record № 10 from 19.05.2015

## Sumy <br> Sumy State University <br> 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 $n|m \Rightarrow d| m$.
7. (Multiplication property) $d \mid n \Rightarrow$ for any $a \in Z: d \mid a \cdot n$.
8. (Linearity property) $d \mid n$ and $d|m \Rightarrow d| a \cdot n+b \cdot m$ 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 $d|a, d| b$ 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 $d||a|$.
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 $2 x+3 y$ is divisible by 17 if and only if (iff) $9 x+5 y$ is divisible by 17 .

## Solution

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

Further, we decompose the right side into sum as follows:
$17|(17 x+34 y+9 x+5 y) \Rightarrow 17| 17 \cdot(x+2 y)+(9 x+5 y)$.
Finally, according to integration property in theorem 1.1, we have $17 \mid(9 x+5 y)$.

And conversely, producing the similar set of operations, we obtain

$$
\begin{aligned}
& 17|(9 x+5 y) \Rightarrow 17|[4(9 x+5 y)], \\
& \text { or } 17|(36 x+20 y) \Rightarrow 17|(34 x+17 y+2 x+3 y) \Rightarrow \\
& \quad 17 \mid 17(2 x+y)+2 x+3 y . \\
& \text { Thus we have proved that } 17 \mid 2 x+3 y .
\end{aligned}
$$

## Example 1.2

Prove that for any integer $m, p, q, n$ such that $(m-p) \mid(m n+p q)$ is an integer, $(m-p) \mid(m q+n p)$ is also the integer.

## Solution

Let $(m-p) \mid(m q+n p)$ be an integer. We can denote this in similar way: $\frac{m n+p q}{m-p}=t_{1} \in Z$.

It is necessary to prove that $\frac{m q+n p}{m-p}=t_{2} \in Z$ or $t_{1}-t_{2} \in Z$. Let us show this. We obviously obtain:

$$
\frac{m n+p q}{m-p}-\frac{m q+n p}{m-p}=\frac{m(n-q)-p(n-q)}{m-p}=\frac{(m-p)(n-q)}{m-p}=n-q \in Z
$$

Therefore $t_{1}-t_{2} \in Z$ and, finally, $\frac{m q+n p}{m-q}=t_{2} \in Z$.

## Example 1.3

$N$ is a five-digit number $N=a_{4} a_{3} a_{2} a_{1} a_{0}, 0 \leq a_{i} \leq 9$. 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

$$
N=10^{4} a_{4}+10^{3} a_{3}+10^{2} a_{2}+10 a_{1}+a_{0}
$$

Let us shift the last digit $a_{0}$ to the first position, as follows: $N_{1}=10^{4} a_{0}+10^{3} a_{4}+10^{2} a_{3}+10 a_{2}+a_{1}$. 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

$$
10 N_{1}=10^{5} a_{0}+10^{4} a_{4}+10^{3} a_{3}+10^{2} a_{2}+10 a_{1}
$$

Then add and subtract $a_{0}$. It yields: $10 N_{1}=10^{5} a_{0}+10^{4} a_{4}+10^{3} a_{3}+10^{2} a_{2}+10 a_{1}+a_{0}-a_{0}$.

By combining the first and last terms of expression, we obtain the number $N$ as a summand: $10 N_{1}=a_{0}\left(10^{5}-1\right)+N=99999 a_{0}+N$.

Further, taking into account that
$41\left|N, \quad 99999=9 \cdot 11111, \frac{11111}{41}=271 \Rightarrow 41\right| 99999$,
we come to conclusion that in the right side both terms are multiples of 41. Thus $41\left|10 N_{1} \Rightarrow 41\right| N_{1}$

## 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:

$$
\begin{aligned}
& \quad\left(m^{5}-m\right)=m\left(m^{4}-1\right)=m\left(m^{2}-1\right)\left(m^{2}+1\right)= \\
& =(m-1) m(m+1)\left(m^{2}-4+5\right)=(m-1) m(m+1)\left(m^{2}-4\right)+ \\
& +5(m-1) m(m+1)=(m-2)(m-1) m(m+1)(\mathrm{m}+2)+5(m-1) m(m+1) . \\
& \left.\frac{(m-2)(m-1) m(m+1)(m+2)}{5!} \in Z \Rightarrow 30 \right\rvert\,(m-2)(m-1) m(m+1)(m+2)
\end{aligned}
$$

And finally, for the second case, we obtain

$$
\begin{aligned}
& \frac{(m-1) m(m+1)}{3!}=\frac{(m-1) m(m+1)}{6} \in \mathrm{Z} \Rightarrow \\
& \Rightarrow 6|(m-1) m(m+1) \Rightarrow 30| 5(m-1) m(m+1)
\end{aligned}
$$

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. $N=\overline{a_{5} a_{4} a_{3} a_{2} a_{1} a_{0}}, 0 \leq a_{i} \leq 9, a_{0}=5$. If we rearrange last digit $a_{0}=5$ to the first place, we will get $N_{1}=4 N$. Find this number $N$.

## Problem 1.3

Prove that

1. $6 \mid n(n+1)(2 n+1)$.
2. $30 \mid m n\left(m^{4}-n^{4}\right)$.

## Problem 1.4

Prove that
$2^{n} \mid(n+1)(n+2) \cdot \ldots \cdot(n+n)$

## 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 $p^{\alpha+l} \downarrow a$, then $\alpha$ 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 $\alpha_{i}$ 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 $N=p_{1} p_{2} \cdot p_{n}+1$. 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 $D=\left\{p_{1}^{\beta_{1}} \cdot p_{2}^{\beta_{2}} \cdot p_{3}^{\beta_{3}} \cdot \ldots \cdot p_{k}^{\beta_{k}}, 0 \leq \beta_{i} \leq \alpha_{i}, i=\overline{1, k}\right\}$.

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

$$
\tau(a)=\left(\alpha_{1}+1\right)\left(\alpha_{2}+1\right) \cdot \ldots \cdot\left(\alpha_{k}+1\right)
$$

## Theorem 2.3

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

## 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
$n \leq p \leq 2 n$.

## 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. $0 \leq r<b$.

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:

$$
N=10^{n} a_{n}+10^{n-1} a_{n-1}+\ldots+10^{3} a_{3}+10^{2} a_{2}+10 a_{1}+a_{0} .
$$

We don't know digits $a_{n}, a_{n-1}, \ldots, a_{3}, a_{2}, a_{1}, a_{0}$, but we can analyze remainders of the division of $10^{i}(i=0,1, \ldots, n)$ by some numbers.

1. Criteria for divisibility of $N$ by $2^{k}$

- Divisibility by 2

Obviously, the number $10^{n} a_{n}+10^{n-1} a_{n-1}+\ldots+10 a_{1}$ is divisible by 2 . If $\mathbf{a}_{0}$ 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 $10 a_{1}+a_{0}$ 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 $10^{2} a_{2}+10 a_{1}+a_{0}$ 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 $\boldsymbol{N}$ by 3 and 9

We can rewrite number $N$ as follows:

$$
\begin{aligned}
& N=\underbrace{999 \ldots 9}_{n} a_{n}+\underbrace{999 \ldots 9}_{n-1} a_{n-1}+\ldots+99 a_{2}+9 a_{1}
\end{aligned} a_{n}+a_{n-1}+\ldots+a_{1}+a_{0}=.
$$

It is evident that $9\left|N_{1}, 3\right| N_{1}$
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 $\boldsymbol{N}$ by $\boldsymbol{5}^{\boldsymbol{k}}$

$$
N=10^{n} a_{n}+10^{n-1} a_{n-1}+\ldots+10^{3} a_{3}+10^{2} a_{2}+10 a_{1}+a_{0} .
$$

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 $\boldsymbol{N}$ by 7

$$
N=10^{n} a_{n}+10^{n-1} a_{n-1}+\ldots+10^{3} a_{3}+10^{2} a_{2}+10 a_{1}+a_{0} .
$$

Consider remainders of division of ten's powers by 7 . We have $10: 10=1 \cdot 7+3$, the remainder is 3
$10^{2}: 100=14 \cdot 7+2$, the remainder is 2
$\mathbf{1 0}^{\mathbf{3}}: 1000=142 \cdot 7+6=\mathbf{1 4 3 \cdot 7} \mathbf{- 1}$, the remainder is 6 or $\mathbf{- 1}$
$10^{4}: 10000=1428 \cdot 7+4$, the remainder is 4
$10^{5}: 100000=14285 \cdot 7+5$, the remainder is 5
$10^{6}: 1000000=142857 \cdot 7+1$, the remainder is $\mathbf{1}$
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
$N=100 a_{2}+10 a_{1}+a_{0}=98 a_{2}+2 \mathrm{a}_{2}+7 a_{1}+3 a_{1}+a_{0}=98 a_{2}+7 a_{1}+$ $+2 a_{2}+3 a_{1}+a_{0}=7\left(14 a_{2}+a_{1}\right)+2 a_{2}+3 a_{1}+a_{0}$.

If $2 a_{2}+3 a_{1}+a_{0}$ 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

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

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

## b. Criteria for $\boldsymbol{n}$-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:

$$
\begin{aligned}
& \quad N=a_{2} a_{1} a_{0}+10^{3} a_{5} a_{4} a_{3}+10^{6} a_{8} a_{7} a_{6}+\ldots= \\
& =a_{2} a_{1} a_{0}+143 \cdot 7 a_{5} a_{4} a_{3}-a_{5} a_{4} a_{3}+142857 \cdot 7 a_{8} a_{7} a_{6}+a_{8} a_{7} a_{6}+\ldots= \\
& \underbrace{143 \cdot 7 a_{5} a_{4} a_{3}+142857 \cdot 7 a_{8} a_{7} a_{6}+\ldots}_{N_{1}: 7}+\underbrace{a_{2} a_{1} a_{0}-a_{5} a_{4} a_{3}+a_{8} a_{7} a_{6}-\ldots}_{N_{2}} \\
& N=\overline{a_{n} \ldots \underbrace{a_{8} a_{7} a_{6}}_{+} \underbrace{a_{5} a_{4} a_{3}}_{-} \underbrace{a_{2} a_{1} a_{0}}_{+}}, \quad N_{2}=a_{2} a_{1} a_{0}-a_{5} a_{4} a_{3}+a_{8} a_{7} a_{6}-\ldots
\end{aligned}
$$

If $N_{2}$ is divisible by 7 , then $N$ is divisible by 7 too.

## Example 3.2

Check if the number $N=23161320$ is divisible by 7.
Solution

$$
N_{2}=320-161+23=182.182: 7=26 . \text { So, } N=23161320 \text { is }
$$ divided by 7. We have $23161320: 7=3308760$.

## 5. Criteria for divisibility of $\boldsymbol{N}$ by 11

$$
N=10^{n} a_{n}+10^{n-1} a_{n-1}+\ldots+10^{3} a_{3}+10^{2} a_{2}+10 a_{1}+a_{0}
$$

Consider the remainders of the division of ten's powers by 11 .
$\mathbf{1 0}: 10=0 \cdot 11+10=\mathbf{1} \cdot \mathbf{1 1} \mathbf{- 1}$, the remainder is 10 or $\mathbf{- 1}$
$10^{2}: 100=9 \cdot 11+1$, the remainder is $\mathbf{1}$
$\mathbf{1 0}^{\mathbf{3}}: 1000=90 \cdot 11+10=\mathbf{9 1} \cdot \mathbf{1 1} \mathbf{- 1}$, the remainder is 10 or $\mathbf{- 1}$
$10^{4}: 10000=901 \cdot 11+1$, the remainder is 1

$$
N=\overline{a_{n} \ldots a_{5} a_{4} a_{3} a_{2} a_{1} a_{0}}, \quad N_{2}=a_{0}-a_{1}+a_{2}-a_{3}+\ldots
$$

If $N_{2}$ is divisible by 11 , then $N$ will be divisible by 11 too.

## Example 3.3

Check if the numbers $N=23161320$ and $N=1186680$ are divisible by 11 .

Solution

1) $N_{2}=0-2+3-1+6-1+3-2=6$. It isn't divisible by 11 . So, $N=23161320$ isn't divisible too.
2) $N_{2}=0-8+6-6+8-1+1=0$. It is divisible by 11 , therefore $N=1186680$ is divisible by 11 too.
6. Criteria for divisibility of $\boldsymbol{N}$ by 13

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

## Example 3.4

Check that $N=3040232$ is divisible by 13 .

## Solution

$232-40+3=195.195: 13=15$. Then 3040232 is divisible by 13.
7. Criteria for divisibility of $\boldsymbol{N}$ by $\boldsymbol{d}=10 \boldsymbol{k}+1(31,41,61, \ldots)$

$$
N=\underbrace{\overline{a_{n} \ldots a_{3} a_{2} a_{1} a_{0}}}_{A}=10 A+a_{0} .
$$

Multiply $N$ by $k$ : $k N=10 k A+k a_{0}+A-A=A(10 k+1)-\left(A-k a_{0}\right)$.
Since $k$ isn't divisible by $10 k+1$, we see that $N$ will be divisible by $10 k+1$ if $N_{2}=A-k a_{0}$ is a multiple of $10 k+1$.

This criterion can be applied until the divisibility or lack of it become apparent.
8. Criteria for divisibility of $\boldsymbol{N}$ by $\boldsymbol{d}=10 \boldsymbol{k}-1(19,29,59, \ldots)$

$$
N=\underbrace{\overline{a_{n} \ldots a_{3} a_{2} a_{1} a_{0}}}_{A}=10 A+a_{0} .
$$

Multiply $N$ by $k$ :

$$
k N=10 k A+k a_{0}+A-A=A(10 k-1)+\left(A+k a_{0}\right) .
$$

Since $k$ isn't divisible by $10 k-1$, it follows that $N$ will be divisible by $10 k-1$ if $N_{2}=A+k a_{0}$ is a multiple of $10 k+1$.

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

## Example 3.5

Check that $N=3040232$ is divisible by 31 .

## Solution

Here, the divisor is 31 , then it is necessary to use the eighth criteria. We get
$31=10 \cdot 3+1, k=3, A=304023, a_{0}=2$.
If $N_{2}=A-3 a_{0}$ is divisible by 31 , then $N$ is divisible by 31:

1. $N_{2}=304023-3 \cdot 2=304017$.
2. $A=30401, a_{0}=7,30401-3 \cdot 7=30380$.
3. $A=3038, a_{0}=0,3038-3 \cdot 0=3038$.
4. $A=303, a_{0}=8,303-3 \cdot 8=279$.
5. $A=17, a_{0}=9,27-3 \cdot 9=0$.

It is clear that 0 is divisible by 31 , so $N=3040232$ is divisible by 31 too. $3040232: 31=98072$.

## Problems for Unit 3

### 3.1. Check that a is divisible by $m$

| $\boldsymbol{m}=\mathbf{3 5}$ |  | $\boldsymbol{m}=\mathbf{3 9}$ |  | $\boldsymbol{m}=\mathbf{5 5}$ |  |
| :--- | :--- | :--- | :--- | :--- | :--- |
| 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. | $a=1200485$ |
| $\boldsymbol{m}=\mathbf{3 1}$ |  | $\boldsymbol{m}=\mathbf{9 1}$ |  | $\boldsymbol{m}=\mathbf{2 9}$ |  |
| 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 $C\left(a_{1}, a_{2}, \ldots, a_{n}\right)$.

## 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 $C\left(a_{1}, a_{2}, \ldots, a_{n}\right)$, except that $\operatorname{gcd}(0,0)=0$.

Denotation of the greatest common divisor for integers $a_{1}, a_{2}, \ldots, a_{n}$ is

$$
\operatorname{gcd}\left(a_{1}, \ldots, a_{n}\right)
$$

## Example 4.2

For results obtained in Example 4.1, we have

1. $\operatorname{gcd}(18,30)$ is the largest integer from the set $C(18,30)=\{-1,1,-2,2,-3,3,-6,6\}$. Then $\operatorname{gcd}(18,30)=6$.
2. $\operatorname{gcd}(10,30,100,130)$ is the largest integer from the set $C(10,30,100,130)=\{-1,1,-2,2,-5,5,-10,10\}$. Then $\operatorname{gcd}(10,30$, $100,130)=10$.

## Definition 4.3

If $\operatorname{gcd}\left(a_{1}, a_{2}, \ldots, a_{n}\right)=1$, 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 $\left(a_{i}, a_{j}\right)(i, j=1,2, \ldots, n)$ from integers $a_{1}, a_{2}, \ldots, a_{n}$ are equal 1 , then $a_{1}, a_{2}, \ldots, a_{n}$ 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 $\operatorname{gcd}(5,15,21,31)=1$. But $\operatorname{gcd}(5,15)=5 \neq 1, \operatorname{gcd}(15,21)=3 \neq 1$.

Gcd $(3,7,11,13)=1$, then numbers $(3,7,11,13)$ are coprime, and $\quad \operatorname{gcd}(3,7)=1, \quad \operatorname{gcd}(3,11)=1, \quad \operatorname{gcd}(3,13)=1, \quad \operatorname{gcd}(7,11)=1$, $\operatorname{gcd}(7,13)=1, \operatorname{gcd}(11,13)=1$. Thus, the numbers are pairwise prime numbers.
Lemma 4.1

$$
\operatorname{gcd}(a, b)=\operatorname{gcd}(b, a) .
$$

Lemma 4.2

$$
\operatorname{gcd}(a, b)=\operatorname{gcd}(|a|,|b|) .
$$

## Lemma 4.3

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

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

## Example 4.4

It follows from considered lemmas that $\operatorname{gcd}(48,732)=$ $=\operatorname{gcd}(-48,732)=\operatorname{gcd}(-48,-732)=\operatorname{gcd}(48,-732)$. We also know that $0<\operatorname{gcd}(48,732) \leq 48$. If $d=\operatorname{gcd}(48,732)$, 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 $g=\operatorname{gcd}(a, b)$, then $\operatorname{gcd}(a / g, b / g)=1$.

## Examples 4.5

$$
g=\operatorname{gcd}(15,21)=3, \operatorname{gcd}(15 / 3,21 / 3)=\operatorname{gcd}(5,7)=1 .
$$

## 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

$$
\operatorname{gcd}(a, b)=s a+t b
$$

## 5. THE EUCLIDEAN ALGORITHM

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

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

## Lemma 5.1

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

## Lemma 5.2

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

## Lemma 5.3

Let $a>b>0$. If $a=b q+r$, then $\operatorname{gcd}(a, b)=\operatorname{gcd}(b, r)$.

## Proof.

If we show that the two sets of common divisors $C(a, b)$ and $\mathrm{C}(b, r)$ 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 $r=a-b q$.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 $a=b q+r$, 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: $a=b \cdot q_{0}+r_{1}, \quad 0<r_{1}<b, \quad \operatorname{gcd}(a, b)=\operatorname{gcd}\left(b, r_{1}\right)$;
Step 2: $b=r_{1} \cdot q_{1}+r_{2}, \quad 0<r_{2}<r_{1}, \quad \operatorname{gcd}\left(b, r_{1}\right)=\operatorname{gcd}\left(r_{1}, r_{2}\right) \Rightarrow$
$\Rightarrow \operatorname{gcd}(a, b)=\operatorname{gcd}\left(r_{1}, r_{2}\right)$;
Step 3: $r_{1}=r_{2} \cdot q_{2}+r_{3}, \quad 0<r_{3}<r_{2}, \quad \operatorname{gcd}\left(r_{1}, r_{2}\right)=\operatorname{gcd}\left(r_{2}, r_{3}\right) \Rightarrow$ $\Rightarrow \operatorname{gcd}(a, b)=\operatorname{gcd}\left(r_{2}, r_{3}\right)$

Step $n: r_{n-2}=r_{n-1} \cdot q_{n-1}+r_{n}, \quad 0<r_{n}<r_{n-1}, \quad \operatorname{gcd}\left(r_{n-2}, \quad r_{n-1}\right)=$ $=\operatorname{gcd}\left(r_{n-1}, r_{n}\right) \Rightarrow \operatorname{gcd}(a, b)=\operatorname{gcd}\left(r_{n-1}, r_{n}\right)$;
Step $n+1: \quad r_{n-1}=r_{n} \cdot q_{n}$
Since there is no remainder in the last division, we get $\operatorname{gcd}\left(r_{n-1}, r_{n}\right)=$ $=r_{n} \Rightarrow \operatorname{gcd}(\boldsymbol{a}, \boldsymbol{b})=\boldsymbol{r}_{\boldsymbol{n}}$.

One can say that for any numbers $\boldsymbol{a}$ and $\boldsymbol{b}$ the last nonzero remainder in a chain of division with the remainders is $\operatorname{gsd}(\boldsymbol{a}, \boldsymbol{b})$.

## Example 5.1

Compute $\operatorname{gcd}(803,154), a=803, b=154$
Step 1: $\operatorname{gcd}(803,154)=\operatorname{gcd}(154,33)$, since $803=154 \cdot 5+33$, $a=b q_{0}+r_{1}, q_{0}=5, r_{1}=33, \quad 0<33<154$.
Step 2: $\operatorname{gcd}(154,33)=\operatorname{gcd}(33,22)$, since $154=33 \cdot 4+22$, $b=r_{1} q_{1}+r_{2}, q_{1}=4, r_{2}=22, \quad 0<22<33$.
Step 3: $\operatorname{gcd}(33,22)=\operatorname{gcd}(22,11)$ since $33=22 \cdot 1+11$, $r_{1}=r_{2} q_{2}+r_{3}, q_{2}=1, r_{3}=11, \quad 0<11<22$.
Step 4: $\quad \operatorname{gcd}(22,11)=11$ since $22=11 \cdot 2, r_{2}=r_{3} q_{3}, q_{3}=2, r_{4}=0$.

Hence, $\operatorname{gcd}(803,154)=\operatorname{gcd}(22,11)=11$.
Recall that Bezout's lemma asserts that for given $a$ and $b$, there exist two numbers $s$ and $t$ such that $\operatorname{gcd}(a, b)=s \cdot a+t \cdot b$. We can use Euclidean algorithm to find $s$ and $t$ by tracing the steps of division in reverse order.

## Example 5.2

Express $\operatorname{gcd}(803,154)$ as a linear combination of 803 and 154. We will use the considered above Example 5.1.
From step 3:
From step 2:

$$
11=33-22 \cdot 1
$$

$=-b \cdot 1+33 \cdot 5$;
From step 1:

$$
22=b-33 \cdot 4, \text { or } \quad 11=33-(b-33 \cdot 4) 1=
$$

$=-26 \cdot b+a \cdot 5$.
Hence, we can express $\operatorname{gcd}(803,154)=11$ as a linear combination of 803 and 154 as follows below:

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

## Lemma 5.4 (Generalization)

Let

$$
\begin{aligned}
& a_{0}=c q_{0}+r_{0}, \quad a_{1}=c q_{1}+r_{1}, \ldots, a_{n}=c q_{n}+r_{n} \Rightarrow \\
\Rightarrow & \operatorname{gcd}\left(a_{0}, a_{1}, \ldots, a_{n}, c\right)=\operatorname{gcd}\left(c, r_{0}, r_{1}, \ldots, r_{n}\right) .
\end{aligned}
$$

## Example 5.3

Compute $\operatorname{gcd}(261,135,48)$.
Step 1: Divide $a_{0}=261$ and $a_{1}=135$ by $c=48$. We get: $261=48 \cdot 5+$ $+21, r_{10}=21 ; \quad 135=48 \cdot 2+39, r_{11}=39$.
Step 2: Find $\operatorname{gcd}(48,39,21)$. 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 $\operatorname{gcd}(21,18,6)$. 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. $\operatorname{Gcd}(18,6)=6$.
Step 4: Find $\operatorname{gcd}(6,3): \operatorname{gcd}(6,3)=3$.
Hence, $\operatorname{gcd}(261,135,48)=3$.

## 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 $\boldsymbol{M}\left(\boldsymbol{a}_{1}, \boldsymbol{a}_{2}, \ldots, \boldsymbol{a}_{\boldsymbol{n}}\right)$ the set of numbers that are common multiples of $\boldsymbol{a}_{1}, \boldsymbol{a}_{2}, \ldots, \boldsymbol{a}_{\boldsymbol{n}}$. 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 $M\left(a_{1}, a_{2}, \ldots, a_{n}\right)$.

Designation of the lowest common multiple for integers $a_{1}, a_{2}, \ldots, a_{n}$ is $\operatorname{lcm}\left(\boldsymbol{a}_{1}, \ldots, \boldsymbol{a}_{\boldsymbol{n}}\right)$.

## Lemma 6.1

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

## Proof

Let $d=\operatorname{gcd}(a, b)$, then $a=a_{1} \cdot d$, and $b=b_{1} \cdot d, \operatorname{gcd}\left(a_{1}, b_{1}\right)=1$ (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

$$
\frac{M}{b}=\frac{k a}{b}=\frac{k a_{1} d}{b_{1} d}=\frac{k a_{1}}{b_{1}}
$$

Since $\operatorname{gcd}\left(a_{1}, b_{1}\right)=1$, we see that $k$ is divisible by $b_{1}$ and $k=b_{1} \cdot t, t \in Z$.

$$
\frac{M}{b}=\frac{k a_{1}}{b_{1}}=\frac{b_{1} t a_{1}}{b_{1}}=t a_{1}, M=a_{1} \cdot b \cdot t=\frac{a_{1} \cdot b \cdot d}{d} t=\frac{a \cdot b}{d} t, t \in Z .
$$

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

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

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

$$
\operatorname{Lcm}(a, b)=\frac{a \cdot b}{g c d(a, b)} . \text { QED. }
$$

## Problems for Unit 6

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

| $\text { 1. } \quad \begin{aligned} & a=1232, \\ & b=1672 \end{aligned}$ | $\text { 2. } \begin{aligned} & a=1329, \\ & b=2136 \end{aligned}$ | $\text { 3. } \quad \begin{aligned} & a=1359 \\ & b=8211 \end{aligned}$ |
| :---: | :---: | :---: |
| $\text { 4. } \quad \begin{aligned} & a=5427, \\ & b=32877 \end{aligned}$ | $\text { 5. } \begin{aligned} & a=5894 \\ & b=3437 \end{aligned}$ | $\begin{gathered} 6 . \quad a=12606, \\ b=6494 \end{gathered}$ |
| $\text { 7. } \begin{aligned} & a=29719, \\ & b=76501 \end{aligned}$ | $\begin{array}{r} \text { 8. } a=162891, \\ b=32176 \end{array}$ | $\text { 9. } \begin{gathered} a=469459, \\ b=579203 \end{gathered}$ |
| $\text { 10. } \begin{aligned} & a=738089 \\ & b=3082607 \end{aligned}$ | $\text { 11. } \begin{aligned} & a=179370199, \\ & b=4345121 \end{aligned}$ | $\text { 12. } \quad a=3327449, ~ 子 ~ b=6314153$ |
| $\text { 13. } \begin{aligned} & a=12870, \\ & b=7650 \end{aligned}$ | $\begin{aligned} & \text { 14. } a=41382 \\ & b=103818 \end{aligned}$ | $\text { 15. } \quad \begin{aligned} & a=3640 \\ & b=14300 \end{aligned}$ |
| $\text { 16. } \begin{aligned} & a=24700, \\ & b=33250 \end{aligned}$ | $\text { 17. } \begin{aligned} & a=7650 \\ & b=25245 \end{aligned}$ | $\text { 18. } \begin{aligned} & a=56595 \\ & b=82467 \end{aligned}$ |
| $\text { 19. } \begin{aligned} & a=35574 \\ & b=192423 \end{aligned}$ | $\text { 20. } \begin{aligned} & a=25245 \\ & b=129591 \end{aligned}$ | $\text { 21. } \begin{aligned} & a=10140 \\ & b=92274 \end{aligned}$ |
| $\text { 22. } \begin{aligned} & a=36372, \\ b & =147220 \end{aligned}$ | $\text { 23. } \begin{aligned} a & =46550, \\ b & =37730 \end{aligned}$ | $\text { 24. } \begin{aligned} & a=1403, \\ b & =1058 \end{aligned}$ |
| $\text { 25. } \begin{aligned} a & =213239, \\ b & =512525 \end{aligned}$ | $\text { 26. } \begin{array}{r} a=138285 \\ b=356405 \end{array}$ | $\text { 27. } \begin{aligned} & a=72348, \\ & b=5632 \end{aligned}$ |
| $\text { 28. } \begin{array}{r} a=354295, \\ b=543440 \end{array}$ | $\text { 29. } \begin{array}{r} a=24789, \\ b=35286 \end{array}$ | $\text { 30. } \begin{array}{r} a=32893, \\ b=72568 \end{array}$ |

### 6.2. Compute $\operatorname{gcd}(a, b, c)$ with Lemma 5.4

| 1. $\mathrm{a}=529, \mathrm{~b}=1541, \mathrm{c}=1817$ | $\begin{aligned} & \text { 2. } \mathrm{a}=67283, \mathrm{~b}=122433, \\ & \mathrm{c}=221703 \end{aligned}$ |
| :---: | :---: |
| $\begin{aligned} & \text { 3. } \mathrm{a}=549493, \mathrm{~b}=863489, \\ & \mathrm{c}=133125 \end{aligned}$ | $\text { 4. } \begin{aligned} & \mathrm{a}=738089, \mathrm{~b}=3082607, \\ & \mathrm{c}=28303937 \end{aligned}$ |
| $\text { 5. } \begin{aligned} & \mathrm{a}=1767, \mathrm{~b}=2223, \\ & \mathrm{c}=11913 \end{aligned}$ | 6. $\mathrm{a}=476, \mathrm{~b}=1258, \mathrm{c}=21114$ |
| $\begin{aligned} & \text { 7. } a=3445, b=4225, \\ & c=5915 \end{aligned}$ | 8. $\mathrm{a}=572, \mathrm{~b}=5746, \mathrm{c}=1118$ |
| $\begin{aligned} & \text { 9. } \mathrm{a}=19074, \mathrm{~b}=13566, \\ & \mathrm{c}=8211 \end{aligned}$ | $\text { 10. } \begin{aligned} & \mathrm{a}=1073, \mathrm{~b}=3683, \\ & \mathrm{c}=34481 \end{aligned}$ |
| $\text { 11. } \begin{aligned} \mathrm{a} & =1012, \mathrm{~b}=1474, \\ \mathrm{c} & =4598 \end{aligned}$ | 12. $\mathrm{a}=988, \mathrm{~b}=2014, \mathrm{c}=42598$ |
| $\text { 13. } \begin{aligned} \mathrm{a} & =2585, \mathrm{~b}=7975, \\ \mathrm{c} & =13915 \end{aligned}$ | 14. $\mathrm{a}=874, \mathrm{~b}=1518, \mathrm{c}=20142$ |
| $\begin{aligned} & \text { 15. } \mathrm{a}=2227, \mathrm{~b}=9911, \\ & \mathrm{c}=952 \end{aligned}$ | 16. $\mathrm{a}=1253, \mathrm{~b}=252, \mathrm{c}=406$ |
| $\text { 17. } \begin{aligned} \mathrm{a} & =2743, \mathrm{~b}=3587, \\ \mathrm{c} & =6963 \end{aligned}$ | $\text { 18. } \begin{aligned} \mathrm{a} & =4345, \mathrm{~b}=6523, \\ \mathrm{c} & =10967 \end{aligned}$ |
| $\text { 19. } \begin{aligned} \mathrm{a} & =7683, \mathrm{~b}=5161, \\ \mathrm{c} & =12909 \end{aligned}$ | $\text { 20. } \begin{aligned} \mathrm{a} & =5174, \mathrm{~b}=12337, \\ \mathrm{c} & =13403 \end{aligned}$ |
| $\text { 21. } \begin{aligned} \mathrm{a} & =10047, \mathrm{~b}=6749, \\ \mathrm{c} & =16881 \end{aligned}$ | $\text { 22. } \begin{aligned} & =6766, b=16133, \\ c & =17527 \end{aligned}$ |
| $\text { 23. } \begin{aligned} \mathrm{a} & =11229, \mathrm{~b}=7543, \\ \mathrm{c} & =18867 \end{aligned}$ | $\text { 24. } \begin{aligned} & \mathrm{a}=7562, \mathrm{~b}=18031, \\ & \mathrm{c}=19589 \end{aligned}$ |
| $\text { 25. } \begin{aligned} & \mathrm{a}=13593, \mathrm{~b}=9131, \\ & \mathrm{c}=22839 \end{aligned}$ | $\text { 26. } \begin{aligned} \mathrm{a} & =9154, \mathrm{~b}=21827 \\ \mathrm{c} & =23713 \end{aligned}$ |
| $\text { 27. } \begin{aligned} & \mathrm{a}=17139, \mathrm{~b}=11513, \\ & \mathrm{c}=28797 \end{aligned}$ | $\text { 28. } \begin{aligned} \mathrm{a} & =11542, \mathrm{~b}=27521, \\ \mathrm{c} & =29899 \end{aligned}$ |
| $\text { 29. } \begin{aligned} & \mathrm{a}=18321, \mathrm{~b}=12307, \\ & \mathrm{c}=30783 \end{aligned}$ | $\text { 30. } \begin{aligned} & \mathrm{a}=12338, \mathrm{~b}=29419, \\ & \mathrm{c}=31961 \end{aligned}$ |

## 7. CONTINUED FRACTIONS

## Theorem 7.1. General Form

A continued fraction is an expression of the form

$$
\begin{array}{r}
\alpha=q_{1}+\frac{b_{1}}{q_{2}+\frac{b_{2}}{q_{3}+\ldots \ldots}} \\
\vdots \\
\ldots \ldots+\frac{b_{s-2}}{q_{s-1}+\frac{1}{\alpha_{s}}}
\end{array}
$$

where $\alpha, q_{i}$ 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:

$$
\frac{a}{b}=q_{1}+\frac{r_{1}}{b}=q_{1}+\frac{1}{\frac{b}{r_{1}}}=q_{1}+\frac{1}{q_{2}+\frac{r_{2}}{r_{1}}}=q_{1}+\frac{1}{q_{2}+\frac{1}{\frac{r_{1}}{r_{2}}}}=
$$

$$
q_{n-1}+\frac{1}{q_{n}}
$$

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

$$
\frac{a}{b}=\left[q_{1}, q_{2}, \ldots, q_{n}\right] .
$$

## Example 7.1

Represent rational number $Q=\frac{151}{13}$ by a continued fraction.
Solution
$\operatorname{Gcd}(151,13)=1$.
$Q=\frac{151}{13}=11+\frac{8}{13}=11+\frac{1}{\frac{13}{8}}=11+\frac{1}{1+\frac{5}{8}}=11+\frac{1}{1+\frac{1}{\frac{8}{5}}}=$
$=11+\frac{1}{1+\frac{1}{1+\frac{3}{5}}}=11+\frac{1}{1+\frac{1}{1+\frac{1}{\frac{5}{3}}}}=$

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

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

$$
\frac{\frac{a}{b}=q_{1}+\frac{1}{q_{2}+\frac{1}{q_{3}+\frac{1}{\cdots}}}}{},
$$

the convergents are

$$
\begin{gathered}
\delta_{1}=q_{1} ; \quad \delta_{2}=q_{1}+\frac{1}{q_{2}} ; \quad \delta_{3}=q_{1}+\frac{1}{q_{2}+\frac{1}{q_{3}}} ; \ldots . \\
\delta_{n}=q_{1}+\frac{1}{q_{2}+\frac{1}{q_{3}+\ldots}}=\frac{a}{b} . \\
\vdots \\
\ldots \ldots+\frac{1}{q_{n-1}+\frac{1}{q_{n}}}
\end{gathered}
$$

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 $\mathrm{i}^{\text {th }}$ convergent by $\delta_{i}=\frac{P_{i}}{Q_{i}}$. Then, $\delta_{l}=q_{1}=\frac{q_{1}}{l}=\frac{P_{1}}{Q_{1}}$, 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 $\delta_{3}$, we have

$$
\delta_{3}=\frac{P_{1}\left(q_{2}+\frac{1}{q_{3}}\right)+P_{0}}{Q_{1}\left(q_{2}+\frac{1}{q_{3}}\right)+Q_{0}}=\frac{q_{3}\left(P_{1} q_{2}+P_{0}\right)+P_{1}}{q_{3}\left(Q_{1} q_{2}+Q_{0}\right)+Q_{1}}=\frac{q_{3} P_{2}+P_{1}}{q_{3} Q_{2}+Q_{1}}=\frac{P_{3}}{Q_{3}} .
$$

For any convergent $\delta_{i}$ 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 $\mathrm{i}^{\text {th }}$ convergent.
The results of convergent computations can be placed into the table.

Table 7.1 - The results of convergent computations

| $\boldsymbol{i}$ | $\mathbf{0}$ | $\mathbf{1}$ | $\mathbf{2}$ | $\cdots$ |
| :--- | :--- | :--- | :--- | :--- |
| $q_{i}$ |  | $q_{1}$ | $q_{2}$ | $\cdots$ |
| $P_{i}$ | 1 | $P_{1}=q_{1}$ | $P_{2}=q_{2} P_{1}+P_{0}$ | $\cdots$ |
| $Q_{i}$ | 0 | $Q_{1}=1$ | $Q_{2}=q_{2} Q_{1}+Q_{0}$ | $\cdots$ |


| $\boldsymbol{j}$ | $\cdots$ | $\boldsymbol{n}$ |
| :--- | :--- | :--- |
| $q_{j}$ | $\cdots$ | $q_{n}$ |
| $P_{j}=q_{j} P_{j-1}+P_{j-2}$ | $\cdots$ | $a=P_{n}=q_{n} P_{n-1}+P_{n-2}$ |
| $Q_{j}=q_{j} Q_{j-1}+Q_{j-2}$ | $\cdots$ | $b=Q_{n}=q_{n} Q_{n-1}+Q_{n-2}$ |

## Property 7.2

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

## Property 7.3

For any $i>1$, the following formula takes place:
$\delta_{i}-\delta_{i-1}=\frac{(-1)^{i}}{Q_{i} Q_{i-1}}$.
Property 7.2 is used for solving the Diophantine equation $a x+b y=1$.

We write down property 7.2 for the last two columns of the table 7.1:
$P_{n} Q_{n-1}-Q_{n} P_{n-1}=(-1)^{n}, \quad P_{n}=a, \quad Q_{n}=b$, then $a Q_{n-1}-b P_{n-1}=(-1)^{n}$.

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

We have got a solution to the Diophantine equation: $x=Q_{n-1}, \quad y=-P_{n-1}$.
2. If $n$ is odd, then $a Q_{n-1}-b P_{n-1}=-1$, or $-a \cdot Q_{n-1}+b \cdot P_{n-1}=1$.

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

## Example 7.1

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

## 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.

$$
\begin{aligned}
& \quad P_{0}=1, Q_{o}=0, P_{1}=q_{1}=11, Q_{1}=1, \delta_{1}=\frac{P_{1}}{Q_{1}}=\frac{11}{1}=11, \\
& P_{2}=q_{2} P_{1}+P_{0}=1 \cdot 11+1=12, Q_{2}=q_{2} Q_{1}+Q_{0}=1 \cdot 1+0=1, \\
& \delta_{2}=\frac{P_{2}}{Q_{2}}=\frac{12}{1}=12, \\
& P_{3}=q_{3} P_{2}+P_{1}=1 \cdot 12+11=23, Q_{3}=q_{3} Q_{2}+Q_{1}=1 \cdot 1+1=2, \\
& \delta_{3}=\frac{P_{3}}{Q_{3}}=\frac{23}{2}=11.5, \\
& P_{4}=q_{4} P_{3}+P_{2}=1 \cdot 23+12=35, Q_{4}=q_{4} Q_{3}+Q_{2}=1 \cdot 2+1=3, \\
& \delta_{4}=\frac{P_{4}}{Q_{4}}=\frac{35}{3} \approx 11.667, \\
& P_{5}=q_{5} P_{4}+P_{3}=1 \cdot 35+23=58, Q_{5}=q_{5} Q_{4}+Q_{3}=1 \cdot 3+2=5, \\
& \delta_{5}=\frac{P_{5}}{Q_{5}}=\frac{58}{5}=11.6, \\
& P_{6}=q_{6} P_{5}+P_{4}=2 \cdot 58+35=151, Q_{6}=q_{6} Q_{5}+Q_{4}=2 \cdot 5+3=13, \\
& \delta_{6}=\frac{P_{6}}{Q_{6}}=\frac{151}{13} \approx 11.615=\frac{a}{b} .
\end{aligned}
$$

| $\boldsymbol{i}$ | $\mathbf{0}$ | $\mathbf{1}$ | $\mathbf{2}$ | $\mathbf{y}$ | $\mathbf{4}$ | $\mathbf{4}$ | $\mathbf{5}$ |
| :---: | :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| $\mathbf{6}$ | $\mathbf{6}$ |  |  |  |  |  |  |
| $q_{i}$ |  | 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 $151 x+13 y=1$ using property 7.2.

$$
P_{6} Q_{5}-Q_{6} P_{5}=(-1)^{6} \text { or } a \cdot 5-b \cdot 58=1 \text { or } a \cdot 5+b \cdot(-58)=1 .
$$

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 $a x+b y=1$.

| 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. $\frac{a}{b}=[0,4,1,3,2,5]$ |
| $\text { 10. } \frac{a}{b}=[22,3,1,4,7]$ | $\text { 11. } \frac{a}{b}=[2,1,30,2,3]$ | $\text { 12. } \frac{a}{b}=[1,24,3,4,5]$ |
| 13. $\frac{a}{b}=[1,25,1,2,3,1,1]$ | 14. $\frac{a}{b}=[11,2,3,5,1,1]$ | 15. $\frac{a}{b}=[31,5,2,3,1,5]$ |
| $\text { 16. } \frac{a}{b}=[1,25,1,2,3,1,1]$ | 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. $\frac{a}{b}=[2,41,2,3,1]$ |
| $\text { 22. } \frac{a}{b}=[2,17,1,5,1]$ | 23. $\frac{a}{b}=[3,19,1,1,3]$ | 24. $\frac{a}{b}=[2,1,1,3,5,1,1]$ |
| $\text { 25. } \frac{a}{b}=[2,11,3,19,1,1,3]$ | $\text { 26. } \frac{a}{b}=[5,9,3,11,1,1,2]$ | 27. $\frac{a}{b}=[21,1,3,7,1,1,3]$ |
| 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 $\boldsymbol{x}$ can be written uniquely as $x=n+\alpha$, where $n \in Z$ and $0 \leq \alpha<1$. We call $n$ the integer part or the floor of $\boldsymbol{x}$ and denote it by $[x]$ or $\lfloor x\rfloor$; and $\alpha$ is called the fractional part of $\boldsymbol{x}$ and is denoted by $\{x\}$. Thus, for $x \in R,[x]$ is the greatest integer not exceeding $x$.

The fractional part of $\boldsymbol{x}$ is commonly thought of as the part after the decimal point, but this notion is correct only for positive $\boldsymbol{x}$. 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. $[123.45]=123 ; \quad\{123.45\}=123.45-[123.45]=123.45-$
$-123=0.45$.
2. $[0.83]=0$;
$\{0.83\}=0.83-[0.83]=0.83-0=0.83$.
3. $[-0.01]=-1 ; \quad\{-0.01\}=-0.01-[-0.01]=-0.01-(-1)=0.9$.
4. $[-10.56]=-11 ; \quad\{-10.56\}=-10.56-[-10.56]=-10.56-$ $-(-11)=0.44$.

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

$13!=1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13$.
From this product write down the set of numbers that will be multiples of 2. Denote this set by $\mathrm{S}_{2}$ :
$S_{2}=\{2,4,6,8,10,12\} ;$
The number of members of $S_{2}$ (the cardinality $\left|S_{2}\right|$ 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 $\mathrm{S}_{4}$ :
$S_{4}=\{4,8,12\}$. 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 $\mathrm{S}_{8}$ :

$$
\mathrm{S}_{8}=\{8\} . \text { The cardinality }\left|S_{8}\right| \text { is }\left[\frac{13}{2^{3}}\right]=1 .
$$

From $\mathrm{S}_{8}$ write down the set of numbers that will be multiples of $2^{4}$. Denote this set by $\mathrm{S}_{16}$ :

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

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

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

## Example 8.3

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

If the prime factorization of $\mathrm{n}>1$ 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

$$
\begin{equation*}
\tau(n)=\tau\left(p_{1}{ }^{\alpha_{1}} \cdot p_{2}^{\alpha_{2}} \cdot \ldots \cdot p_{k}{ }^{\alpha_{k}}\right)=\left(\alpha_{1}+1\right)\left(\alpha_{2}+1\right) \cdot \ldots \cdot\left(\alpha_{k}+1\right), \tag{8.4.1}
\end{equation*}
$$

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

$$
\begin{equation*}
\sigma\left(p_{1}^{\alpha_{1}} \cdot p_{2}^{\alpha_{2}} \cdot \ldots \cdot p_{k}^{\alpha_{k}}\right)=\frac{p_{1}^{\alpha_{1}+1}-1}{p_{1}-1} \cdot \frac{p_{2}^{\alpha_{2}+1}-1}{p_{2}-1} \cdot \ldots \cdot \frac{p_{k}^{\alpha_{k}+1}-1}{p_{k}-1}, \tag{8.4.2}
\end{equation*}
$$

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 $\mathbf{n}$ 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

$$
\begin{equation*}
\phi(p)=p-1 \text {; } \tag{8.7.1}
\end{equation*}
$$

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

$$
\begin{equation*}
\phi\left(p^{\alpha}\right)=p^{\alpha}-p^{\alpha-1}=p^{\alpha-1}(p-1)=p^{\alpha}\left(1-\frac{1}{p}\right) \tag{8.7.2}
\end{equation*}
$$

If $n=p_{1}{ }^{\alpha_{1}} \cdot p_{2}{ }^{\alpha_{2}} \cdot \ldots \cdot p_{k}{ }^{\alpha_{k}}$, then

$$
\begin{align*}
& \phi(n)=\phi\left(p_{1}^{\alpha_{1}} \cdot p_{2}^{\alpha_{2}} \cdot \ldots \cdot p_{k}^{\alpha_{k}}\right)=\phi\left(p_{1}^{\alpha_{1}}\right) \phi\left(p_{2}^{\alpha_{2}}\right) \cdot \ldots \cdot \phi\left(p_{k}^{\alpha_{k}}\right)= \\
= & \left(p_{1}^{\alpha_{1}}-p_{1}^{\alpha_{1}-1}\right)\left(p_{2}^{\alpha_{2}}-p_{2}^{\alpha_{2}-1}\right) \cdot \ldots \cdot\left(p_{k}^{\alpha_{k}}-{p_{k}{ }^{\alpha_{k}-1}}^{\alpha_{1}}\right)= \\
= & p_{1}^{\alpha_{1}-1} p_{2}^{\alpha_{2}-1} \cdot \ldots \cdot p_{k}^{\alpha_{k}-1}\left(p_{1}-1\right)\left(p_{2}-1\right) \cdot \ldots \cdot\left(p_{k}-1\right)= \\
= & n\left(1-\frac{1}{p_{1}}\right)\left(1-\frac{1}{p_{2}}\right) \cdot \ldots \cdot\left(1-\frac{1}{p_{k}}\right) . \tag{8.7.3}
\end{align*}
$$

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

## 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)

$$
\phi(25)=\phi\left(5^{2}\right)=5^{2}-5=5(5-1)=20 \text {; }
$$

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)

$$
\begin{aligned}
& \quad \phi(100)=\phi\left(2^{2} \cdot 5^{2}\right)=\phi\left(2^{2}\right) \phi\left(5^{2}\right)=\left(2^{2}-2\right)\left(5^{2}-5\right)= \\
& =2 \cdot 5 \cdot(2-1)(5-1)=10 \cdot 4=40 ;
\end{aligned}
$$

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

$$
\begin{aligned}
& \quad \phi(1000)=\phi\left(2^{3} \cdot 5^{3}\right)=\phi\left(2^{3}\right) \phi\left(5^{3}\right)=\left(2^{3}-2^{2}\right)\left(5^{3}-5^{2}\right)= \\
& =2^{2} \cdot 5^{2} \cdot(2-1)(5-1)=100 \cdot 4=400 .
\end{aligned}
$$

## 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 $\boldsymbol{n}$ !

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

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 $\boldsymbol{n}>\mathbf{1}$ 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. $\quad a=3^{5} \cdot 5^{3} \cdot 11 \cdot 13$ | 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 $\rightarrow$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| Quotient $\downarrow$ |  |  |  |  |  |  |  |
|  | 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 |
| $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ |
| 20 | 140 | 141 | 142 | 143 | 144 | 145 | 146 |
| $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ |
| 33 | 231 | 232 | 233 | 234 | 235 | 236 | 237 |
| $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ |
| $\mathbf{q}$ | $\mathbf{7 q}$ | $\mathbf{7 q}+\mathbf{1}$ | $\mathbf{7 q}+\mathbf{2}$ | $\mathbf{7 q}+\mathbf{3}$ | $\mathbf{7 q}+\mathbf{4}$ | $\mathbf{7 q}+\mathbf{5}$ | $\mathbf{7 q}+\mathbf{6}$ |
| $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ |

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 7 q . All numbers of class 1 have the remainder $\mathrm{r}=1$ from division by 7 and we denote this class as $7 \mathrm{q}+1$. We denote classes $2,3,4,5,6$ as $7 \mathrm{q}+2,7 \mathrm{q}+3,7 \mathrm{q}+$ $+4,7 q+5,7 q+6$ 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 $7 \mathrm{q}+1$. We denote this fact as: $141 \equiv 15(\bmod 7)$.

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

Generalizing the consideration, we can make a conclusion.
For every integer $\boldsymbol{m}$ called modulus, we can consider the set of $\boldsymbol{m}$ remainders $\left\{0,1,2, \ldots, \boldsymbol{r}_{\boldsymbol{i}}, \ldots, \boldsymbol{m} \mathbf{- 1}\right\}$. Each remainder $\boldsymbol{r}_{\boldsymbol{i}}$ of this set forms a corresponding number class. This class is denoted as $\boldsymbol{m} \times \boldsymbol{q}+\boldsymbol{r}_{\boldsymbol{i}}, \boldsymbol{q} \in \mathbf{Z}, \boldsymbol{r}_{\boldsymbol{i}}<\boldsymbol{m}$. All numbers from the class $\boldsymbol{m} \times \boldsymbol{q}+\boldsymbol{r}_{\boldsymbol{i}}$ are congruent to each other modulo $m$. This fact is denoted as $\forall a, b \in m q+r_{i} \Rightarrow a \equiv b(\bmod m)$. Another notation is $a=b+m q$.

## Definition 9.1.1

The relationship $a \equiv b(\bmod m)$ is called congruence modulo $\boldsymbol{m}$.
Numbers from different classes are not congruent modulo $m$. This fact is denoted as

$$
\forall a \in m q+r_{i} \& \forall b \in m t+r_{j}, i \neq j, a \not \equiv b(\bmod m) .
$$

## 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 $\boldsymbol{m}$. In particular, $\{0,1, \ldots$, $\mathrm{m}-1\}$ 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 $m$ $m q \equiv O(\bmod m), \forall q \in Z$. 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:

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

Really, $41=7 \cdot 5+6,7 \cdot 5 \in 7 \cdot q$, then $7 \cdot 5 \equiv 0(\bmod 7)$ and $41 \equiv 6(\bmod 7)$. On the other hand,
$41=7 \cdot 6-1,7 \cdot 6 \in 7 \cdot q$, then $7 \cdot 6 \equiv 0(\bmod 7)$ and $41 \equiv-1(\bmod 7)$. Thus, $6 \equiv 6-7=-1(\bmod 7)$.

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

## Lemma 9.1.1

For any $\mathbf{a}, \mathbf{b}>\mathbf{0}$ and positive $\boldsymbol{m}$, the following statement holds. If $a \equiv b(\bmod m)$, then $a \equiv b-m(\bmod m)$ and $a-m \equiv b(\bmod m)$.

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 $0,1,2, \ldots, \frac{m-1}{2}$ 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 $\left\{0, \pm 1, \pm 2, \ldots, \pm \frac{m-1}{2}\right\}$.
2. Secondly, if $m$ is even, then the residues $0,1,2, \ldots, \frac{m}{2}$ 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

$$
\left\{-\frac{m}{2}+1, \ldots,-2,-1,0,1,2, \ldots, \frac{m}{2}\right\}
$$

## 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 $\{0,1,2,3,4-7,5-7,6-7\}=(0, \pm 1, \pm 2, \pm 3\}$ 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 $\mathrm{a}, \mathrm{b}, \mathrm{c}$, and $\mathrm{m}>0$ the following properties hold:

1. Reflexivity property $a \equiv a(\bmod m)$

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

## 2. Symmetry property $a \equiv b(\bmod m) \Rightarrow b \equiv a(\bmod m)$

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

For example: $24 \equiv 38(\bmod 7) \Rightarrow 38 \equiv 24(\bmod 7)$. 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 $a \equiv b(\bmod m)$ and $b \equiv c(\bmod m)$, then $a \equiv c(\bmod m)$.
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: $24 \equiv 38(\bmod 7), 38 \equiv 150(\bmod 7) \Rightarrow 24 \equiv 150(\bmod 7)$. 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 $\boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{Z}$ and positive $\boldsymbol{m}>\mathbf{1}, \boldsymbol{m} \in \boldsymbol{Z}, a \equiv b(\bmod m)$ iff $m \mid(a-b)$.

## Proof

Clearly if $m \mid(a-b)$, then
$a-b=m q \Rightarrow a=b+m q \Rightarrow a \equiv b(\bmod m)$.
On the other hand,
$a \equiv b(\bmod m) \Rightarrow a=b+m t \Rightarrow a-b=m t \Rightarrow m \mid(a-b)$.
So, the difference of any two numbers from the same class belongs to class $\mathbf{0}$,
$a-b \equiv O(\bmod m)$.

## Theorem 9.1.3

If $a \equiv b(\bmod m)$ and $c \equiv d(\bmod m)$, then

1) $a+c \equiv b+d(\bmod m)$ and $a-c \equiv b-d(\bmod m)-$ algebraic

## addition.

Consequence: $a+c \equiv b(\bmod m) \Rightarrow a \equiv b-c(\bmod m)$;
2) $a c \equiv b d(\bmod m)-$ multiplication;
3) $a^{n} \equiv b^{n}(\bmod m)$ for all $n \geq 1$ - powering;
4) $\forall k \in Z \quad k a \equiv k b(\bmod m)$ - multiplication by number;
5) $\forall a, b, a_{1}, b_{1}, k \in Z, \operatorname{gcd}(m, k)=1$,
$a=k \cdot a_{1}, b=k \cdot b_{1}: a \equiv b(\bmod m) \Rightarrow a_{1} \equiv b_{1}(\bmod m)$;
6) If $a_{i} \equiv b_{i}(\bmod m), i=\overline{1, n}$ and $x \equiv y(\bmod m)$, then
$\sum_{i=0}^{n} a_{n-i} x^{n-i} \equiv \sum_{i=0}^{n} b_{n-i} y^{n-i}(\bmod m) \quad$ for all polynomials with integer coefficients.

## Proof

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

The addition of both equations produces
$a+c=m \cdot t+b+m \cdot q+d=m \cdot(t+q)+b+d$;
$t+q=s \in Z ; m \cdot s \equiv 0(\bmod m) \Rightarrow a+c \equiv b+d(\bmod m)$.
Similarly, if we add two congruences such that $a+c \equiv b(\bmod m)$, and $-c \equiv-c(\bmod m)$, then we will get
$a \equiv b-c(\bmod m)$.
2) $a \equiv b(\bmod m)$ means that $a=m \cdot t+b, t \in Z ; c \equiv d(\bmod m)$ signifies that $c=m \cdot q+d, q \in Z$. Product of both equations yields

$$
\begin{aligned}
& \quad a \cdot c=(m t+b)(m q+d)=m t m q+m t d+b m q+b d= \\
& =m(m t q+t d+b q)+b d ; \\
& \quad m t q+t d+b q=\mathrm{s} \in \mathrm{Z} ; \mathrm{ms} \equiv 0(\operatorname{modm}) \Rightarrow a c \equiv b d(\bmod m) .
\end{aligned}
$$

3) $a^{n} \equiv b^{n}(\bmod m)$ is got by successive multiplication of congruences by themselves. Hence, property (3) is indeed true.
4) $a \equiv b(\bmod m) \Leftrightarrow a=b+m q$, we multiply the last expression by $k$ :
$k a=k b+m k q, k q=q_{1} \in Z \Rightarrow k a=k b+m q_{1} \Rightarrow k a \equiv k b(\bmod m)$.
5) $a=k \cdot a_{1}, b=k \cdot b_{1}: a \equiv b(\bmod m) \Rightarrow$
$\Rightarrow k a_{1} \equiv k b_{1}(\bmod m) \quad$ or $k a_{1}=k b_{1}+m q$. According to Integration property in Theorem 1.2, we can write $k \mid m q$. Since $\operatorname{gcd}(m, k)=1$, it follows that $k \mid q, q=k q_{1}$. So, we have $k a_{1}=k b_{1}+m k q_{1}$. Finally, by dividing the last expression by $k$, we will get $a_{1}=b_{1}+m q_{1} \Rightarrow a_{1} \equiv b_{1}(\bmod m)$.
6) Let us consider a congruence

$$
a_{n} x^{n}+a_{n-1} x^{n-1}+\ldots+a_{1} x+a_{0}=\sum_{i=0}^{n} a_{n-i} x^{n-i} \equiv 0(\bmod m) .
$$

Taking into account that $a_{i} \equiv b_{i}(\bmod m), i=\overline{1, n}$ and $x \equiv y(\bmod m)$, or $a_{i}=b_{i}+m q_{i} ; \quad x=y+m t$, we obtain

$$
\begin{aligned}
& \sum_{i=0}^{n} a_{n-i} x^{n-i}=\sum_{i=0}^{n}\left(b_{n-i}+\boldsymbol{m} \boldsymbol{q}_{n-i}\right) x^{n-i}=\sum_{i=0}^{n} b_{n-i} x^{n-i}+\boldsymbol{m} \sum_{i=0}^{n} \boldsymbol{q}_{n-1} \equiv \\
\equiv & \sum_{i=0}^{n} b_{n-i} x^{n-i}(\bmod m) .
\end{aligned}
$$

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

$$
\begin{aligned}
& \sum_{i=0}^{n} b_{n-i} x^{n-i}=\sum_{i=0}^{n} b_{n-i}(\boldsymbol{y}+\boldsymbol{m} \boldsymbol{t})^{n-i}= \\
= & \sum_{i=0}^{n} b_{n-i}\left(y^{n-i}+C_{\mathrm{n}-\mathrm{i}}^{1} y^{n-i-1} m t+\ldots+C_{\mathrm{n}-\mathrm{i}}^{\mathrm{n}-\mathrm{i}-1} y(m t)^{n-i-1}+(m t)^{n-i}\right) .
\end{aligned}
$$

By denoting

$$
\begin{aligned}
& q=C_{n-i}{ }^{l} y^{n-i-1} t+\ldots+C_{n-i}^{n-i-1} y m^{n-i-2} t^{n-i-1}+m^{n-i-1} t^{n-i} \in Z, \text { we have } \\
& \sum_{i=0}^{n} b_{n-i}(\boldsymbol{y}+\boldsymbol{m} \boldsymbol{t})^{n-i}=\sum_{i=0}^{n} b_{n-i}\left(y^{n-i}+m q\right)=\sum_{i=0}^{n} b_{n-i} y^{n-i}+\sum_{i=0}^{n} b_{n-i} \boldsymbol{m} \boldsymbol{q}=
\end{aligned}
$$

$=\sum_{i=0}^{n} b_{n-i} y^{n-i}+m \sum_{i=0}^{n} b_{n-i} \boldsymbol{q}$.
By introducing $q_{1}=\sum_{i=0}^{n} b_{n-i} q \in Z$, we get
$\sum_{i=0}^{n} b_{n-i} x^{n-i}=\sum_{i=0}^{n} b_{n-i} y^{n-i}+m \sum_{i=0}^{n} b_{n-i} \boldsymbol{q}=\sum_{i=0}^{n} b_{n-i} y^{n-i}+m q_{1} \equiv$
$\equiv \sum_{i=0}^{n} b_{n-i} y^{n-i}(\bmod m)$.
As a result, we deduce $\sum_{i=0}^{n} a_{n-i} x^{n-i} \equiv \sum_{i=0}^{n} b_{n-i} y^{n-i}(\bmod m)$.

## Examples 9.1.2

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

1) The sum of $3 \equiv 52(\bmod 7)$ and $5 \equiv 40(\bmod 7)$ is $8 \equiv 92(\bmod 7)$. The obtained congruence is true because $8 \equiv 1(\bmod 7)$ and $92 \equiv 1(\bmod 7)$. The difference between them is $-2 \equiv 12(\bmod 7)$. Such congruence is correct, because $-2 \equiv 5(\bmod 7)$ and $12 \equiv 5(\bmod 7)$.
2) The product of given congruences is $15 \equiv 2080(\bmod 7)$. One can see that $15 \equiv 1(\bmod 7)$ and $2080=7 \cdot 297+1 \Rightarrow 2080 \equiv 1(\bmod 7)$. Hence, this congruence is correct.
3) Raise the first congruence to the second power:

$$
\begin{aligned}
& (3 \equiv 52(\bmod 7))^{2} \Rightarrow 3^{2} \equiv 52^{2}(\bmod 7) \Rightarrow 9 \equiv 2704(\bmod 7) \\
& 9 \equiv 2(\bmod 7) ; 2704=7 \cdot 386+2 \Rightarrow 2704 \equiv 2(\bmod 7)
\end{aligned}
$$

So, if $3 \equiv 52(\bmod 7)$ is true, then $3^{2} \equiv 52^{2}(\bmod 7)$ is indeed true.
4) Multiply through the congruence $3 \equiv 52(\bmod 7)$ by 10 . We obtain $30 \equiv 520(\bmod 7) ; 30=7 \cdot 4+2 ; 520=7 \cdot 74+2$. Both numbers 30
and 520 leave the same remainder 2 when divided by 7 ; hence $3 \cdot 10 \equiv 52 \cdot 10(\bmod 7)$ is true.
5) Take the congruence $5 \equiv 40(\bmod 7)$. 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 $1 \equiv 8(\bmod 7)$ 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 $1348^{26}$ $1348=13 \cdot 103+9 \Rightarrow 1348 \equiv 9(\bmod 13) ; 9<13 ; \operatorname{gcd}(9,13)=1 . \quad$ The integer 9 is the least positive residue for the integer 1348 modulo 13. Then using property (6), we can write $1348^{26} \equiv 9^{26}(\bmod 13)$.

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

$$
\begin{aligned}
& 9^{24}=\left(9^{2}\right)^{13}=81^{13}=(13 \cdot 6+3)^{13} \equiv 3^{13}(\bmod 13) \\
& 3^{13}=3^{12} \cdot 3=\left(3^{4}\right)^{3} \cdot 3=81^{3} \cdot 3 \equiv 3^{3} \cdot 3(\bmod 13) \\
& 3^{3} \cdot 3=27 \cdot 3=(13 \cdot 2+1) \cdot 3 \equiv 3(\bmod 13) ; \mathbf{3}<\mathbf{1 3}
\end{aligned}
$$

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 $a \equiv b(\bmod m)$, 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:

$$
\left(\frac{a}{k}\right) \equiv\left(\frac{b}{k}\right)\left(\bmod \frac{m}{k}\right) \text { or } a_{1} \equiv b_{1}\left(\bmod m_{1}\right)
$$

For example, we have
$155 \equiv 85(\bmod 35) ; \quad \frac{155}{5}=31 ; \frac{85}{5}=17 ; \frac{35}{5}=7 \Rightarrow 31 \equiv 17(\bmod 7) ;$
2) $\forall k \in Z \quad k a \equiv k b(\bmod k m)$ - multiplication by number.

For example, multiply the congruence $31 \equiv-2(\bmod 11)$ by 5 . We obtain $155 \equiv-10(\bmod 55)$. 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 $d|\boldsymbol{b} \Rightarrow d| a)$.
For example, $x \equiv 93(\bmod 144) ; \operatorname{gcd}(93,144)=3 \Rightarrow 3 \mid x ;$
4) if $a \equiv b\left(\bmod m_{1}\right)$, and $a \equiv b\left(\bmod m_{2}\right)$, and......, and $a \equiv b\left(\bmod m_{k}\right) \Leftrightarrow$ then $a \equiv b\left(\bmod \operatorname{Lcm}\left(m_{I}, m_{2}, \ldots, m_{k}\right)\right)$. Moreover, if $\operatorname{gcd}\left(m_{1}, m_{2}, \ldots, m_{k}\right)=1$, then $a \equiv b\left(\bmod m_{1} m_{2} \ldots m_{k}\right)$.

For example,
a) Suppose $x \equiv 3(\bmod 5), x \equiv 3(\bmod 11), x \equiv 3(\bmod 7)$, we get $x \equiv 3(\bmod 5 \cdot 11 \cdot 7)$.
b) Assume that $x \equiv 3(\bmod 5), x \equiv 3(\bmod 35), x \equiv 3(\bmod 21)$, $\operatorname{lcm}(5,35,21)=105$, then $x \equiv 3(\bmod 105)$.

### 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 $p(\operatorname{gcd}(a, p)=1)$, then

$$
p \mid\left(a^{p}-a\right)
$$

This is the same as

$$
a^{p-1} \equiv 1(\bmod p)
$$

Theorem 9.3.2. (Euler's theorem) If $m>0$ and a is a coprime to $m$
$(\operatorname{gcd}(a, m)=1)$, then
$a^{\varphi(m)} \equiv 1(\bmod m)$.
Example 9.3.1. Check, if $167^{10} \equiv 1(\bmod 11)$
Solution
Consider the following congruence:
$167 \equiv 2(\bmod 11) \Rightarrow \operatorname{gcd}(167,11)=1$.
Hence, with Fermat's little theorem 9.3.1,
$167^{10} \equiv 2^{10}(\bmod 11)$,
$2^{10}=\left(2^{5}\right)^{2}=32^{2} \equiv(32-3 \cdot 11)^{2}=(-1)^{2}=1(\bmod 11)$.
Then $167^{10} \equiv 1(\bmod 11)$ and Fermat's little theorem holds.
Example 9.3.2. Find the remainder from the division of $23^{1443}$ by 13.

## Solution

We have
$23^{1443} \equiv x(\bmod 13) ; 23 \equiv-3(\bmod 13) \Rightarrow 23^{1443} \equiv(-3)^{1443}(\bmod 13)$.
Taking into account that $\operatorname{gcd}(3,13)=1$, then with Fermat's little theorem we can write $(-3)^{12} \equiv 1(\bmod 13)$.

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

$$
\left((-3)^{12}\right)^{120} \equiv 1^{120}(\bmod 13) \Rightarrow(-3)^{1440} \equiv 1(\bmod 13)
$$

Obviously, $1443=1440+3$, so we have

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

$\equiv-27+3 \cdot 13 \equiv 12(\bmod 13)$.
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 $\mathbf{1 0 0 0}$.

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

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

$$
\varphi(1000)=\varphi\left(2^{3} \cdot 5^{3}\right)=\left(2^{3}-2^{2}\right)\left(5^{3}-5^{2}\right)=4 \cdot 100=400 .
$$

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 $13^{1600} \equiv 13 x(\bmod 1000)$. Using property (3) in Theorem 9.1.10, we can write down that $13^{1600}=\left(13^{400}\right)^{4} \equiv 1(\bmod 1000)$. So, $13 x \equiv 1(\bmod 1000)$. Then, taking into account property (1) in Theorem 9.1, we add the modulus 1000 to the right side of the congruence:

$$
13 x \equiv 1001(\bmod 1000) ; 1001=13 \cdot 77 ; \operatorname{gsd}(13,1000)=1
$$

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

$$
x \equiv 77(\bmod 1000)
$$

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: $348^{128} \equiv x(\bmod 21)$.

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

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

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

$$
\begin{aligned}
& 348^{128}=348^{127} \cdot 348 \equiv 3 y(\bmod 21) \Rightarrow 348^{127} \cdot 116 \equiv y(\bmod 7) \\
& 348=7^{3}+5 ; 116=7 \cdot 16+4 \Rightarrow 348 \equiv 5(\bmod 7) \\
& 116 \equiv 4(\bmod 7) \stackrel{\text { prop }(6)}{\Rightarrow}(5)^{127} \cdot 4 \equiv y(\bmod 7)
\end{aligned}
$$

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

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

Since $5^{6} \equiv 1(\bmod 7) \Rightarrow\left(5^{6}\right)^{21} \equiv 1(\bmod 7)$ (the property $(3)$ in Theorem $\quad 9.1 .10)$ and $\quad 5^{127} \cdot 4=\left(5^{6}\right)^{21} \cdot 5 \cdot 4 \equiv 20(\bmod 7)$, $20 \equiv 6(\bmod 7) \Rightarrow y \equiv 6(\bmod 7)$.

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

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: $143^{50}+343^{50} \equiv x(\bmod 17)$.

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

$$
143^{50} \equiv x_{1}(\bmod 17) ; \quad 343^{50} \equiv x_{2}(\bmod 17)
$$

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. $143^{50} \equiv x_{1}(\bmod 17)$.
$\operatorname{gcd}(143,17)=1 ; 17$ is prime $\stackrel{\text { Th9.3.1. }}{\Rightarrow} 143^{16} \equiv 1(\bmod 17)$,
$50=16 \cdot 3+2 \Rightarrow 143^{50}=\underbrace{\left(143^{16}\right)^{3}}_{\equiv l(\bmod 17)} \cdot 143^{2} \equiv 143^{2}(\bmod 17)$,
$143=17 \cdot 8+7 \Rightarrow 143 \equiv 7(\bmod 17) \Rightarrow 143^{2} \equiv 7^{2}(\bmod 17)$,
$7^{2}=49=17 \cdot 2+15=17 \cdot 3-2 \Rightarrow 7^{2} \equiv-2(\bmod 17)$.
Thus $x_{1} \equiv-2(\bmod 17)$ is a solution to the first congruence.
2. Now, we will consider the second congruence. We get $343^{50} \equiv x_{2}(\bmod 17)$.
$\operatorname{gcd}(343,17)=1 ; 17$ is prime $\stackrel{\text { Th9.3.1 }}{\Rightarrow} 343^{16} \equiv 1(\bmod 17)$,
$50=16 \cdot 3+2 \Rightarrow 341^{50}=\underbrace{\left(343^{16}\right)^{3}}_{\equiv I(\bmod 17)} \cdot 343^{2} \equiv 343^{2}(\bmod 17)$,
$343=17 \cdot 20+3 \Rightarrow 343 \equiv 3(\bmod 17) \Rightarrow 343^{2} \equiv 3^{2}(\bmod 17)$, $3^{2}=9<17$.

Thus we have obtained $x_{2} \equiv 9(\bmod 17)$.
3. Finally, the total solution to the given problem is $x=x_{1}+x_{2} \equiv-2+9=7(\bmod 17)$.

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 | $\begin{aligned} & 2 . \\ & 2100+3100 \text { by } 5 \end{aligned}$ | 3. <br> 11802 by 1000 | 4. <br> 172001 by 1000 |
| :---: | :---: | :---: | :---: |
| 5. $192402 \text { by } 100$ | $\begin{aligned} & 6 . \\ & 17852 \text { by } 11 \end{aligned}$ | $\begin{aligned} & \hline 7 . \\ & 19671968 \text { by } 11 \end{aligned}$ | 8. 383175 by 45 |
| $\begin{aligned} & 9 . \\ & 109345 \text { by } 14 \end{aligned}$ | $\begin{aligned} & 10 . \\ & 439291 \text { by } 60 \end{aligned}$ | $\begin{aligned} & 11 . \\ & 293275 \text { by } 48 \end{aligned}$ | 12. 6617 by 7 |
| $\begin{aligned} & 13 . \\ & 11753 \text { by } 11 \end{aligned}$ | $\begin{aligned} & 14 . \\ & 570+750 \text { by } 12 \end{aligned}$ | $\begin{aligned} & 15 . \\ & 580+7100 \text { by } 13 \end{aligned}$ | $\begin{aligned} & 16 . \\ & 550+13100 \text { by } 18 \end{aligned}$ |
| 17. <br> 111841 by 7 | $\begin{aligned} & 15 . \\ & 580+7100 \text { by } 13 \end{aligned}$ | $\begin{aligned} & 16 . \\ & 550+13100 \text { by } 18 \end{aligned}$ | $\begin{aligned} & 20 . \\ & 122751 \text { by } 10 \end{aligned}$ |
| $\begin{aligned} & 21 . \\ & 343741 \text { by } 26 \end{aligned}$ | $\begin{aligned} & 22 . \\ & 1782741 \text { by } 22 \end{aligned}$ | $\begin{aligned} & 23 . \\ & 111201 \text { by } 1000 \end{aligned}$ | $\begin{aligned} & 24 . \\ & 71199 \text { by } 1000 \end{aligned}$ |
| $\begin{aligned} & 25 . \\ & 3157 \text { by } 100 \end{aligned}$ | $\begin{aligned} & 26 . \\ & 1778 \text { by } 100 \end{aligned}$ | 27. <br> 1979 by 100 | $\begin{aligned} & 28 . \\ & 7114 \text { by } 100 \end{aligned}$ |
| $\begin{aligned} & 29 . \\ & 11203 \text { by } 100 \end{aligned}$ | $\begin{aligned} & 30 . \\ & 7332 \text { by } 100 \end{aligned}$ |  |  |

## 10. LINEAR CONGRUENCES WITH ONE UNKNOWN

### 10.1. CONGRUENCES OF THE First Order. Solving Congruences

## Definition 10.1.1

An expression of the form

$$
a x+b \equiv 0(\bmod m) \text { or } a x \equiv b(\bmod m)
$$

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 $x_{1}+m t, t \in Z$ such that substitution of each residue into the congruence yields the equivalent congruence $b \equiv b(\bmod m)$.

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 $a x$ 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 $a x \equiv b(\bmod m)$ has a unique solution.

Secondly, let us consider the congruence $a x \equiv b(\bmod m)$ and assume that $(a, m)=d>1$ :

$$
a x \equiv b(\bmod m) \Rightarrow a x=b+m t
$$

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

$$
a=a_{1} d, b=b_{1} d, m=m_{1} d, \quad\left(a_{1}, m_{1}\right)=\left(b_{1}, m_{1}\right)=1
$$

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

$$
a_{1} x \equiv b_{1}\left(\bmod m_{1}\right) .
$$

From the above, it has a unique solution $x \equiv x_{1}\left(\bmod m_{1}\right)$ or $x=m_{1} t+x_{1}$. On the other hand, if we consider the complete system of incongruent residues to modulus $m=d m_{1}$, then we will be able to see that there will be solutions in the interval $[0, m]$ as follows:

$$
x_{1}, x_{1}+m_{1}, x_{1}+2 m_{1}, \ldots, x_{1}+(d-1) m_{1}
$$

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:

$$
x_{2}=x_{1}+m_{1}, \ldots, x_{d}=x_{1}+(d-1) m_{1} .
$$

## A linear congruence can be solved by several methods.

### 10.1.1. APPLICATION OF CONGRUENCE'S PROPERTIES

## Examples

a) Solve the congruence: $15 x \equiv 25(\bmod 17)$.

## 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 : $3 x \equiv 5(\bmod 17)$. The number 5 corresponds to the least absolute residue -12 , which is multiple of 3 . Finely, we cancel off equation $3 x \equiv-12(\bmod 17)$ by 3 , this yields: $x \equiv-4(\bmod 17)$. 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 $10 x \equiv 35(\bmod 55)$.

## Solution

We get $(10,55)=5>1,5 \mid 35$.
Hence, the congruence has just five solutions.
Then cancellation by $d=5$ produces
$2 x \equiv 7(\bmod 11)$.
Taking into account $(2,11)=1$, we can make a conclusion that such congruence possesses a unique solution

$$
2 x \equiv 7+11(\bmod 11) \Rightarrow 2 x \equiv 18(\bmod 11) \Rightarrow x \equiv 9(\bmod 11) .
$$

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

$$
\begin{aligned}
& x_{0} \equiv 9(\bmod 55), \quad x_{1} \equiv 9+11 \cdot 1=18(\bmod 55), \\
& x_{2} \equiv 9+11 \cdot 2=31(\bmod 55), \\
& x_{3} \equiv 9+11 \cdot 3=42(\bmod 55), \quad x_{4} \equiv 9+11 \cdot 4=53(\bmod 55)
\end{aligned}
$$

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

Thus solutions $x_{0}, x_{1}, x_{2}, x_{3}, x_{4}$ are incongruent modulo 55 and $x_{5} \equiv x_{0}(\bmod 55)$.

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

$$
x \equiv 9+11 t(\bmod 55), \quad t=[0, \ldots, d-1]=[0, \ldots, 4] .
$$

c) Solve the congruence $10 x \equiv 33(\bmod 55)$.

## 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 $a x \equiv b(\bmod m),(a, m)=1$.
Let us expand the given below ratio into continued fraction

$$
\begin{aligned}
\frac{m}{a}=q_{1}+\frac{1}{q_{2}+\ldots} & \\
& +\frac{1}{q_{n}}
\end{aligned}
$$

We shall get a set of partial quotients $q_{1}, q_{2}, \ldots, q_{n}$. 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, $m Q_{n-1}-a P_{n-1}=(-1)^{n}$. Since $Q_{n-1}$ is an integer, we may suppose that $m Q_{n-1}$ is a modular period which can be truncated. This leads to $a P_{n-1}=(-1)^{n-1} \bmod (m)$. Multiplying both parts of the expression by number $(-1)^{n} b$, we obtain

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

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

## Example

Solve the congruence $256 x \equiv 179(\bmod 337)$.

## 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:

$$
\begin{array}{ll}
\frac{337}{256}=1+\frac{81}{256}, q_{1}=1 ; & \frac{256}{81}=3+\frac{13}{81}, q_{2}=3 ; \\
\frac{81}{13}=6+\frac{3}{13}, q_{3}=6 ; & \frac{13}{3}=4+\frac{1}{3}, q_{4}=4 ; \\
\frac{3}{1}=3, q_{5}=3 . &
\end{array}
$$

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

$$
\begin{aligned}
n & =5, P_{n-1}=P_{4}=104, b=179 \Rightarrow \\
\Rightarrow x & =(-1)^{4} 104 \cdot 179(\bmod 337) ; \quad \frac{104 \cdot 179}{337}=55+\frac{81}{337} .
\end{aligned}
$$

Thus the solution is $x \equiv 81(\bmod 337)$.

### 10.2. MULTIPLICATIVE INVERSE

## Definition 10.2.1

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

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

$$
a x \equiv 1(\bmod m)
$$

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 $a x \equiv 1(\bmod m)$ :

$$
x \equiv a^{\varphi(m)-1}(\bmod m)
$$

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:

$$
a^{-1} \equiv a^{\varphi(m)-1}(\bmod m)
$$

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:

$$
a^{-1} \equiv a^{p-2}(\bmod p)
$$

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

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

$$
\frac{43}{1}=43, q_{4}=43
$$

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 |
| $Q_{i}$ | 0 | 1 | 2 | 3 | 131 |
| $m$ |  |  |  |  |  |

Using their properties, one can write the following:

$$
P_{4} \cdot Q_{3}-P_{3} \cdot Q_{4}=(-1)^{4} \text { or } \underbrace{437 \cdot 3}_{\equiv 0(\bmod 437)}-10 \cdot 131=1 .
$$

Therefore, we come to a conclusion that
$(-10) \cdot 131 \equiv 1(\bmod 437)$.
Finely, we have
$131^{-1} \equiv-10(\bmod 437) \quad$ or $131^{-1} \equiv 427(\bmod 437)$.

## 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

Let us assume that $m_{1}, m_{2}, \ldots, m_{k}$ are pairwise prime numbers such that $\left(m_{i}, m_{j}\right)=1, i=\overline{1, k} ; j=\overline{1, k} ; i \neq j$.

## Definition 10.3.1

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

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

$$
\left\{\begin{array}{c}
x \equiv c_{1}\left(\bmod m_{1}\right),  \tag{2}\\
x \equiv c_{2}\left(\bmod m_{2}\right), \\
\cdots \cdots \cdots \cdots \cdots \\
x \equiv c_{k}\left(\bmod m_{k}\right) .
\end{array}\right.
$$

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 $m_{1}, m_{2}, \ldots, m_{k}$ be pairwise coprime positive integers and let $c_{1}, c_{2}, \ldots, c_{k}$ be integers satisfying the inequalities $0 \leq c_{i} \leq m_{i}-1, \quad i=\overline{1, k}$. Then, there exists a unique integer $\alpha$ such that $c_{i}$ will be the remainder on dividing $\alpha$ by $m_{i}$, i.e., $\alpha \equiv c_{i}\left(\bmod m_{i}\right)$.

## Proof

We shall prove the theorem by constructing a number $\alpha$. Denote by $M$ the gcd of all moduli. Since they are pairwise coprime, then $M=m_{1} m_{2} \ldots m_{k}$. Further, we build a system of numbers as follows:

$$
M_{i}=\frac{M}{m_{i}}=\frac{m_{1} m_{2} \ldots m_{i} \ldots m_{k}}{m_{i}}=m_{1} m_{2} \ldots m_{i-1} m_{i+1} \ldots m_{k}, i=\overline{1, k} .
$$

Being pairwise coprime with $m_{i}$, each $M_{i}$ has an inverse

$$
M_{i}^{-1} \equiv M_{i}^{\varphi\left(m_{i}\right)-1} \bmod \left(m_{i}\right) .
$$

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

$$
x \equiv \alpha(\bmod M)
$$

Indeed, let us substitute $\alpha$ to the first congruence of the system (2):

$$
M_{1} M_{1}^{-1} c_{1}+M_{2} M_{2}^{-1} c_{2}+\ldots+M_{k} M_{k}^{-1} c_{k} \equiv c_{1}\left(\bmod m_{1}\right) .
$$

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, $M_{1} M_{1}^{-1} \equiv 1\left(\bmod m_{1}\right)$ and, consequently, $\left(M_{1}, m_{1}\right)=1$. Finally, there will remain only equivalent congruence $c_{1} \equiv c_{1}\left(\bmod m_{1}\right)$.

In the second equation, the only term incongruent to 0 modulo $m_{2}$ is $M_{2} M_{2}^{-1} c_{2}$. Thus, $\alpha$ 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 $x=\alpha+M t, \quad t \in Z$.

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

## Example

Solve a system of congruences

$$
\left\{\begin{array}{l}
743 x \equiv 16(\bmod 13), \\
59 x \equiv 128(\bmod 5), \\
136 x \equiv 82(\bmod 3) .
\end{array}\right.
$$

## 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.

$$
\left\{\begin{array}{c}
2 x \equiv 3(\bmod 13), \\
4 x \equiv 3(\bmod 5), \\
x \equiv 1(\bmod 3) .
\end{array}\right.
$$

We bring the system to the type (2):

$$
\left\{\begin{array}{l}
2 x \equiv 3+13(\bmod 13) \Rightarrow 2 x \equiv 16(\bmod 13) \underset{(2,13)=1}{\Rightarrow} x \equiv 8(\bmod 13), \\
4 x \equiv 3+5(\bmod 5) \Rightarrow 4 x \equiv 8(\bmod 5) \underset{(4,5)=1}{\Rightarrow} x \equiv 2(\bmod 5), \\
x \equiv 1(\bmod 3) .
\end{array}\right.
$$

This yields the reduced system as follows:

$$
\left\{\begin{array}{c}
x \equiv 8(\bmod 13) \\
x \equiv 2(\bmod 5) \\
x \equiv 1(\bmod 3)
\end{array}\right.
$$

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 $x \equiv 8(\bmod 13)$. We can rewrite it via such equality:

$$
\begin{equation*}
x=8+13 t_{1} . \tag{*}
\end{equation*}
$$

Since $x$ is a solution for every congruences, we substitute it into the second congruence and deduce value for unknown $t_{1}$ :

$$
\begin{aligned}
& 8+13 t_{1}=2(\bmod 5) \Rightarrow 13 t_{1} \equiv-6(\bmod 5) \Rightarrow \\
\Rightarrow & 3 t_{1} \equiv-6+5 \cdot 3(\bmod 5) \Rightarrow 3 t_{1} \equiv 9(\bmod 5) .
\end{aligned}
$$

Taking into account that $(3,5)=1$, we divide both parts of the congruence by 3 :
$t_{1} \equiv 3(\bmod 5)$, this yields $t_{1}=3+5 t_{2}$.
Then we substitute $t_{1}$ into formula (*); this produces

$$
x=8+13\left(3+5 t_{2}\right)=8+39+13 \cdot 5 t_{2}=47+13 \cdot 5 t_{2}
$$

$$
x \equiv 47(\bmod 13 \cdot 5)
$$

We get

$$
\begin{equation*}
x=47+13 \cdot 5 t_{2} . \tag{**}
\end{equation*}
$$

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

$$
\begin{aligned}
& 47+13 \cdot 5 t_{2} \equiv 1(\bmod 3) \Rightarrow 65 t_{2} \equiv-46(\bmod 3) \Rightarrow \\
\Rightarrow & -t_{2} \equiv-1(\bmod 3) \Rightarrow t_{2} \equiv 1(\bmod 3) \Rightarrow t_{2}=1+3 t_{3} .
\end{aligned}
$$

If we replace $t_{2}$ by its expression in $\left({ }^{* *}\right)$, we obtain

$$
x=47+13 \cdot 5\left(1+3 t_{3}\right)=47+65+13 \cdot 5 \cdot 3 t_{3}=112+13 \cdot 5 \cdot 3 t_{3} .
$$

Thus we have

$$
x \equiv 112(\bmod 13 \cdot 5 \cdot 3) \text { or } x \equiv 112(\bmod 195)
$$

## Answer

$$
x \equiv 112(\bmod 195)
$$

## Solution check

$$
\left\{\begin{array}{l}
2 \cdot 112=224=13 \cdot 17+3 \Rightarrow 2 \cdot 112 \equiv 3(\bmod 13) \\
4 \cdot 112=448 \equiv 3(\bmod 5) \\
112=3 \cdot 37+1 \Rightarrow 112 \equiv 1(\bmod 3)
\end{array}\right.
$$

Solution is correct.

## Remark

1. If in the system (1) there is a congruence $a_{i} x \equiv b_{i}\left(\bmod m_{i}\right)$ possessing properties $\left(a_{i}, m_{i}\right)=d>1, d \mid b_{i}$, 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: $x \equiv c_{i}+t_{j} \frac{m_{i}}{d}\left(\bmod m_{i}\right), \quad t_{j}=\overline{0,(d-1)}$. 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

$$
\left\{\begin{array}{l}
x \equiv c_{1}\left(\bmod m_{1}\right), \\
x \equiv c_{2}\left(\bmod m_{2}\right)
\end{array}\right.
$$

is solvable iff two conditions hold $\left(m_{1}, m_{2}\right)=d>1$ 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. | 2. | 3. | 4. | 5. | 6. |
| :--- | :--- | :--- | :--- | :--- | :--- |
| $a=142$, | $a=137$, | $a=95$, | $a=37$, | $a=37$, | $a=113$, |
| $m=439$ | $m=932$ | $m=308$ | $m=107$ | $m=217$ | $m=311$ |
| 7. | 8. | 9. | 10. | 11. | 12. |
| $a=221$, | $a=41$, | $a=31$, | $a=93$, | $a=23$, | $a=137$, |
| $m=367$ | $m=101$ | $m=142$ | $m=133$ | $m=691$ | $m=323$ |
| 13. | 14. | 15. | 16. | 17. | 18. |
| $a=97$, | $a=101$, | $a=103$, | $a=91$, | $a=137$, | $a=59$, |
| $m=323$ | $m=931$ | $m=1031$ | $m=323$ | $m=837$ | $m=311$ |
| 19. | 20. | 21. | 22. | 23. | 24. |
| $a=97$, | $a=113$, | $a=89$, | $a=47$, | $a=67$, | $a=64$, |
| $m=433$ | $m=923$ | $m=323$ | $m=311$ | $m=691$ | $m=531$ |
| 25. | 26. | 27. | 28. | 29. | 30. |
| $a=64$, | $a=71$, | $a=83$, | $a=93$, | $a=128$, | $a=29$, |
| $m=743$ | $m=531$ | $m=323$ | $m=531$ | $m=1025$ | $m=531$ |
|  |  |  |  |  |  |

## Problem 2

Solve the system of congruences, simplifying it first.

1. $\left\{\begin{array}{l}913 x \equiv 132(\bmod 17), \\ 138 x \equiv 245(\bmod 19), \\ 457 x \equiv 623(\bmod 13) .\end{array}\right.$
2. $\left\{\begin{array}{l}913 x \equiv 132(\bmod 23), \\ 138 x \equiv 245(\bmod 11), \\ 457 x \equiv 623(\bmod 17) .\end{array}\right.$
3. $\left\{\begin{array}{l}913 x \equiv 132(\bmod 29), \\ 138 x \equiv 245(\bmod 17), \\ 457 x \equiv 623(\bmod 23),\end{array}\right.$
4. $\left\{\begin{aligned} 253 x & \equiv 429(\bmod 17), \\ 338 x & \equiv 545(\bmod 19), \\ 579 x & \equiv 741(\bmod 13) .\end{aligned}\right.$
5. $\left\{\begin{aligned} 253 x & \equiv 429(\bmod 31), \\ 338 x & \equiv 545(\bmod 23), \\ 579 x & \equiv 741(\bmod 19) .\end{aligned}\right.$
6. $\left\{\begin{aligned} 253 x & \equiv 429(\bmod 37), \\ 338 x & \equiv 545(\bmod 29), \\ 579 x & \equiv 741(\bmod 23) .\end{aligned}\right.$
7. $\left\{\begin{array}{l}353 x \equiv 529(\bmod 17), \\ 138 x \equiv 945(\bmod 19), \\ 279 x \equiv 241(\bmod 13) .\end{array}\right.$
8. $\left\{\begin{array}{l}353 x \equiv 529(\bmod 31), \\ 137 x \equiv 945(\bmod 23), \\ 279 x \equiv 241(\bmod 17) .\end{array}\right.$
9. $\left\{\begin{array}{l}353 x \equiv 529(\bmod 37), \\ 137 x \equiv 945(\bmod 17), \\ 279 x \equiv 241(\bmod 23) .\end{array}\right.$
10. $\left\{\begin{array}{l}347 x \equiv 519(\bmod 17), \\ 438 x \equiv 345(\bmod 29), \\ 271 x \equiv 541(\bmod 37) .\end{array}\right.$
11. $\left\{\begin{array}{l}347 x \equiv 519(\bmod 31), \\ 438 x \equiv 327(\bmod 23), \\ 271 x \equiv 541(\bmod 19) .\end{array}\right.$
12. $\left\{\begin{array}{l}347 x \equiv 519(\bmod 37), \\ 438 x \equiv 327(\bmod 17), \\ 271 x \equiv 541(\bmod 23) .\end{array}\right.$
13. $\left\{\begin{array}{l}547 x \equiv 219(\bmod 17), \\ 639 x \equiv 175(\bmod 29), \\ 371 x \equiv 341(\bmod 37) .\end{array}\right.$
14. $\left\{\begin{array}{l}547 x \equiv 219(\bmod 31), \\ 638 x \equiv 145(\bmod 23), \\ 371 x \equiv 341(\bmod 19) .\end{array}\right.$
15. $\left\{\begin{array}{l}547 x \equiv 219(\bmod 37), \\ 638 x \equiv 145(\bmod 17), \\ 371 x \equiv 341(\bmod 23) .\end{array}\right.$
16. $\left\{\begin{array}{l}747 x \equiv 319(\bmod 17), \\ 838 x \equiv 195(\bmod 29), \\ 571 x \equiv 241(\bmod 37) .\end{array}\right.$
17. $\left\{\begin{array}{l}747 x \equiv 319(\bmod 31), \\ 838 x \equiv 195(\bmod 23), \\ 571 x \equiv 241(\bmod 19) .\end{array}\right.$
18. $\left\{\begin{array}{l}747 x \equiv 319(\bmod 37), \\ 838 x \equiv 195(\bmod 17), \\ 571 x \equiv 241(\bmod 23) .\end{array}\right.$
19. $\left\{\begin{array}{l}437 x \equiv 719(\bmod 17), \\ 925 x \equiv 395(\bmod 29), \\ 771 x \equiv 225(\bmod 37) .\end{array}\right.$
20. $\left\{\begin{array}{l}437 x \equiv 719(\bmod 31), \\ 925 x \equiv 395(\bmod 23), \\ 771 x \equiv 225(\bmod 41) .\end{array}\right.$
21. $\left\{\begin{array}{l}437 x \equiv 719(\bmod 37), \\ 925 x \equiv 395(\bmod 17), \\ 771 x \equiv 225(\bmod 23) .\end{array}\right.$
22. $\left\{\begin{array}{c}333 x \equiv 579(\bmod 17), \\ 1025 x \equiv 495(\bmod 29), \\ 797 x \equiv 245(\bmod 37) .\end{array}\right.$
23. $\left\{\begin{array}{c}333 x \equiv 579(\bmod 31), \\ 1025 x \equiv 495(\bmod 23), \\ 797 x \equiv 245(\bmod 41) .\end{array}\right.$
24. $\left\{\begin{array}{l}337 x \equiv 525(\bmod 37), \\ 1025 x \equiv 495(\bmod 17), \\ 797 x \equiv 245(\bmod 23) .\end{array}\right.$
25. $\left\{\begin{array}{l}733 x \equiv 571(\bmod 17), \\ 625 x \equiv 405(\bmod 29), \\ 707 x \equiv 295(\bmod 37) .\end{array}\right.$
26. $\left\{\begin{array}{l}733 x \equiv 571(\bmod 31), \\ 625 x \equiv 405(\bmod 23), \\ 707 x \equiv 295(\bmod 19) .\end{array}\right.$
27. $\left\{\begin{array}{l}733 x \equiv 571(\bmod 37), \\ 625 x \equiv 405(\bmod 17), \\ 707 x \equiv 295(\bmod 23) .\end{array}\right.$
28. $\left\{\begin{array}{l}398 x \equiv 171(\bmod 17), \\ 925 x \equiv 605(\bmod 29), \\ 507 x \equiv 395(\bmod 37) .\end{array}\right.$
29. $\left\{\begin{array}{l}398 x \equiv 171(\bmod 31), \\ 925 x \equiv 605(\bmod 19), \\ 507 x \equiv 395(\bmod 11) .\end{array}\right.$
30. $\left\{\begin{array}{l}398 x \equiv 171(\bmod 11), \\ 925 x \equiv 605(\bmod 13), \\ 507 x \equiv 395(\bmod 41) .\end{array}\right.$

## 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 pecypc]. - Режим доступу : safo@problemsolvings.com.
4. Collins Darren C. Continued Fraction / Darren C. Collins // MIT Undegraduate Journal of Mathematics.

Навчальне видання

## Елементи теорї̈ чисел

Конспект лекцій та контрольні завдання для студентів напрямів підготовки 6.04030101 „Прикладна математика" та 6.040302 „Інформатика" ycix форм навчання
(Англомовний курс)

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

Формат $60 \times 84 / 16$. 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.

