

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Локтионова Оксана Геннадьевна  
Должность: проректор по учебной работе  
Дата подписания: 08.02.2021 16:53:45  
Уникальный программный ключ:  
0b817ca911e6668abb13a5d426d39e91fc11eabb75e945df4a4851faa56d089

## МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Юго-Западный государственный университет»  
(ЮЗГУ)

Кафедра «Информационная безопасность»

УТВЕРЖДАЮ

Проректор по учебной работе

О.Г. Локтионова

2016 г.



## СРАВНЕНИЯ

Методические указания по выполнению практической работы  
для студентов специальностей 10.05.03, 10.05.02, 10.03.01

Курск 2016

УДК 511.172

Составитель М.А. Ефремов

Рецензент

Кандидат технических наук, доцент *М.О. Таныгин*

**Сравнения:** методические указания по выполнению практической работы / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов. Курск, 2016. 15 с. Библиогр.: с. 15.

Содержат основные теоретические сведения о сравнениях и способах их решения. Указывается порядок выполнения работы, правила оформления и содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по образованию в области информационной безопасности (УМО ИБ).

Предназначены для студентов специальностей 10.05.03, 10.05.02, 10.03.01 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.  
Усл.печ. л. . Уч.-изд.л. . Тираж 30 экз. Заказ. Бесплатно.  
Юго-Западный государственный университет.  
305040, г. Курск, ул. 50 лет Октября, 94.

**СОДЕРЖАНИЕ**

1. ЦЕЛЬ РАБОТЫ	4
2. ЗАДАНИЕ	4
3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ	4
4. СОДЕРЖАНИЕ ОТЧЕТА	4
5. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ	5
5.1. Определения	5
5.2. Свойства равенства по модулю	5
5.3. Связанные определения	6
5.3.1. Классы вычетов	6
5.3.2. Свойства классов вычетов по модулю $m$	7
5.3.3. Системы вычетов	7
5.4. Решение сравнений первой степени	8
6. ПРАКТИЧЕСКИЕ ЗАДАНИЯ	12
7. КОНТРОЛЬНЫЕ ВОПРОСЫ	14
8. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ	15

## **1. ЦЕЛЬ РАБОТЫ**

Цель лабораторной работы – изучив теоретический материал, научиться решать сравнения различными способами.

## **2. ЗАДАНИЕ**

Ознакомиться с теоретическим материалом. Решить сравнения одним из описанных способов. Оформить отчет.

## **3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ**

1. Получить задание.
2. Изучить теоретическую часть.
3. Решить сравнения под номером, соответствующим номеру по журналу.
4. Составить отчет.

## **4. СОДЕРЖАНИЕ ОТЧЕТА**

1. Титульный лист.
2. Краткая теория.
3. Решение сравнений.
4. Вывод.

## 5. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

### 5.1. Определения

Два целых числа  $a$  и  $b$  сравнимы по модулю натурального числа  $n$  (или равноостаточны при делении на  $n$ ), если при делении на  $n$  они дают одинаковые остатки.

Эквивалентные формулировки:  $a$  и  $b$  сравнимы по модулю  $n$ , если их разность  $a-b$  делится на  $n$ , или если  $a$  может быть представлено в виде  $a = b + kn$ , где  $k$  — некоторое целое число. Например: 32 и -10 сравнимы по модулю 7, так как

$$32 = 7 \cdot 4 + 4 \text{ и } -10 = 7 \cdot (-2) + 4$$

Утверждение “ $a$  и  $b$  сравнимы по модулю  $n$ ” записывается в виде:

$$a \equiv b \pmod{n}$$

### 5.2. Свойства равенства по модулю

Отношение сравнения по модулю обладает свойствами

- рефлексивности: для любого целого  $a$  справедливо  $a \equiv a \pmod{n}$
- симметричности: если  $a \equiv b \pmod{n}$  то  $b \equiv a \pmod{n}$
- транзитивности: если  $a \equiv b \pmod{n}$  и  $b \equiv c \pmod{n}$ , то  $a \equiv c \pmod{n}$

Любые два целых числа  $a$  и  $b$  сравнимы по модулю 1.

Для того, чтобы числа  $a$  и  $b$  были сравнимы по модулю  $n$ , необходимо и достаточно, чтобы их разность делилась на  $n$ .

Если числа  $a_1, a_2, \dots, a_n$  и  $b_1, b_2, \dots, b_n$  попарно сравнимы по модулю  $n$ , то их суммы  $a_1+a_2+\dots+a_n$  и  $b_1+b_2+\dots+b_n$ , а также произведения  $a_1 \cdot a_2 \cdot \dots \cdot a_n$  и  $b_1 \cdot b_2 \cdot \dots \cdot b_n$  тоже сравнимы по модулю  $n$ .

Если числа  $a$  и  $b$  сравнимы по модулю  $n$ , то их степени  $a^k$  и  $b^k$  тоже сравнимы по модулю  $n$  при любом натуральном  $k$ .

Если числа  $a$  и  $b$  сравнимы по модулю  $n$ , и  $n$  делится на  $m$ , то  $a$  и  $b$  сравнимы по модулю  $m$ .

Для того, чтобы числа  $a$  и  $b$  были сравнимы по модулю  $n$ , представленному в виде его канонического разложения на простые сомножители  $p_i$

$$n = \prod_{i=1}^n p_i^{\alpha_i}$$

необходимо и достаточно, чтобы

$$a \equiv b \pmod{p_i^{\alpha_i}}, \quad i = 1, 2, \dots, n$$

Отношение сравнения является отношением эквивалентности и обладает многими свойствами обычных равенств. Например, их можно складывать и перемножать: если

$$\begin{aligned} a_1 &\equiv b_1 \pmod{n}; & a_2 &\equiv b_2 \pmod{n}, & \text{то} \\ a_1 a_2 &\equiv b_1 b_2 \pmod{n}; & a_1 + a_2 &\equiv b_1 + b_2 \pmod{n}; \end{aligned}$$

Сравнения нельзя делить друг на друга или на другие числа. Пример:  $14 \equiv 20 \pmod{6}$ , однако, сократив на 2, мы получаем ошибочное сравнение:  $7 \equiv 10 \pmod{6}$ . Правила сокращения для сравнений следующие.

- Можно делить обе части сравнения на число, взаимно простое с модулем: если  $ac \equiv bc \pmod{n}$  и  $\text{НОД}(c, n) = 1$ , то  $a \equiv b \pmod{n}$ .
- Можно одновременно разделить обе части сравнения и модуль на их общий делитель: если  $ac \equiv bc \pmod{n}$ , то  $a \equiv b \pmod{n}$ .

Нельзя также выполнять операции со сравнениями, если их модули не совпадают.

Другие свойства:

- Если  $a \equiv b \pmod{m_1}$  и  $a \equiv b \pmod{m_2}$ , то  $a \equiv b \pmod{m}$ , где  $m = [m_1 \cdot m_2]$ .

### 5.3. Связанные определения

#### 5.3.1. Классы вычетов

Множество всех чисел, сравнимых с  $a$  по модулю  $n$  называется классом вычетов  $a$  по модулю  $n$ , и обычно обозначается  $[a]_n$  или  $\bar{a}_n$ . Таким образом, сравнение  $a \equiv b \pmod{n}$  равносильно равенству классов вычетов  $[a]_n = [b]_n$ .

Поскольку сравнение по модулю  $n$  является отношением эквивалентности на множестве целых чисел  $\mathbb{Z}$ , то классы вычетов по модулю  $n$  представляют собой классы эквивалентности; их количество равно  $n$ . Множество всех классов вычетов по модулю  $n$  обозначается  $\mathbb{Z}_n$  или  $\mathbb{Z}/n\mathbb{Z}$ .

Операции сложения и умножения на  $\mathbb{Z}$  индуцируют соответствующие операции на множестве  $\mathbb{Z}_n$ :

$$\begin{aligned} [a]_n + [b]_n &= [a + b]_n \\ [a]_n \cdot [b]_n &= [a \cdot b]_n \end{aligned}$$

Относительно этих операций множество  $\mathbb{Z}_n$  является конечным кольцом, а если  $n$  простое — конечным полем.

### 5.3.2. Свойства классов вычетов по модулю $m$

1. Для того, чтобы  $a \equiv b \pmod{m}$ , необходимо и достаточно, чтобы  $\bar{a} = \bar{b}$ .
2. Для того, чтобы  $a \not\equiv b \pmod{m}$ , необходимо и достаточно, чтобы  $\bar{a} \cap \bar{b} = \emptyset$ .
3. Любые  $m$  чисел, попарно не сравнимые по модулю  $m$ , образуют полную систему вычетов.
4. Если  $(a, m) = 1$  и  $x$  пробегает полную систему вычетов по модулю  $m$ , то  $ax + b$ ,  $b \in \mathbb{Z}$ , также пробегает полную систему вычетов по модулю  $m$ .
5. Если  $(a, m) = 1$  и  $x$  пробегает приведённую систему вычетов по модулю  $m$ , то  $ax$ , также пробегает приведённую систему вычетов по модулю  $m$ .

### 5.3.3. Системы вычетов

Система вычетов позволяет осуществлять арифметические операции над конечным набором чисел, не выходя за его пределы. Полная система вычетов по модулю  $n$  — любой набор из  $n$  не сравнимых между собой по модулю  $n$  целых чисел. Обычно в качестве полной системы вычетов по модулю  $n$  берутся наименьшие неотрицательные вычеты

$$0, 1, \dots, n - 1$$

или абсолютно наименьшие вычеты, состоящие из чисел

$$0, \pm 1, \pm 2, \dots, \pm \frac{n-1}{2},$$

в случае нечётного  $n$  и чисел

$$0, \pm 1, \pm 2, \dots, \pm \left(\frac{n}{2} - 1\right), \frac{n}{2}$$

в случае чётного  $n$ .

Набор не сравнимых чисел, взаимно простых с  $n$ , называется приведённой системой вычетов.

### 5.4. Решение сравнений первой степени

В теории чисел, криптографии и других областях науки часто возникает задача отыскания решений сравнения первой степени вида

$$ax \equiv b \pmod{m}$$

Решить сравнение – значит найти все те  $x$ , которые удовлетворяют данному сравнению, при этом весь класс чисел по  $\pmod{m}$  считается за одно решение.

Решение такого сравнения начинается с вычисления НОД( $a, m$ )= $d$ . При этом возможны 2 случая:

- Если  $b$  не кратно  $d$ , то у сравнения нет решений.
- Если  $b$  кратно  $d$ , то у сравнения существует единственное решение по модулю  $\frac{m}{d}$ , или, что то же самое,  $d$  решений по модулю  $m$ . В этом случае в результате сокращения исходного сравнения на  $d$  получается сравнение:

$$a_1x \equiv b_1 \pmod{m_1},$$

где  $a_1 = \frac{a}{d}$ ,  $b_1 = \frac{b}{d}$  и  $m_1 = \frac{m}{d}$  являются целыми числами, причем  $a_1$  и  $m_1$  взаимно просты. Поэтому число  $a_1$  можно обратить по модулю  $m_1$ , то есть найти такое число  $s$ , что  $s \cdot a_1 \equiv 1 \pmod{m_1}$  (другими словами,  $s \equiv a_1^{-1} \pmod{m_1}$ ). Теперь решение находится умножением полученного сравнения на  $s$

$$x \equiv sa_1x \equiv sb_1 \equiv a_1^{-1}b_1 \pmod{m_1}$$

Практическое вычисление значения  $s$  можно осуществить разными способами:  $s$  с помощью теоремы Эйлера, алгоритма Евклида, теории цепных дробей.

В частности, теорема Эйлера позволяет записать значение  $s$  в виде:

$$s \equiv a_1^{-1} \equiv a_1^{\varphi(m_1)-1} \pmod{m_1}$$

Пример.

Для сравнения

$$4x \equiv 26 \pmod{22}$$

имеем  $d = 2$ , поэтому по модулю 22 сравнение имеет два решения. Заменим 26 на 4, сравнимое с ним по модулю 22,

$$4x \equiv 4 \pmod{22}$$

и затем сократим все три числа на 2:

$$2x \equiv 2 \pmod{11}$$



Поскольку 2 взаимно просто с модулем 11, можно сократить левую и правую части на 2. В итоге получаем одно решение по модулю 11

$$x \equiv 1(\text{mod } 11),$$

эквивалентное двум решениям по модулю 22:

$$x \equiv 1(\text{mod } 22) \text{ и } x \equiv 12(\text{mod } 22).$$

Алгоритм решения сравнения  $ax \equiv b(\text{mod } n)$  со взаимно простыми  $a$  и  $n$  состоит из двух частей:

1. Решаем сравнение  $ax \equiv 1(\text{mod } n)$ . Для этого при помощи расширенного алгоритма Евклида ищем решение  $(x_0, y_0)$  уравнения  $ax + ny = 1$ . Взяв по модулю  $n$  последнее равенство, получим  $ax_0 \equiv 1(\text{mod } n)$ .

2. Умножим на  $b$  равенство  $ax_0 \equiv 1(\text{mod } n)$ . Получим  $a(bx_0) \equiv b(\text{mod } n)$ , откуда решением исходного сравнения  $ax \equiv b(\text{mod } n)$  будет  $x \equiv bx_0(\text{mod } n)$

Лемма.

Если  $\text{НОД}(k,m)=1$ , то равенство  $ak \equiv bk(\text{mod } m)$  эквивалентно  $a \equiv b(\text{mod } m)$ .

Доказательство.

Из  $ak \equiv bk(\text{mod } m)$   $ak = bk (\text{mod } m)$  следует, что  $(a - b) \cdot k$  делится на  $m$ . Но поскольку  $k$  и  $m$  взаимно просты, то  $a - b$  делится на  $m$ , то есть  $a \equiv b(\text{mod } m)$ .

Пример 1.

Решить сравнение  $5x \equiv 26(\text{mod } 12)$ .

Решение.  $d = (5,12) = 1$ , следовательно, сравнение имеет единственное решение.

Способ №1. Решаем сравнение  $5U \equiv 1(\text{mod } 12)$ , где  $U$  – мультипликативно-обратный элемент к 5 по модулю 12.

$$\begin{array}{r}
 12 \mid 5 \\
 \hline
 \phantom{12} \phantom{\mid} 2 \\
 \phantom{12} \phantom{\mid} \phantom{2} \phantom{\mid} 5 \\
 \phantom{12} \phantom{\mid} \phantom{2} \phantom{\mid} \phantom{5} \phantom{\mid} 2 \\
 \phantom{12} \phantom{\mid} \phantom{2} \phantom{\mid} \phantom{5} \phantom{\mid} \phantom{2} \phantom{\mid} 1=(12,5) \\
 \phantom{12} \phantom{\mid} \phantom{2} \phantom{\mid} \phantom{5} \phantom{\mid} \phantom{2} \phantom{\mid} \phantom{1=(12,5)} \phantom{\mid} 2 \\
 \phantom{12} \phantom{\mid} \phantom{2} \phantom{\mid} \phantom{5} \phantom{\mid} \phantom{2} \phantom{\mid} \phantom{1=(12,5)} \phantom{\mid} \phantom{2} \phantom{\mid} 0
 \end{array}$$

i	Остатки	Частные	$x_i$	$y_i$
-1	12	-	1	0
0	5	-	0	1
1	2	2	$1-0*2=1$	$0-1*2=-2$
2	$1=d$	2	$0-1*2=-2$	$1-(-2)*2=5=U$
3	0	2	-	-

$$x \equiv 26 \cdot 5 \pmod{12} = 10 \pmod{12}$$

$$\begin{array}{r} 130 \quad | \quad 12 \\ \hline \quad \quad | \quad 10 \\ \hline \quad \quad | \quad 0 \end{array}$$

$x \equiv 10 \pmod{12}$  – решение исходного сравнения.

Способ №2. (Способ Эйлера).

$$\varphi(12) = 4; U = 5^{4-1} = 5^3 = 125$$

$$x \equiv 26 \cdot 125 \pmod{12} = 3250 \pmod{12} = 10 \pmod{12}$$

$$x \equiv 10 \pmod{12}$$

Пример 2. Решить сравнение  $2775x \equiv 825 \pmod{624}$

Решение.

$$\begin{array}{r} 2775 \quad | \quad 624 \\ \hline \quad \quad | \quad 4 \\ \hline 279 \end{array}$$

$$\begin{array}{r} 825 \quad | \quad 624 \\ \hline \quad \quad | \quad 1 \\ \hline 201 \end{array}$$

$$2775 \equiv 825 \pmod{624} \Leftrightarrow 279x \equiv 201 \pmod{12}$$

$$\begin{array}{r} \phantom{624} \quad | \quad 279 \\ \phantom{624} \quad | \quad 2 \\ \hline 279 \quad | \quad 66 \\ \phantom{279} \quad | \quad 4 \\ \hline 66 \quad | \quad 15 \\ \phantom{66} \quad | \quad 4 \\ \hline 15 \quad | \quad 6 \\ \phantom{15} \quad | \quad 2 \\ \hline 6 \quad | \quad 3=(624,279)=d \\ \phantom{6} \quad | \quad 2 \\ \hline 0 \end{array}$$

$d=3|201$ , следовательно, сравнение  $279x \equiv 201(\text{mod}12)$ , а, значит, и исходное сравнение, разрешимо и имеет 3 решения по модулю 624.

$$\left. \begin{array}{l} 279 = 3 \cdot 93 \\ 624 = 3 \cdot 208 \\ 201 = 3 \cdot 67 \end{array} \right\} \Rightarrow 279x \equiv 201(\text{mod}12) \Leftrightarrow 93x \equiv 67(\text{mod}208)$$

$$\begin{array}{r} 208 \quad | \quad 93 \\ 186 \quad | \quad 2 \\ \hline 93 \quad | \quad 22 \\ 88 \quad | \quad 4 \\ \hline 22 \quad | \quad 5 \\ 20 \quad | \quad 4 \\ \hline 5 \quad | \quad 2 \\ 4 \quad | \quad 2 \\ \hline 2 \quad | \quad 1=(208,93)=d \\ 2 \quad | \quad 2 \\ \hline 0 \end{array}$$

С помощью расширенного алгоритма Евклида находим мультипликативно-обратный элемент  $U$  к 93 по модулю 208.

$i$	Остатки	Частные	$x_i$	$y_i$
-1	208	-	1	1
0	93	-	0	0
1	22	2	$1-0*2=1$	$0-1*2=-2$
2	5	4	$0-1*4=-4$	$1-(-2)*4$
3	2	4	$1-(-4)*4=17$	$-2-9*4=-38$
4	$1=d$	2	$-4-17*2=-38$	$9-(-38)*2=85=dU$
5	0	2	-	-

$$x_1 = 67 \cdot 85(\text{mod}208) = 5695(\text{mod}208) = 79$$

$$x_2 = 79 + 208 = 287$$

$$x_3 = 79 + 2 \cdot 208 = 495$$

**6. ПРАКТИЧЕСКИЕ ЗАДАНИЯ**

- №1.  $2781x \equiv 1452 \pmod{951}$   
№2.  $5980x \equiv 2300 \pmod{1555}$   
№3.  $2703x \equiv 597 \pmod{1011}$   
№4.  $3370x \equiv 1355 \pmod{1835}$   
№5.  $4272x \equiv 1686 \pmod{1167}$   
№6.  $3249x \equiv 1674 \pmod{1203}$   
№7.  $3393x \equiv 1836 \pmod{1293}$   
№8.  $3507x \equiv 573 \pmod{1329}$   
№9.  $3681x \equiv 1950 \pmod{1371}$   
№10.  $3336x \equiv 844 \pmod{2012}$   
№11.  $2652x \equiv 2304 \pmod{1461}$   
№12.  $2930x \equiv 1560 \pmod{1046}$   
№13.  $4023x \equiv 2160 \pmod{1437}$   
№14.  $3837x \equiv 753 \pmod{1389}$   
№15.  $2610x \equiv 2304 \pmod{1383}$   
№16.  $2155x \equiv 3560 \pmod{2215}$   
№17.  $2958x \equiv 1608 \pmod{1126}$   
№18.  $3086x \equiv 2838 \pmod{1142}$   
№19.  $2760x \equiv 2340 \pmod{1497}$   
№20.  $3090x \equiv 1592 \pmod{1114}$   
№21.  $4395x \equiv 2610 \pmod{1555}$   
№22.  $3948x \equiv 2496 \pmod{1388}$   
№23.  $3435x \equiv 2106 \pmod{1257}$   
№24.  $2160x \equiv 807 \pmod{1317}$   
№25.  $3550x \equiv 3390 \pmod{1985}$   
№26.  $3915x \equiv 2358 \pmod{1437}$   
№27.  $2720x \equiv 2640 \pmod{1636}$

- №28.  $3507x \equiv 573 \pmod{1329}$
- №29.  $3681x \equiv 1950 \pmod{1371}$
- №30.  $3336x \equiv 844 \pmod{2012}$
- №31.  $2652x \equiv 2304 \pmod{1461}$
- №32.  $2930x \equiv 1560 \pmod{1046}$
- №33.  $4023x \equiv 2160 \pmod{1437}$
- №34.  $3837x \equiv 753 \pmod{1389}$
- №35.  $2610x \equiv 2304 \pmod{1383}$
- №36.  $2155x \equiv 3560 \pmod{2215}$
- №37.  $2958x \equiv 1608 \pmod{1126}$
- №38.  $3086x \equiv 2838 \pmod{1142}$
- №39.  $2760x \equiv 2340 \pmod{1497}$
- №40.  $3090x \equiv 1592 \pmod{1114}$
- №41.  $4395x \equiv 2610 \pmod{1555}$
- №42.  $3948x \equiv 2496 \pmod{1388}$
- №43.  $3435x \equiv 2106 \pmod{1257}$
- №44.  $2160x \equiv 807 \pmod{1317}$
- №45.  $3550x \equiv 3390 \pmod{1985}$
- №46.  $3915x \equiv 2358 \pmod{1437}$
- №47.  $2720x \equiv 2640 \pmod{1636}$
- №48.  $4272x \equiv 1686 \pmod{1167}$
- №49.  $3249x \equiv 1674 \pmod{1203}$
- №50.  $3393x \equiv 1836 \pmod{1293}$

## 7. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое взаимно простые числа?
2. Перечислите свойства сравнений.
3. Что такое классы вычетов?
4. Назовите свойства классов вычетов.
5. Что такое полная и приведённая системы вычетов?
6. Что такое мультипликативно-обратные по модулю элементы?
7. Функция Эйлера и её свойства.
8. Что такое мультипликативные функции?
9. Какова формула для вычисления функции Эйлера.
10. Назовите условия разрешимости сравнения.

## 8. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Александров В.А., Горшенин С.М. Задачник – практикум по теории чисел. М.: Учпедгиз, 1972.
2. Виноградов И.М. Основы теории чисел. М.: Наука, 1995.
3. Гайнов А.Т. Теория чисел. Изд - во НГУ, 1995.
4. Галочкин А.И., Нестеренко Н.В., Шидловский А.Б. Введение в теорию чисел. Изд - во МГУ, 1995.
5. Кудреватов Г.А. Сборник задач по теории чисел. М.: Просвещение, 1970.
6. Ляпин С.Е., Баранова И.В., Борчугова З.Г. Сборник задач по элементарной математике. М.: Просвещение, 1973.
7. Пензин Ю.Г., Клейменов В.Ф. Сравнения. Учебно-методические разработки (тексты лекций). Изд-во ИГУ, 1998.
8. И.М. Виноградов «Элементы высшей математики» М., «Высшая школа», 1999
9. Л.Я. Куликов, А.И. Москаленко, А.А. Фомин «Сборник задач по алгебре и теории чисел» М., «Просвещение», 1993
10. Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Ажевич «Математические и компьютерные основы криптологии» Минск, «Новое знание», 2003