ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

ГОУ ВПО "НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ
ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ"

**А.И.Кузьмичёв, М.П.Тропин**

# ТЕОРИЯ ЧИСЕЛ

Задачник-практикум для студентов 3-го курса

Новосибирск 2009

УДК 511(075.8)
ББК 22.13я73-4
К893

Печатается по решению
Редакционно-издательского
совета НГПУ

Р е ц е н з е н т ы :
кандидат физико-математических наук, старший
научный сотрудник ИМ СО РАН
*М.В.Нещадим;*
кандидат физико-математических наук, доцент
кафедры алгебры НГПУ
*Ю.В.Сосновский;*
Н а у ч н ы й р е д а к т о р :
кандидат физико-математических наук, заведующий
кафедрой алгебры НГПУ
*М.П.Тропин*

**Кузьмичёв, А.И.**

К893 Теория чисел: задачник-практикум для студентов 3-го курса/ А.И.Кузьмичёв, М.П.Тропин. – Новосибирск: Изд. НГПУ, 2009. – 119 с.

Пособие входит в серию «Учебно-дидактические комплексы кафедры алгебры». В нём рассмотрены такие темы, как «Сравнения и вычеты», «Диофантовы уравнения», «Цепные дроби», «Первообразные корни и индексы», «Арифметические приложения». Задачник является дополнением к пособию Тропина М.П. «Теория чисел: курс лекций для студентов математического факультета» (Изд.НГПУ, 2006).

Пособие предназначено для преподавателей и студентов математических специальностей педагогических вузов. Оно может быть использовано для проведения практических занятий и организации самостоятельной работы студентов по теории чисел.

**УДК 511(075.8)**

**ББК 22.13я73-4**

# *ТЕМА 1.* СРАВНЕНИЯ И ВЫЧЕТЫ

## §1. Делимость и простые числа

**Определение.** Говорят, что целое число $a$ *делится* на целое число $b$, если существует такое $q \in \mathbb{Z}$, что $a = bq$. Коротко этот факт записывается так:

$$a \vdots b .$$

Число $a$ называется *делимым*, $b$ – *делителем*, а $q$ – *частным.*

**Теорема** (простейшие свойства делимости). *Для любых целых чисел* $a, b, c$ *выполняются следующие свойства.*

*1)* $a \vdots a$ *(рефлексивность);*

*2) если* $a \vdots b,\ b \vdots c$, *то* $a \vdots c$ *(транзитивность);*

*3) если* $a \vdots c,\ b \vdots c$, *то* $(a \pm b) \vdots c$;

*4) если* $a \vdots c$, *то* $ab \vdots c$;

*5) если* $a \vdots b$, *то* $\pm a \vdots \pm b$ *(делимость не зависит от сомножителя* $\pm 1$*);*

*6)* $0 \vdots a,\ a \vdots \pm 1,\ a \vdots \pm a$ *(тривиальные делимости);*

*7) если* $a \vdots b,\ a \neq 0$, *то* $|a| \geq |b|$.

**Определение.** Числа $a$ и $b$ называются *взаимно простыми,* если они не имеют других общих делителей кроме $\pm 1$. Или, другими словами, если $НОД(a, b) = 1$.

*8) Если* $ab \vdots c$ *и числа* $a$ *и* $c$ *взаимно просты, то* $b \vdots c$.

*9) Если* $a \vdots b,\ a \vdots c$ *и числа* $b, c$ *взаимно просты, то* $a \vdots bc$.

**Теорема** (о делении с остатком). *Для любых целых чисел* $a$ *и* $b$, $b \neq 0$, *существуют единственные целые числа* $q, r$ *такие, что*

$$\begin{cases} a = bq + r, \\ 0 \le r < |b|. \end{cases}$$

Теорема о делении с остатком позволяет во многих задачах от чисел переходить к их остаткам, которые меньше по абсолютной величине.

**Свойства простых чисел:** *1) Всякое натуральное число* $n$ *и простое число* $p$ *либо взаимно просты, либо* $n \vdots p$.

*2) Если* $ab \vdots p$, $p$ *– простое число, то* $a \vdots p$ *или* $b \vdots p$.

*3) Число* $n$ *является простым тогда и только тогда, когда оно не имеет (простых) делителей, удовлетворяющих условию* $p \le \sqrt{n}$.

**Теорема** (основная теорема арифметики). *Всякое число* $n > 1$ *может быть разложено в произведение степеней простых сомножителей:*

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

*где* $p_1, p_2, \ldots, p_k$ *– попарно различные простые числа и* $\alpha_i \in \mathbb{N}$.

*Это разложение единственно с точностью до порядка сомножителей.*

Разложение такого вида называется *каноническим.* Оно позволяет получать достаточно сложные свойства целых чисел. Например, описать общий вид всех делителей целого числа, найти их количество, дать формулы для вычисления НОД и НОК.

**Теорема** (формула для делителей). *Если число* $n > 1$ *представлено в каноническом виде* $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ *и* $d$ *– некоторый его натуральный делитель, то* $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$ *для подходящих* $0 \le \beta_i \le \alpha_i,\ 1 \le i \le k$. *Количество различных натуральных делителей числа* $n$ *равно* $(\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \ldots \cdot (\alpha_k + 1)$.

**Теорема** (формулы для вычисления НОД и НОК). *Пусть даны два произвольных натуральных числа* $n, m > 1$ *и их согласованные канонические разложения*

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k},\quad m = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}.$$

*Пусть* $\gamma_i = \min(\alpha_i, \beta_i)$ *и* $\delta_i = \max(\alpha_i, \beta_i)$, *тогда*

$$НОД(n, m) = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \ldots \cdot p_k^{\gamma_k},\ НОК(n, m) = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot \ldots \cdot p_k^{\delta_k}.$$

## Занятие 1

**Теоретический материал.** Отношение делимости, его свойства. Теорема о делении с остатком. Простые числа, свойства простых чисел. Основная теорема арифметики, нахождение всех делителей числа, НОД и НОК двух чисел.

**Основные типы задач.** Проверка делимостей при помощи свойств, вычислении остатков от деления, разложение на простые сомножители, нахождение все делителей целого числа.

### Задания для практических занятий

**1.** Дайте определение отношения делимости целых чисел. Сформулируйте свойства отношения делимости, используемые для решения задач (сложение, умножение. возведение в квадрат делимостей).

**2.** Докажите, используя свойства делимости:

а) $\left(221^{45}+247\cdot 297\right)\vdots 13$;

б) $\left(\left(207^{11}\cdot 91^{19}-25^{13}\cdot 117^{12}\right)+7631\right)\vdots 13$;

в) $\left(221^{45}+247\cdot 289\right)\cdot\left(207^{10}\cdot 68^{11}-215^{13}\cdot 119^{12}\right)\vdots 17$;

г) $(391\cdot 393\cdot 395\cdot 397\cdot 399\cdot 401+585\cdot 587\cdot 589)\vdots 19$.

**3.** Сформулируйте теорему о делении с остатком.

**4.** Найдите остаток от деления $a$ на $b$:

а) $a=13518,\quad b=23$; б) $a=1318,\quad b=17$;

в) $a=-1318,\quad b=17$; г) $a=1318,\quad b=-17$;

д) $a=-1318,\quad b=-17$; е) $a=7^n-2,\quad b=7$;

ж) $a=38^{38},\quad b=7$.

**5.** Дайте определение простого числа. Сформулируйте признак простоты числа, алгоритм разложения числа на простые сомножители.

**6.** Разложите на простые сомножители:

а) 15015; б) 2431;

в) 43771; г) 5491.

**7.** Запишите формулу для делителей числа. Найдите все целые делители чисел:

а) $3^2\cdot 5^3$; б) $2\cdot 5\cdot 6^2$;

в) $12^3$; г) 991.

**8.** Запишите формулу для НОД и НОК двух чисел. Найдите НОД и НОК чисел:

а) $2^2 \cdot 5^3 \cdot 11^4$ и $2^3 \cdot 3^3 \cdot 11^2$;

б) $2^3 \cdot 3^4 \cdot 5^6$ и $3^3 \cdot 4^4 \cdot 6^6$;

в) $5^3 \cdot 11^2 \cdot 7^2$ и 1648801;

г) $7^3 \cdot 9^2 \cdot 13$ и 2790207.

## Дополнительные задания

**9.** Докажите, что:

а) $\left(11^{10}-1\right) \vdots 100$; б) $\left(66^3+34^3\right) \vdots 400$;

б) $\left(26^{30}-1\right) \vdots 3 \cdot 5 \cdot 7 \cdot 11$; г) $\left(222^{555}+555^{222}\right) \vdots 7$.

**10.** Докажите, что для любого натурального $n$:

а) $\left(10^{n+3}+10^n\right) \vdots 7$; б) $\left(10^n+18n-1\right) \vdots 27$;

в) $\left(3^{4n+3}-117\right) \vdots 10$; г) $\left(9^{2m+1}+8^{m+2}\right) \vdots 73$.

**11.** Докажите, что не могут быть квадратами целых чисел числа вида:

а) $3n+2$; б) $4n+2$;

в) $4n+3$; г) $5n+2$.

**12.** Найдите все целые числа, удовлетворяющие уравнению:

а) $(n+2)(m-3)=4$; б) $(n+1)(nm-1)=3$;

в) $n^2-4nm-5m^2=169$; г) $n^2=m^2+2m+13$.

**13.** Найдите все целые числа, при делении которых на 7 неполное частное оказывается равным остатку.

**14.** Найдите наибольшее натуральное число, которое при делении на 17 даёт неполное частное 5.

**15.** Докажите, что не имеет целых решений уравнение:

а) $x^2 - y^2 = 30$; б) $x^2 + 3y = 2$;

в) $3y^2 + 8 = x^2$; г) $3x^2 - 4y^2 = 13$.

## §2. Сравнения

**Определение.** Пусть $m$ произвольное натуральное число. Целые числа $a$ и $b$ называются *сравнимыми по модулю* $m$, если $(a-b) \vdots m$. Этот факт записывается так:

$$a \equiv b \pmod{m}.$$

Число $m$ называется *модулем.* Оно фиксируется в каждом конкретном случае. Можно считать, что $m > 1$, т.к. случай $m = 1$ тривиален.

**Пример.** $-50 \equiv 13 \pmod{7}$, т.к. $(-50-13) = -63 \vdots 7$;

$47 \not\equiv 18 \pmod{9}$, т.к. $(47-18) = 29 \not\vdots 9$.

**Теорема** (о признаках сравнимости).

*1)* $a \equiv b \pmod{m} \Leftrightarrow \exists\, t \ (a = b + mt)$;

*2)* $a \equiv b \pmod{m} \Leftrightarrow a, b$ *при делении на* $m$ *дают одинаковые остатки.*

**Свойства.** *Для любых целых чисел* $a, b, c$ *выполняются следующие свойства.*

*1)* $a \equiv a \pmod{m}$,

*2)* $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$,

*3)* $a \equiv b \pmod{m}$, $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$.

**Замечание.** Многократное применение транзитивности позволяет от цепочки сравнений

$$a_1 \equiv a_2 \equiv a_3 \equiv \ldots a_{n-1} \equiv a_n \pmod{m}$$

переходить к сравнению $a_1 \equiv a_n \pmod{m}$.

*4) Если* $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, *то* $a \pm c \equiv b \pm d \pmod{m}$, $ac \equiv bd \pmod{m}$, $a^n \equiv b^n \pmod{m}$, *т.е. верные сравнения можно почленно складывать, вычитать, умножать и возводить в степень.*

*5) Числа из одной части сравнения можно переносить в другую часть сравнения с противоположным знаком:*

$$a + b \equiv c \pmod{m} \Leftrightarrow a \equiv c - b \pmod{m}.$$

*6) К одной части сравнения можно добавлять числа, кратные* $m$ *:*

$$a \equiv b \pmod{m} \Rightarrow a + mc \equiv b \pmod{m}.$$

*7)* $ac \equiv bc \pmod{mc}$ *тогда и только тогда, когда* $a \equiv b \pmod{m}$.

*8) Если* $ac \equiv bc \pmod{m}$ *и* $c$ *взаимно просто с* $m$, *то* $a \equiv b \pmod{m}$.

*9) Если* $a \equiv b \pmod{m}$ *и* $m \vdots d$, *то* $a \equiv b \pmod{d}$.

*10) Если числа* $m_1$ *и* $m_2$ *взаимно просты, то*

$$a \equiv b \pmod{m_1 m_2} \Leftrightarrow \begin{cases} a \equiv b \pmod{m_1}, \\ a \equiv b \pmod{m_2}. \end{cases}$$

*11) Всякое число сравнимо по модулю* $m$ *со своим остатком от деления на* $m$ .

*12) Если* $a \equiv b \pmod{m}$, *то* $НОД(a, m) = НОД(b, m)$.

**Пример.** Найти остаток от деления числа $25^{25}$ на 11.

Составим цепочку сравнений по модулю 11, которая начинается с данного числа, а заканчивается числом $0 \le r < 11$, которое и будет искомым остатком согласно определению остатка и свойству 11.

$25^{25} \equiv 3^{25}$, т.к. $25 \equiv 3 (\mathrm{mod} 11)$;

$3^{25} = 27^8 \cdot 3$;

$27^8 \cdot 3 \equiv 5^8 \cdot 3 = 25^4 \cdot 3 \equiv 3^4 \cdot 3 = 243 \equiv 1 (\mathrm{mod} 11)$.

В результате $25^{25} \equiv 1 (\mathrm{mod} 11)$, и искомый остаток равен 1.

## Занятие 2

**Теоретический материал.** Сравнения, свойства сравнений. Признаки сравнимости.

**Основные типы задач.** Нахождение остатков от деления целых чисел.

### Задания для практических занятий

**16.** Дайте определение отношения сравнимости. Сформулируйте признаки сравнимости.

**17.** Проверьте истинность следующих соотношений:

а) $404 \equiv 5 (\mathrm{mod} 7)$; б) $409 \equiv -15 (\mathrm{mod} 8)$;

в) $5301 \equiv 485 (\mathrm{mod} 9)$; г) $41 \cdot 21 \equiv 51 \cdot 35 (\mathrm{mod} 14)$.

**18.** Запишите при помощи сравнений следующие высказывания:

а) остаток от деления числа $(-759)$ на 18 равен 3;

б) $m = 17k + 5,\ \ k \in Z$;

в) число 931 делится на 19;

г) последняя цифра десятичной записи числа $n$ равна 4;

д) десятичная запись числа $n$ оканчивается на 71.

**19.** Сформулируйте основные свойства сравнений (транзитивность, сложение, умножение сравнений, возведение сравнений в степень).

**20.** Проверьте, что:

а) $53 \cdot 201 \equiv 44 \cdot 21 (\mathrm{mod}\, 9)$;

б) $73^5 \cdot 284^8 \equiv 51^5 \cdot 31^8 \,(\mathrm{mod}\, 11)$;

в) $3^{2007} \equiv 3 (\mathrm{mod}\, 7)$;

г) $4^{2007} + 5^{2008} \equiv 3 (\mathrm{mod}\, 7)$.

**21.** Найдите остаток от деления числа $n$ на $m$:

а) $n = 3^{451},\ m = 10$;

б) $n = 312^{341},\ m = 11$;

в) $n = 372^{378} + 563^{207},\ m = 13$;

г) $n = 37^{89} \cdot 2^{378} + 5^{75} \cdot 61^{207},\ m = 7$.

**22.** Используя свойства сравнений, найдите последнюю цифру десятичной записи числа:

а) $373^{378} - 57^{207}$; б) $732^{78} - 59^{2007}$;

в) $123^{456} \cdot 7^{123} - 78^{910} \cdot 4^{44}$.

**23.** Докажите, что при любом натуральном $n$:

а) $\left(3^{3n+2}+2^{4n+1}\right)\vdots 11$; б) $\left(1+3^{3n+1}+9^{3n+1}\right)\vdots 13$;

в) $\left(6^{2n+1}+5^{n+2}\right)\vdots 31$; г) $\left(5^{2n+1}+2^{n+4}+2^{n+1}\right)\vdots 23$.

## Дополнительные задания

**24.** Докажите, что для любых целых $a$ и $b$:

а) если $a-5b\equiv 0(\mathrm{mod}19)$, то $10a+7b\equiv 0(\mathrm{mod}19)$;

б) если $3a\equiv 2b(\mathrm{mod}19)$, то $11a\equiv b(\mathrm{mod}19)$;

в) если $5a\equiv -2b(\mathrm{mod}11)$, то $6a-2b\equiv 0(\mathrm{mod}11)$;

г) если $3a-5b\equiv 0(\mathrm{mod}7)$, то $5a+b\equiv 0(\mathrm{mod}7)$.

**25.** Найдите остаток от деления числа $n$ на $m$:

а) $n=3^{22}+7^{91}$, $m=13$;

б) $n=2007^{2008}+2009^{2010}$, $m=17$;

в) $n=\left(2008^{2009}\right)^{2010}+2008^{\left(2009^{2010}\right)}$, $m=11$;

г) $n=\left(\left(39^{40}+41^{42}\right)^{43}+44\right)^{45}$, $m=12$.

**26.** Найдите две последние цифры чисел:

а) $1234^{5678}\cdot 9^{10}$; б) $2009^{2009}$.

**27.** Докажите, что

а) $\left(1^{19}+2^{19}+\ldots+36^{19}\right)\vdots 37$;

б) уравнение $2^x+7^y=19^z$ не имеет решений в натуральных числах;

в) числа вида $4n+3$ не могут являться суммой двух квадратов;

г) если $\dfrac{a-5b}{17}$ – целое число, то $\dfrac{2a+7b}{17}$ также целое число.

## §3. Классы вычетов

Из свойств 1–3 сравнений следует, что отношение сравнимости по некоторому модулю является отношением эквивалентности. Как всякое отношение эквивалентности, оно разбивает основное множество $\mathbb{Z}$ на непересекающиеся классы эквивалентности.

**Определение.** *Классом вычетов* элемента $a$ по модулю $m$ называется множество

$$[a]_m = \{x \in \mathbb{Z} \mid x \equiv a \pmod m\}.$$

**Свойства** (классов вычетов). *1) Классы вычетов по данному модулю образуют разбиение множества $\mathbb{Z}$, в частности, любые два класса либо вообще не имеют общих элементов, либо совпадают.*

*2)* $[a]_m = [b]_m \Leftrightarrow a \equiv b \pmod m$. *В частности, всякий класс вычетов однозначно определяется любым своим элементом.*

*3)* $[a]_m = \{a + mt \mid t \in \mathbb{Z}\}$. *В частности, всякий класс эквивалентности – бесконечное множество.*

*4) Класс вычетов содержит те и только те числа, которые имеют данный остаток при делении данного числа на $m$.*

*5) Количество различных классов вычетов по модулю $m$ равно $m$.*

**Пример.** Найти все классы вычетов по модулю 3.

$$[0]_3 = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod m\} = \{x = 0 + 3t \mid t \in \mathbb{Z}\} =$$

$$= \{0, \pm 3, \pm 6, \pm 9, \ldots\}.$$

Это множество всех целых чисел, которые при делении на 3 имеют остаток 0. По свойству 2 классов вычетов

$$[0]_3 = [3]_3 = [-3]_3 = [6]_3 = [-6]_3 = \ldots.$$

$$[1]_3 = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod m\} = \{x = 1 + 3t \mid t \in \mathbb{Z}\} =$$

$$= \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}.$$

Это множество всех целых чисел, которые при делении на 3 имеют остаток 1. Кроме того

$$[1]_3 = [4]_3 = [-2]_3 = [7]_3 = [-5]_3 = \ldots.$$

$$[2]_3 = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod m\} = \{x = 2 + 3t \mid t \in \mathbb{Z}\} =$$

$$= \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}.$$

*б)* (свойство классов вычетов с кратными модулями). *Элементы любого класса по модулю $m$ образуют ровно $k$ классов вычетов по модулю $mk$. Причём*

$$[c]_m = [c]_{mk} \cup [c + m]_{mk} \cup [c + 2m]_{mk} \cup \ldots \cup [c + (k-1)m]_{mk}. \quad (*)$$

Пусть $\mathbb{Z}_m = \{[a]_m \mid a \in \mathbb{Z}\}$ – множество всех классов вычетов по модулю $m$. Это множество имеет в точности $m$ элементов. Определим операции сложения и умножения на нём согласно следующему правилу:

$$[a]_m + [b]_m = [a + b]_m, \ [a]_m \cdot [b]_m = [ab]_m.$$

Обозначим

$$\bar{1} = [1]_m,\ \bar{0} = [0]_m.$$

**Теорема.** *$\mathbb{Z}_m$ является коммутативным кольцом с единицей. Это кольцо не содержит делителей нуля тогда и только тогда, когда $m$ – простое число.*

**Пример.** Множество всех классов по модулю 7 можно записать так:

$$[0]_7,\ [1]_7,\ [2]_7,\ [3]_7,\ [4]_7,\ [5]_7,\ [6]_7.$$

Все вычисления в $\mathbb{Z}_7$ удобно проводить и записывать в этой системе обозначений. Например,

$$[5]_7 + [4]_7 = [9]_7 = [2]_7,$$

$$[5]_7 \cdot [4]_7 = [20]_7 = [6]_7,$$

$$\frac{[5]_7}{[4]_7} = [5]_7 \cdot \left([4]_7\right)^{-1} = [5]_7 \cdot [2]_7 = [10]_7 = [3]_7.$$

Если модуль $m$ фиксирован, то для краткости можно использовать упрощённые обозначения, а именно, вместо квадратных скобок рисовать черту сверху. Например, $[5]_7 = \bar{5}$ или в общем случае $[k]_m = \bar{k}$.

## Занятие 3

**Теоретический материал.** Классы вычетов, свойства классов вычетов. Свойство классов вычетов с кратными модулями. Кольцо классов вычетов.

**Основные типы задач.** Вычисление элементов классов вычетов, запись классов вычетов в виде объединения классов с кратными модулями, вычисления в кольцах вычетов.

## Задания для практических занятий

**28.** Дайте определение класса вычетов по модулю $m$ и сформулируйте его свойства.

**29.** Проверьте, что:

а) $33 \in [8]_5$;

б) $1963 \in [572]_{13}$;

в) $537^{648} \in [15]_7$;

г) $10 \in \left[296^{35}\right]_{11}$.

**30.** Найдите все классы вычетов по модулю 5 и 7.

**31.** Вычислите все элементы $n$ данного класса вычетов, удовлетворяющие условию $50 \le n \le 150$:

а) $[15]_{17}$;

б) $[-135]_{19}$;

в) $[-134565]_{13}$;

г) $\left[-34^{13} \cdot 56^{43}\right]_{13}$.

**32.** Проверьте, что:

а) $[-39]_5 = [1]_5$;

б) $[2007]_{13} = [-567]_{13}$;

в) $\left[5^{648}\right]_7 = [15]_7$.

**33.** Сформулируйте свойство классов вычетов с кратными модулями.

**34.** Представьте данный класс вычетов как объединение классов вычетов по модулю $m$:

а) $[2]_3$, $m = 12$;

б) $[2]_4$, $m = 12$;

в) $[2]_6$, $m = 12$;

г) $[3]_5$, $m = 15$.

**35.** Дайте определение кольца вычетов $Z_m$.

**36.** Составьте таблицу сложения и умножения $Z_7$.

**37.** Вычислите в $Z_7$:

а) $\overline{2}\cdot\left(\overline{3}+\overline{6}\right)-\overline{3}^2$;

б) $\dfrac{\overline{2}+\overline{3}\cdot\overline{5}}{\overline{4}}$;

в) $\dfrac{\overline{1}}{\overline{2}}+\dfrac{\overline{1}}{\overline{3}}+\dfrac{\overline{1}}{\overline{4}}$;

г) $\left(\dfrac{\overline{2}-\dfrac{\overline{3}}{\overline{4}}}{\overline{5}}\right)\cdot\overline{2}+\left(\overline{3}\right)^{-1}$.

**38.** Решите в $Z_7$ уравнения:

а) $\overline{3}x+\overline{2}=\overline{5}$;

б) $\overline{4}\cdot\left(\overline{3}x-\overline{2}\right)=\overline{5}$;

в) $\dfrac{\overline{1}}{\overline{6}}\cdot\left(\dfrac{\overline{5}}{\overline{3}}x-\dfrac{\overline{1}}{\overline{4}}\right)=\overline{2}$;

г) $\dfrac{\overline{2}x+\overline{3}}{\overline{4}x-\overline{5}}=\dfrac{\overline{5}}{\overline{2}}$.

## Дополнительные задания

**39.** Составьте таблицу сложения и умножения $Z_{11}$.

**40.** Решите в $Z_{11}$ уравнения:

а) $\overline{7}x+\overline{2}=\overline{5}$;

б) $\overline{4}\cdot\left(\overline{3}x-\overline{8}\right)=\overline{5}$;

в) $\dfrac{\overline{1}}{\overline{6}}\cdot\left(\dfrac{\overline{5}}{\overline{9}}x-\dfrac{\overline{7}}{\overline{4}}\right)=\overline{2}$;

г) $x^2=\overline{3}$;

д) $\overline{2}x^2+\overline{3}x+\overline{1}=0$.

**41.** Составьте таблицу умножения для $Z_{10}$. Определите, для каких элементов существует обратный, из каких элементов извлекается квадратный корень?

## §4. Системы вычетов

Любой класс вычетов и результаты арифметических действий над классами однозначно определяются любыми элементами-представителями этих классов. Во многих случаях удобно зафиксировать какую-то конкретную систему представителей всех классов, так называемую полную систему вычетов.

**Определение.** *Полной системой вычетов по модулю* $m$ (сокращённо ПСВ) называется множество чисел, взятых ровно по одному из каждого класса вычетов.

**Пример.** 1) *Полная система наименьших неотрицательных вычетов*:

$$0, 1, 2, 3, \ldots, m-1 .$$

Из каждого класса вычетов взят наименьший неотрицательный элемент. Этот элемент совпадает с остатком от деления элементов класса на $m$ .

2) *Полная система наименьших положительных вычетов*:

$$1, 2, 3, \ldots, m .$$

Из каждого класса взят наименьший положительный элемент. Отличие от предыдущей системы состоит в том, что из класса $[0]_m$ взято число $m$ : $[0]_m = [m]_m$ .

3) *Полная система наименьших по абсолютной величине вычетов.*

Из каждого класса взято наименьшее по абсолютной величине число. Если $m$ – чётно, $m = 2k$ , то это

$$-k+1,\ -k+2,\ \ldots,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ \ldots,\ k .$$

Если $m$ – нечётно, $m = 2k+1$ , то это

$$-k,\ -k+1,\ \ldots,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ \ldots,\ k .$$

**Теорема** (свойства полных систем вычетов). *1) Любые $m$ попарно несравнимых друг с другом по модулю $m$ чисел образуют ПСВ по модулю $m$.*

*2) Любые $m$ подряд идущих целых чисел образуют ПСВ по модулю $m$.*

*3) Если $x_1, x_2, \ldots, x_m$ – ПСВ по модулю $m$, $a, b$ – целые числа, причём $a \neq 0$ и взаимно просто с $m$, то числа*

$$ax_1 + b,\ ax_2 + b,\ ax_3 + b,\ \ldots,\ ax_m + b$$

*образуют ПСВ по модулю $m$.*

## Занятие 4

**Теоретический материал.** Полные системы вычетов (ПСВ), их свойства.

**Основные типы задач.** Составление ПСВ с заданными свойствами.

### Задания для практических занятий

**42.** Найдите а) наименьшие неотрицательные вычеты, б) наименьшие положительные вычеты, в) наименьшие по абсолютной величине вычеты чисел $-27, -5, 12,\ 125,\ 1253, -3789$ по модулям $m = 7$; $m = 12$; $m = 17$; $m = 25$.

**43.** Дайте определение полной системы вычетов по модулю $m$. Сформулируйте свойства ПСВ. Укажите различные способы нахождения ПСВ.

**44.** Проверьте, образуют ли ПСВ по модулю $m$ следующие наборы чисел:

а) 235, 341, 638, 37, 76, 94, 291; $m = 7$;

б) 167, 274,385, 486, 572, 627, 741; $m = 8$;

в) 47, 58, 61, 72, 81, 98; $m = 6$;

г) 761, 620, –574, 774, 633, 244, 166, –173, 231; $m = 9$.

**45.** Составьте ПСВ по модулю m, содержащую числа:

а) 234567, 9374562; $m = 7$;

б) $23^{4567}$, $937^{4562}$; $m = 7$;

в) $23 \cdot 4^{567}$, $93 \cdot 74^{562}$; $m = 9$.

**46.** Составьте:

а) ПСВ по модулю 10, содержащую только числа вида $3k + 1$;

б) ПСВ по модулю 8, содержащую только числа вида $5k + 3$.

### Дополнительные задания

**47.** Докажите, что ПСВ по модулю 7 не может состоять из квадратов целых чисел.

**48.** В двух группах студентов числится 55 человек. Докажите, что хотя бы двое из них празднуют свой день рождения в одну неделю.

## §5. Функция Эйлера и её свойства

**Определение.** Количество натуральных чисел, взаимно простых с $m$ и не превосходящих $m$ обозначается $\varphi(m)$. Функция $\varphi : \mathbb{N} \to \mathbb{N}$ называется *функцией Эйлера.*

**Пример.** 1) Пусть $m = 10$. Величину $\varphi(10)$ можно вычислить по определению. Для этого выпишем все натуральные числа, меньшие 10, и вычеркнем те из них, которые имеют с числом 10 нетривиальные общие делители:

$$1,\ \cancel{2},\ 3,\ \cancel{4},\ \cancel{5},\ \cancel{6},\ 7,\ \cancel{8},\ 9\,.$$

Остались не зачёркнутыми четыре числа, поэтому $\varphi(10)=4$.

2) Пусть $p$ – простое число, тогда в последовательности $1, 2, 3, \ldots, p-1$ все числа взаимно просты с $p$, поэтому $\varphi(p)=p-1$.

**Замечание.** 1) Согласно свойству 12 сравнимостей, если $a \equiv b \pmod m$, то $\text{НОД}(a,m)=\text{НОД}(b,m)$. Если $\text{НОД}(a,m)=1$, то это выполняется для всех чисел из класса $[a]_m$. Классы с таким свойством называются *взаимно простыми с модулем* $m$. Их количество равно $\varphi(m)$.

2) Всякая ПСВ по модулю $m$ содержит $\varphi(m)$ чисел, взаимно простых с $m$.

**Определение.** *Приведённой системой вычетов по модулю* $m$ называется множество чисел, взятых ровно по одному из каждого класса вычетов, взаимно простого с модулем $m$.

**Теорема** (свойства приведённых систем вычетов). 1*) Любые* $\varphi(m)$ *попарно несравнимых по модулю* $m$ *и взаимно простых с модулем чисел образуют приведённую систему вычетов по модулю* $m$.

*2) Если* $x_1, x_2, \ldots, x_{\varphi(m)}$ *– некоторая приведённая система вычетов по модулю* $m$, *а число* $a$ *взаимно просто с* $m$, *то* $ax_1$, $ax_2$, …, $ax_{\varphi(m)}$ *– также приведённая система вычетов по модулю* $m$.

Приведённые системы вычетов используются для того, чтобы представлять классы вычетов, взаимно простые с модулем.

**Теорема** (Эйлер). *Если числа $a, m$ – взаимно просты, то*

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

**Следствие 1** (малая теорема Ферма). *Если $p$ – простое число и $a \not\vdots p$, то*

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

**Следствие 2.** *Если $p$ – простое число, то*

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

**Теорема** (о мультипликативности функции Эйлера). *Если числа $a, b$ взаимно просты, то $\varphi(ab) = \varphi(a) \cdot \varphi(b)$.*

**Следствие** (формулы для вычисления $\varphi$).

*1) Если $p$ – простое число, то $\varphi\left(p^n\right) = p^n - p^{n-1}$.*

*2) Если $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ – каноническое разложение числа $m$, то*

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

**Замечание.** В последней формуле не участвуют показатели степеней $\alpha_i$. Для того, чтобы применить формулу, достаточно знать исходное число $m$ и простые числа, которые входят в его каноническое разложение.

**Пример.** Вычислим $\varphi(7000)$. Очевидно, в каноническое разложение числа 7000 входят только числа 2, 5 и 7, поэтому

$$\varphi(7000) = 7000 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right) = 7000 \cdot \frac{1}{2} \cdot \frac{4}{5} \cdot \frac{6}{7} = 2400.$$

Теорема Эйлера-Ферма может быть использована для нахождения обратных элементов в кольце $\mathbb{Z}_m$.

**Теорема.** *Кольцо $\mathbb{Z}_m$ является полем тогда и только тогда, когда $m$ – простое число.*

Если $m$ – простое число, то обратный элемент для $\overline{a} \neq \overline{0}$ вычисляется по формуле:

$$\left(\overline{a}\right)^{-1} = \overline{a}^{m-2}.$$

## Занятие 5

**Теоретический материал.** Функция Эйлера. Формулы для вычисления функции Эйлера. Приведённые системы вычетов, их свойства. Теорема Эйлера-Ферма.

**Основные типы задач.** Вычисление значения функции Эйлера, составление приведённых систем вычетов с данными свойствами.

### Задания для практических занятий

**49.** Дайте определение функции Эйлера.

**50.** Вычислите по определению $\varphi(13), \varphi(14), \varphi(15)$.

**51.** Приведите формулы для вычисления функции Эйлера. Вычислите:

а) $\varphi(27)$; б) $\varphi(1000)$;

в) $\varphi\left(2^2 \cdot 3^3 \cdot 5\right)$; г) $\varphi\left(3^2 \cdot 4^2 \cdot 5 \cdot 6\right)$.

**52.** Решите уравнение:

а) $\varphi\left(5^x\right) = 2500$; б) $\varphi\left(7^x\right) = 2058$.

**53.** Найдите количество натуральных чисел, которые:

а) не превосходят 120 и взаимно просты с 30;

б) не превосходят 1665 и имеют с 1665 наибольший общий делитель, равный 9.

**54.**Дайте определение приведённой системы вычетов. Сформулируйте свойства ПривСВ.

**55.** Составьте приведённую систему вычетов:

а) по модулю 9;

б) по модулю 14;

в) по модулю 7, состоящую из степеней числа 3;

г) по модулю 10, содержащую числа $3^{333}$ и $7^{777}$.

**56.** Сформулируйте теорему Эйлера. С помощью теоремы Эйлера найдите остаток от деления:

а) $7^{512}$ на 9; б) $9^{356}$ на 14;

в) $5^{3247}+3^{524}$ на 7; г) $\left(57^{311}+31^{503}\right)^{11}$ на 13.

## Дополнительные задания

**57.** Найдите натуральное число $n$, если известно, что $n=3^x\cdot 5^y\cdot 7^z$ и $\varphi(n)=3600$.

**58.** Найдите количество натуральных чисел, которые:

а) не превосходят 150 и не являются взаимно простыми с 50;

б) не превосходят 1665 и имеют с ним наибольший общий делитель, равный 37;

в) находятся в промежутке от 1000 до 1500 и имеют с числом 160 наибольший общий делитель, равный 20;

г) меньше 300 и имеют с ним наибольший общий делитель, равный 20.

**59.** С помощью теоремы Эйлера-Ферма докажите, что:

а) $\left(1^{16}+3^{16}+7^{16}+9^{16}-4\right)$ делится на 10;

б) $\left(1^{14}+5^{14}+7^{14}+11^{14}-4\right)$ делится на 12;

в) $\left(1^{13}+2^{13}+4^{13}+5^{13}+7^{13}+8^{13}\right)$ делится на 9;

г) $\left(1^{17}+3^{17}+5^{17}+9^{17}+11^{17}+13^{17}\right)$ делится на 14.

**60.** Докажите, что

а) если числа $a$ и 7 взаимно просты, то $\left(a^{12}-1\right)\vdots 7$;

б) если числа $a$ и $b$ взаимно просты с числом 65, то $\left(a^{12}-b^{12}\right)$ делится на 65;

**61.** Докажите, что для любого целого числа $n$:

а) $n^{361}-n$ делится на 11;

б) $n^{2001}-n$ делится на 11;

в) $n^{7}-n$ делится на 42;

г) $n^{13}-n$ делится на 2730.

## Контрольная работа №1

*Примерный вариант*

1. Найдите остаток от деления числа $n=37^{451}+21^{374}$ на $m=17$.

2. Решите в $Z_{11}$ уравнение $\frac{\bar{1}}{\bar{7}} \cdot \left( \frac{\bar{9}}{\bar{4}} x - \frac{\bar{2}}{\bar{5}} \right) = \bar{3}$.

3. Составьте приведённую систему вычетов по модулю 22, содержащую числа $37^{38}$ и $71^{72}$.

# *ТЕМА 2.* СРАВНЕНИЯ И ДИОФАНТОВЫ УРАВНЕНИЯ

## §1. Алгебраические сравнения

**Определение.** *Алгебраическим сравнением* степени $n$ по модулю $m$ называется сравнение вида

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 \pmod{m}, \qquad (1)$$

где $a_n \not\equiv 0 \pmod{m}$, $a_i \in \mathbb{Z}$ – *коэффициенты*, $x$ – *неизвестное*. Задача состоит в нахождении всех целых значений $x$, удовлетворяющих сравнению (1).

**Замечание.** *Если $x$ – удовлетворяет сравнению (1) и $x \equiv y \pmod{m}$, то $y$ также удовлетворяет сравнению (1).*

Ввиду этого, классы вычетов попадают в решения сравнения (1) целиком, поэтому кроме чисел решениями сравнения (1) можно считать и классы.

**Определение.** Класс вычетов по модулю $m$ называется *решением сравнения* (1), если все его элементы удовлетворяют (1). *Числом решений* сравнения (1) называют число классов вычетов по модулю $m$, удовлетворяющих (1).

**Пример.** Решить сравнение $13x^3 + 15x - 8 \equiv 0 \pmod{6}$.

Так как $13 \equiv 1 \pmod{6}$, $15 \equiv 3 \pmod{6}$ и $-8 \equiv -2 \pmod{6}$, то для любого $x$

$$13x^3 + 15x - 8 \equiv x^3 + 3x - 2 \pmod{6}$$

и достаточно решить сравнение с меньшими коэффициентами $x^3 + 3x - 2 \equiv 0 \pmod{6}$.

Так как классы вычетов являются решениями целиком и их конечное число (6 штук), то можно решать *методом*

*перебора.* Чтобы перебрать все классы, выбираем ПСВ по модулю 6. В куб выгоднее возводить наименьшие по абсолютной величине числа:

$$-2, -1, 0, 1, 2, 3 .$$

Получаем следующее.

$$(-2)^3 + 3(-2) - 2 = -16 \equiv 2 \not\equiv 0 \pmod 6,$$

$$(-1)^3 + 3(-1) - 2 = -6 \equiv 0 \pmod 6,$$

$$0^3 + 3(0) - 2 = -2 \equiv 4 \not\equiv 0 \pmod 6,$$

$$1^3 + 3 \cdot 1 - 2 = 2 \not\equiv 0 \pmod 6,$$

$$2^3 + 3 \cdot 2 - 2 = 12 \equiv 0 \pmod 6,$$

$$3^3 + 3 \cdot 3 - 2 = 34 \equiv 4 \not\equiv 0 \pmod 6.$$

В результате решениями исходного сравнения будут классы

$$[-1]_6, \ [2]_6 .$$

**Пример.** Решить сравнение $x^8 + x - 1 \equiv 0 \pmod 7$.

Согласно следствию 2 из теоремы Эйлера

$$x^7 \equiv x \pmod 7 .$$

Поэтому исходное сравнение равносильно сравнению

$$x^2 + x - 1 \equiv 0 \pmod 7 ,$$

которое имеет меньшую степень и, следовательно, легче решается. Перебирая полную систему наименьших по абсолютной величине вычетов по модулю 7:

$$-3, -2, -1, 0, 1, 2, 3,$$

убеждаемся, что сравнение решений не имеет.

Если модуль – большое число, то метод перебора является громоздким. Однако, если модуль – составное число, то данное сравнение можно свести к системе сравнений по меньшим модулям согласно следующей

**Теореме.** *Пусть дано каноническое разложение модуля* $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$. *Алгебраическое сравнение вида* $f(x) \equiv 0 (\mathrm{mod}\, m)$ *равносильно системе алгебраических сравнений*

$$\begin{cases} f(x) \equiv 0 \left(\mathrm{mod}\, p_1^{\alpha_1}\right), \\ f(x) \equiv 0 \left(\mathrm{mod}\, p_2^{\alpha_2}\right), \\ \qquad \ldots \\ f(x) \equiv 0 \left(\mathrm{mod}\, p_k^{\alpha_k}\right). \end{cases} \qquad (2)$$

Систему (2) можно решать в следующей последовательности. Сначала решаем каждое сравнение системы. Если хотя бы одно сравнение решений не имеет, то не имеет решений и вся система. Если каждое сравнение системы (2) имеет решения, то система (2) сводится к решению систем сравнений первой степени вида

$$\begin{cases} x \equiv a_1 \left(\mathrm{mod}\, p_1^{\alpha_1}\right), \\ x \equiv a_2 \left(\mathrm{mod}\, p_2^{\alpha_2}\right), \\ \qquad \ldots \\ x \equiv a_k \left(\mathrm{mod}\, p_k^{\alpha_k}\right), \end{cases}$$

где $a_i$ – одно из решений $i$-того сравнения системы. Рассмотрев все варианты таких систем, мы получим все решения системы (2), а, следовательно, и сравнения (1).

Можно доказать, что *сравнение вида* $f(x) \equiv 0 \left(\mathrm{mod}\ p^{\alpha}\right)$ *по модулю степени простого числа сводится к решению нескольких сравнений по модулю* $p$.

Ввиду этого, случай, когда $m = p$ – простое число, является основным.

**Теорема** (о количестве решений). *Сравнение вида*

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 (\mathrm{mod}\ p), \qquad (*)$$

*где* $p$ *– простое число,* $a_n \not\equiv 0 (\mathrm{mod}\ p)$, *имеет не более* $n$ *решений.*

**Частный случай.** *Сравнение* $x^{p-1} - 1 \equiv 0 (\mathrm{mod}\ p)$ *имеет ровно* $(p-1)$ *решений.*

**Следствие 2.** *Если* $\varphi(p) = (p-1) \vdots d$, *то сравнение* $x^d - 1 \equiv 0 (\mathrm{mod}\ p)$ *имеет ровно* $d$ *решений.*

## Занятие 6

**Теоретический материал.** Алгебраические сравнения. Метод перебора. Сведение произвольного сравнения к сравнению с коэффициентами, меньшими числа $m$ по абсолютной величине, и степенью, меньшей $\varphi(m)$. Теорема о количестве решений сравнения по простому модулю и её следствия.

**Основные типы задач.** Сведение данного сравнения к сравнениям с меньшими коэффициентами и по меньшему модулю, решение сравнений методом перебора.

## Задания для практических занятий

**62.** Дайте определение алгебраического сравнения. Сформулируйте простейшие свойства его решений, дайте понятие количества решений.

**63.** Сформулируйте простейшие приёмы уменьшения коэффициентов и степени сравнения. Найдите равносильное сравнение с меньшей степенью и меньшими коэффициентами:

а) $41x^3 + 64x^2 - 23x + 78 \equiv 0 \pmod 5$;

б) $x^{13} + 4x^{12} - 2x^{11} - 3x^9 + x^3 - 2x + 3 \equiv 0 \pmod 5$;

в) $x^{13} + 44x^{10} - 25x^9 - 36x^7 + 7x^2 - 82x + 93 \equiv 0 \pmod 7$;

г) $71x^{12} + 42x^{10} - 46x^5 + 6x^4 - 57x^2 - 86x + 7 \equiv 0 \pmod 8$.

**64.** Сформулируйте теорему о количестве решений сравнения по простому модулю.

**65.** Решите методом подбора:

а) $x^2 - 3x + 2 \equiv 0 \pmod 4$;

б) $x^2 - 2x + 2 \equiv 0 \pmod 5$;

в) $x^5 - 3x^2 + 15x - 1 \equiv 0 \pmod 4$;

г) $8x^3 + x - 2 \equiv 0 \pmod 7$.

## Дополнительные задания

**66.** Решите сравнения:

а) $20x^{80} + 15x^{30} + 5x^2 \equiv 1 \pmod{35}$;

б) $6x^3 + 27x^2 + 17x + 20 \equiv 0 \pmod{30}$;

в) $4x^{32} + 5x^{21} + 6x^{11} + 7x^2 \equiv 0 \pmod{22}$;

г) $2x^5 + x^4 - 2x - 1 \equiv 0 \pmod{5}$.

## §2. Сравнения первой степени

Рассмотрим *сравнения первой степени*, которые обычно записываются в виде:

$$ax \equiv b \pmod{m}, \quad a \not\equiv 0 \pmod{m}. \qquad (1)$$

**Теорема** (условие существования решений сравнения первой степени). *Сравнение (1) имеет решения тогда и только тогда, когда*

$$b \vdots НОД(a, m).$$

**Пример.** Сравнение $78x \equiv 3 \pmod{46}$ решений не имеет, т.к.

$$\text{НОД}(78, 46) = 2 \text{ и } 3 \not\vdots 2.$$

**Замечание.** Согласно свойству 7 сравнений:

$$acx \equiv bc \pmod{mc} \Leftrightarrow ax \equiv b \pmod{m}.$$

Поэтому, сравнение можно сокращать до тех пор, пока числа $a$ и $m$ не станут взаимно простыми. Полученное сокращённое сравнение равносильно исходному сравнению.

**Теорема** (сокращённый случай). *Если числа $a$ и $m$ взаимно просты, то сравнение (2) имеет единственное решение, которое можно записать так:* $\left[ b \cdot a^{\varphi(m)-1} \right]_m$.

**Теорема** (общий случай). *Пусть $d = НОД(a, m)$ и $b \vdots d$. Решениями сравнения $ax \equiv b \pmod{m}$ будут $d$ классов*

*вычетов по модулю $m$, которые образуют один класс вычетов по модулю $\frac{m}{d}$.*

**Пример.** 1) Решить сравнение $3x \equiv 2 (\mathrm{mod}\, 7)$.

Находим решение по формуле:

$$\varphi(7) = 6, \quad x \equiv 2 \cdot 3^{6-1} = 2 \cdot 27 \cdot 9 \equiv 2 \cdot 6 \cdot 2 = 24 \equiv 3 (\mathrm{mod}\, 7).$$

Другим способом решения можно записать так:

$$x = 3 + 7t, \ t \in \mathbb{Z}.$$

2) Решить сравнение $24x \equiv 14 (\mathrm{mod}\, 9)$.

Так как $\text{НОД}(24, 9) = 3$ и $14 \not\vdots 3$, то решений нет.

3) Решить сравнение $9x \equiv 6 (\mathrm{mod}\, 21)$.

Так как $\text{НОД}(9, 21) = 3$ и $6 \vdots 3$, то решения есть. Сокращаем сравнение на $\text{НОД}(9, 21)$:

$$9x \equiv 6 (\mathrm{mod}\, 21) \ \Leftrightarrow \ 3x \equiv 2 (\mathrm{mod}\, 7).$$

Решением будет один класс по модулю 7 (см. пример выше), или три класса по модулю 21:

$$[3]_7 = [3]_{21} \cup [3+7]_{21} \cup [3+14]_{21} = [3]_{21} \cup [10]_{21} \cup [17]_{21}.$$

Сравнения первой степени можно также решать при помощи равносильных преобразований.

**Пример.** Решить сравнение $3x \equiv 1 (\mathrm{mod}\, 7)$.

Очевидно, что если сократить коэффициент при $x$, то решение будет найдено. Этого можно добиться при помощи свойств 6 и 8 сравнений. Будем добавлять к коэффициенту 1 числа кратные 7 (свойство 6) до тех пор, пока не получится число кратное 3, затем сократим на 3 (свойство 8).

$$3x \equiv 1 \pmod 7 \overset{6)}{\Leftrightarrow} 3x \equiv 1+7 \pmod 7,\ 8 \not\vdots 3;$$

$$3x \equiv 8 \pmod 7 \overset{6)}{\Leftrightarrow} 3x \equiv 8+7 \pmod 7,\ 15 \vdots 3;$$

$$3x \equiv 15 \pmod 7 \overset{8)}{\Leftrightarrow} x \equiv 5 \pmod 7.$$

Решениями исходного сравнения будут все элементы класса $[5]_7$.

## Занятие 7

**Теоретический материал.** Сравнения первой степени. Условие существования решения. Решение сравнений первой степени в общем случае. Методы решения сравнений первой степени.

**Основные типы задач.** Решение сравнений первой степени разными способами.

### Задания для практических занятий

**67.** Дайте определение сравнения первой степени. Сформулируйте условие существования решения и метод решения в случае взаимной простоты старшего коэффициента и модуля.

**68.** Решите сравнения:

а) $3x \equiv 1 \pmod 7$; б) $5x \equiv 3 \pmod{11}$;

в) $8x \equiv 3 \pmod{12}$; г) $11x \equiv 9 \pmod{21}$;

д) $8x \equiv 5 \pmod{15}$.

**69.** Сформулируйте свойство сокращения сравнений и свойство классов вычетов с кратными модулями.

**70.** Решите сравнения, предварительно их сократив. Запишите ответ в виде классов вычетов по исходному модулю.

а) $12x \equiv 9 \pmod{21}$; б) $20x \equiv 16 \pmod{28}$;

в) $14x \equiv 6 \pmod{10}$; г) $20x \equiv 30 \pmod{35}$.

**71.** Сформулируйте свойства сравнений (сокращение, добавление к одной части числа, кратного модулю), которые позволяют решать сравнения при помощи преобразований.

**72.** Решите сравнения при помощи преобразований.

а) $12x \equiv 9 \pmod{17}$; б) $12x \equiv 6 \pmod{21}$;

в) $32x \equiv 24 \pmod{44}$; г) $40x \equiv 15 \pmod{12}$.

ДОПОЛНИТЕЛЬНЫЕ ЗАДАНИЯ

**73.** Решите методом подбора сравнения из задания 72.

## §3. Системы сравнений первой степени

Система произвольных алгебраических сравнений либо не имеет решений, либо сводится к системам, состоящим из сравнений вида $x \equiv b \pmod{m}$. Для начала разберём частный случай такой системы:

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}. \end{cases} \qquad (1)$$

Пусть $d = \text{НОД}(m_1, m_2)$, $M = \text{НОК}(m_1, m_2)$. Из первого сравнения системы получаем $x - b_1 = m_1 t \Rightarrow x = b_1 + m_1 t$. Подставляем это выражение во второе сравнение и получаем

$$b_1 + m_1 t \equiv b_2 \pmod{m_2} \Rightarrow m_1 t \equiv b_2 - b_1 \pmod{m_2}.$$

Последнее сравнение имеет решения тогда и только тогда, когда $(b_2 - b_1) \vdots d$. Решением будет некоторый класс по модулю $\frac{m_2}{d}$:

$$[c]_{\frac{m_2}{d}}.$$

По-другому эти решения можно записать так: $t = c + \frac{m_2}{d}u$. Если подставить эти значения $t$ в решение первого сравнения, то мы получим все решения первого сравнения, которые удовлетворяют второму сравнению, т.е. решения системы:

$$x = b_1 + m_1 t = x = b_1 + m_1\left(c + \frac{m_2}{d}u\right) = b_1 + m_1 c + \frac{m_1 m_2}{d}u.$$

Согласно известному свойству, связывающему НОД и НОК, $\frac{m_1 m_2}{d} = M$, поэтому

$$x = b_1 + m_1 c + Mu.$$

В результате получилась

**Теорема.** *Если* $(b_2 - b_1) \not\vdots d$, *то система (1) не имеет решений. Если* $(b_2 - b_1) \vdots d$, *то система (1) имеет одно решение, которое является классом вычетов по модулю* $M$. *Кроме того, система равносильна одному сравнению по модулю* $M$:

$$x \equiv b_1 + m_1 c \pmod{M}.$$

На последнем утверждении этой теоремы и основан метод решения таких систем с большим количеством сравнений:

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \qquad \cdots \\ x \equiv b_k \pmod{m_k}. \end{cases} \qquad (2)$$

Решаем первые два сравнения и сводим их к одному, затем к полученному сравнению добавляем третье и опять сводим их к одному сравнению, затем добавляем четвёртое, пятое и т.д. сравнения, пока не получим решение всей системы. Возможны два случая: *либо система (2) не имеет решений, либо имеет одно решение, которое будет классом вычетов по наименьшему общему кратному модулей всех сравнений.*

**Пример.** Решить систему

$$\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 1 \pmod 4, \\ x \equiv -1 \pmod 6. \end{cases}$$

Подставив $x = 2 + 3t$ во второе сравнение, находим $t$ :

$$2 + 3t \equiv 1 \pmod 4 \;\Leftrightarrow\; 3t \equiv -1 \pmod 4 \;\Rightarrow\; t = 1 + 4u$$

Решение можно найти методом подбора. В результате

$$x = 2 + 3(1 + 4u) = 5 + 12u \;\Leftrightarrow\; x \equiv 5 \pmod{12}.$$

Исходная система трёх сравнений свелась к системе двух сравнений

$$\begin{cases} x \equiv 5 \pmod{12}, \\ x \equiv -1 \pmod 6. \end{cases}$$

Далее действуем аналогично.

$$x = 5 + 12u \equiv -1 \pmod 6 \;\Leftrightarrow\; 12u \equiv -6 \pmod 6 \;\Leftrightarrow\; 2u \equiv -1 \pmod 1.$$

Последнему сравнению удовлетворяет любое $u$. Подставляем его обратно в $x$ и получаем

$$x = 5 + 12u,\ u \in \mathbb{Z}.$$

Решением исходной системы оказался класс $[5]_{12}$.

Основным является случай, когда модули сравнений системы попарно взаимно просты.

**Теорема.** *Если числа $m_1, m_2, \ldots, m_k$ попарно взаимно просты, то система (2) имеет решение, которое будет классом вычетов по модулю $M = m_1 \cdot m_2 \cdot \ldots \cdot m_k$.*

Для решения систем вида (2) можно воспользоваться

**Теоремой** (Китайская теорема об остатках). *Пусть числа $m_1, m_2, \ldots, m_k$ – попарно взаимно просты, $M = m_1 \cdot m_2 \cdot \ldots \cdot m_k$ и числа $y_1, y_2, \ldots, y_k$ подобраны так, что*

$$\frac{M}{m_1} y_1 \equiv 1 (\mathrm{mod}\, m_1),\ \frac{M}{m_2} y_2 \equiv 1 (\mathrm{mod}\, m_2),\ \ldots,\ \frac{M}{m_k} y_k \equiv 1 (\mathrm{mod}\, m_k).$$

*Система (2) имеет единственное решение $x \equiv x_0 (\mathrm{mod}\, M)$, где*

$$x_0 = \frac{M}{m_1} y_1 b_1 + \frac{M}{m_2} y_2 b_2 + \ldots + \frac{M}{m_k} y_k b_k.$$

**Пример.** Найти все числа, которые при делении на 3,4,5 дают соответственно остатки 2, 1, 2.

Для того, чтобы найти все такие целые числа достаточно решить систему

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

Числа 3, 4, 5 попарно взаимно просты. Воспользуемся китайской теоремой об остатках. Имеем

$$M = 3 \cdot 4 \cdot 5 = 60,\ \frac{M}{3} = 20,\ \frac{M}{4} = 15,\ \frac{M}{5} = 12.$$

Составляем вспомогательные сравнения и находим их решения (подбором).

$$20y \equiv 1 (\mathrm{mod}\, 3) \ \Rightarrow\ y_1 = 2;$$

$$15y \equiv 1 (\mathrm{mod}\, 4) \ \Rightarrow\ y_2 = 3;$$

$$12y \equiv 1 (\mathrm{mod}\, 5) \ \Rightarrow\ y_3 = 3;$$

$$x_0 = 20 \cdot 2 \cdot 2 + 15 \cdot 3 \cdot 1 + 12 \cdot 3 \cdot 2 = 197.$$

Решениями исходной системы будут числа $x \equiv 197 \equiv 17 (\mathrm{mod}\, 60)$.

## Занятие 8

**Теоретический материал.** Системы сравнений первой степени, условие существования решений. Китайская теорема об остатках.

**Основные типы задач.** Решение систем сравнений первой степени разными способами.

### Задания для практических занятий

**74.** Сформулируйте алгоритм решения систем сравнений первой степени.

**75.** Решите системы:

а) $\begin{cases} x \equiv 2 (\mathrm{mod}\, 5), \\ x \equiv 8 (\mathrm{mod}\, 11); \end{cases}$ б) $\begin{cases} x \equiv 7 (\mathrm{mod}\, 33), \\ x \equiv 3 (\mathrm{mod}\, 63); \end{cases}$

в) $\begin{cases} 4x \equiv 3 (\mathrm{mod}\, 7), \\ 5x \equiv 4 (\mathrm{mod}\, 6); \end{cases}$ г) $\begin{cases} 3x \equiv 4 (\mathrm{mod}\, 8), \\ 5x \equiv 3 (\mathrm{mod}\, 6); \end{cases}$

д) $\begin{cases} 17x \equiv 7 \pmod 2, \\ 2x \equiv 1 \pmod 3, \\ 2x \equiv 2 \pmod 5. \end{cases}$

**76.** Найдите все числа, которые:

а) при делении на 2, 5 и 7 дают соответственно остатки 1, 2 и 3;

б) при делении на 7, 5, 3 и 11 дают соответственно остатки 3, 2, 1 и 9;

в) кратны 7 и при делении на 2, 3, 4, 5 и 6 дают остаток 1.

**77.** Сформулируйте китайскую теорему об остатках. При каком условии она применима к системе?

**78.** Решите при помощи китайской теоремы об остатках следующие системы:

а) $\begin{cases} x \equiv 3 \pmod 4, \\ x \equiv 1 \pmod 3, \\ x \equiv 2 \pmod 5; \end{cases}$ б) $\begin{cases} 3x \equiv 5 \pmod 7, \\ 2x \equiv 3 \pmod 5, \\ 3x \equiv 2 \pmod 8. \end{cases}$

## Дополнительные задания

**79.** При каких значениях параметра a совместны системы:

а) $\begin{cases} x \equiv 5 \pmod{18}, \\ x \equiv 8 \pmod{21}, \\ x \equiv a \pmod{35}; \end{cases}$ б) $\begin{cases} x \equiv 3 \pmod{11}, \\ x \equiv 1 \pmod{20}, \\ x \equiv 1 \pmod{15}, \\ x \equiv a \pmod{18}? \end{cases}$

**80.** Найдите все натуральные числа, которые:

а) при делении на 2, 3, 4, 5 и 7 дают соответственно остатки 1, 2, 3, 4 и 0;

б) находятся в промежутке от 200 до 500 включительно и при делении на 4, 5 и 7 дают остатки 3, 4 и 5 соответственно.

## §4. Диофантовы уравнения

*Диофантовыми уравнениями первой степени с двумя неизвестными* или просто *диофантовыми уравнениями* называются уравнения вида

$$ax + by = c,$$

где $a, b, c$ – целые числа, $a, b \neq 0$, а $x, y$ – целочисленные неизвестные.

Один из способов решения диофантовых уравнений основан на сведении диофантова уравнения к сравнению первой степени.

**Теорема** (о сведении диофантовых уравнений к сравнениям). *Пусть* $b > 0$. *1) Если* $(x_0, y_0)$ – *некоторое решение уравнения* $ax + by = c$, *то* $x_0$ – *решение сравнения* $ax \equiv c \pmod{b}$.

*2) Если* $x_0$ – *решение сравнения* $ax \equiv c \pmod{b}$, *то существует такое* $y_0$, *что пара* $(x_0, y_0)$ *будет решением уравнения* $ax + by = c$.

**Пример.** Решить уравнение $5x + 4y = 3$.

Воспользовавшись предыдущей теоремой, получаем сравнение $5x \equiv 3 \pmod{4}$. Так как $\text{НОД}(5, 4) = 1$, то решением будет один класс по модулю 4:

$$\left[5^{\varphi(4)-1} \cdot 3\right]_4 = \left[5^1 \cdot 3\right]_4 = [3]_4.$$

Решения сравнения имеют вид $x = 3 + 4t,\ t \in \mathbb{Z}$. Соответствующее значение $y$ находим из исходного уравнения.

$$5x + 4y = 3 \ \Rightarrow\ 5(3 + 4t) + 4y = 3 \ \Rightarrow$$

$$\Rightarrow\ 15 + 20t + 4y = 3 \ \Rightarrow\ y = -3 - 5t\,.$$

**Ответ:** $x = 3 + 4t,\ y = -3 - 5t,\ t \in \mathbb{Z}$. Решений бесконечно много.

Условие существования решений диофантова уравнения и их вид даёт следующая

**Теорема** (о решениях диофантовых уравнений).

*1) Уравнение $ax + by = c$ имеет решения тогда и только тогда, когда $c \vdots НОД(a, b)$.*

*2) Если $k = НОД(a, b)$, $c \vdots k$ и $(x_0, y_0)$ – некоторое решение уравнения, то решений бесконечно много и их можно найти по формуле*

$$x = x_0 + \frac{b}{k}t,\ y = y_0 - \frac{a}{k}t,\ t \in \mathbb{Z}\,.$$

Данная теорема служит основой для нескольких способов решения диофантовых уравнений.

**Способ, основанный на применении тождества Безу.**

*Составляем тождество Безу для чисел $a$ и $b$ (например, используя алгоритм Евклида), из тождества находим частное решение $(x_0, y_0)$, затем применяем формулу.*

**Пример.** Решить уравнение $8x - 14y = 6$.

Так как $НОД(8, 14) = 2,\ 6 \vdots 2$, то решения есть. Записываем алгоритм Евклида для чисел 8 и 14. Всё кроме

частных в этом алгоритме обозначаем буквами и выражаем остатки.

$$\begin{aligned} &14 = 8\cdot 1 + 6, && b = a\cdot 1 + r_1; && r_1 = b - a,\\ &8 = 6\cdot 1 + 2, && a = r_1\cdot 1 + k; && k = a - r_1.\\ &6 = 2\cdot 3; \end{aligned}$$

Здесь $a = 8,\ b = 14,\ k = \text{НОД}(a, b) = 2$.

Начиная с верхнего равенства, выражаем остатки через $a$ и $b$.

$$r_1 = b - a,\quad k = a - r_1 = a - (b - a) = 2a - b.$$

Возвращаемся обратно к числам и подгоняем полученное равенство к виду $8x - 14y = 6$, чтобы получить решение.

$$8\cdot 2 - 14\cdot 1 = 2 \ \Rightarrow \text{(умножаем на 3)} \Rightarrow\ 8\cdot 6 - 14\cdot 3 = 6 \ \Rightarrow$$

$$\Rightarrow\ x_0 = 6,\ y_0 = 3.$$

Затем применяем формулу, не забыв сократить коэффициенты на $k = 2$.

$$x = x_0 + \frac{b}{k}t = 6 + \frac{-14}{2}t = 6 - 7t,$$

$$y = y_0 - \frac{a}{k}t = 3 - \frac{8}{2}t = 3 - 4t,\ t \in \mathbb{Z}.$$

**Ответ:** $x = 6 - 7t,\ y = 3 - 4t,\ t \in \mathbb{Z}$.

**Метод подбора.**

*Первая компонента $x$ является арифметической прогрессией с разностью $\frac{b}{k}$. Если взять $\frac{b}{k}$ подряд идущих чисел, то ровно одно из них входит в решение. Его можно определить, вычисляя соответствующее ему значение $y$. В*

*результате будет найдено некоторое решение* $(x_0, y_0)$, *а затем можно применить формулу.*

*Подбор решения можно начать и с неизвестного* $y$.

**Пример.** Решить уравнение $8x - 14y = 6$.

Сократим уравнение на 2:

$$4x - 7y = 3.$$

Согласно формуле $x = x_0 - 7t,\ y = y_0 - 4t,\ t \in \mathbb{Z}$.

Рассматриваем семь подряд идущих чисел и находим одно из решений данного уравнения.

$x = 0,\quad y = \dfrac{4x-3}{7} = -\dfrac{3}{7} \notin \mathbb{Z}$;

$x = 1,\quad y = \dfrac{1}{7} \notin \mathbb{Z}$;

$x = 2,\quad y = \dfrac{5}{7} \notin \mathbb{Z}$;

$x = 3,\quad y = \dfrac{9}{7} \notin \mathbb{Z}$;

$x = 4,\quad y = \dfrac{13}{7} \notin \mathbb{Z}$;

$x = 5,\quad y = \dfrac{17}{7} \notin \mathbb{Z}$;

$x = 6,\quad y = 3$. Вот оно решение!

**Ответ:** $x = 6 - 7t,\ y = 3 - 4t,\ t \in \mathbb{Z}$.

Попробуем подобрать $y$. Для этого нужно испытать четыре подряд идущих числа.

$y = 0, \quad x = \dfrac{7y+3}{4} = \dfrac{3}{4} \notin \mathbb{Z}$;

$y = 1, \quad x = \dfrac{10}{4} \notin \mathbb{Z}$;

$y = 2, \quad x = \dfrac{17}{4} \notin \mathbb{Z}$;

$y = 3, \quad x = \dfrac{24}{4} = 6$. Решение найдено.

Этот перебор выгоднее, т.к. в общем случае четыре числа перебрать проще, чем семь.

**Метод последовательных замен переменных.**

Если один из коэффициентов $a, b$ равен $\pm 1$, то уравнение $ax + by = c$ сразу решается. Например:

$$5x + y = 7 \;\Rightarrow\; y = 7 - 5x, \;\; x = t \in \mathbb{Z} \text{ – любое} \;\Rightarrow$$

$$\Rightarrow \;\; x = t, \;\; y = 7 - 5t, \;\; t \in \mathbb{Z}.$$

*Метод состоит в том, чтобы уменьшать коэффициенты при $x, y$ до тех пор, пока один из них не станет равным 1 или $-1$.*

Это можно делать при помощи следующих приёмов.

*1) Если в уравнении $ax + by = c$ коэффициенты $a, b \vdots k$ и оно имеет решения, то $c \vdots k$ и уравнение можно сократить на $k$, уменьшив все коэффициенты.*

*2) Если в уравнении, например, $a > b$, то*

$$ax + by = c \;\Leftrightarrow\; (a-b)x + b(x+y) = c.$$

*Сделав замену $u = x + y$, получим уравнение, в котором один из коэффициентов стал меньше.*

*3) Если два коэффициента, например $a$ и $c$, делятся на некоторое $k$, а третий коэффициент взаимно прост с $k$, то из равенства $ax+by=c$ следует, что $y \vdots k$, тогда можно сделать замену $y=ku$ и сократить на $k$.*

**Пример.** Решить уравнение $8x-18y=6$.

Так как все коэффициенты делятся на 2, то можно сократить на 2:

$$4x-9y=3.$$

Так как $9y,\ 3 \vdots 3$, то

$$4x \vdots 3 \ \Rightarrow\ x \vdots 3 \ \Rightarrow\ \boxed{x=3u}.$$

Подставляем это в уравнение и упрощаем.

$$4\cdot 3u-9y=3 \ \Leftrightarrow\ 4u-3y=1.$$

Теперь воспользуемся второй возможностью.

$$4u-3y=1 \ \Leftrightarrow\ u+3u-3y=1 \ \Leftrightarrow\ u+3(u-y)=1 \ \Leftrightarrow$$

$$\Leftrightarrow\ u+3v=1,\ \boxed{v=u-y}.$$

Коэффициент при $u$ равен 1. Поэтому последнее уравнение можно решить. При этом $u$ выразится через $v$. После этого, двигаясь по заменам в обратном порядке, мы можем выразить все неизвестные через $v$, в частности, $x, y$ выразятся через $v$ и получится общее решение исходного уравнения.

$u=1-3v$,

$y=u-v=(1-3v)-v=1-4v$,

$x=3u=3(1-3v)=3-9v,\ v\in\mathbb{Z}$.

**Ответ:** $x=3-9v,\ y=1-4v,\ v\in\mathbb{Z}$.

## Занятие 9

**Теоретический материал.** Диофантовы уравнения первой степени. Связь диофантовых уравнений и сравнений первой степени. Теорема о решениях диофантовых уравнений. Различные способы решения диофантовых уравнений первой степени.

**Основные типы задач.** Решение диофантовых уравнений первой степени разными способами.

### Задания для практических занятий

**81.** Дайте определение диофантова уравнения первой степени от двух неизвестных. Сформулируйте теорему о взаимосвязи диофантовых уравнений и сравнений первой степени.

**82.** Решите диофантовы уравнения, используя сравнения:

а) $5x - 7y = 1$; б) $12x + 17y = 2$;

в) $15x - 27y = 4$; г) $51x + 7y = 6$.

**83.** Сформулируйте теорему об общем виде решений диофантова уравнения. Укажите способы решения диофантовых уравнений (способ, основанный на подборе частного решения, метод уменьшения коэффициентов последовательными заменами неизвестных).

**84.** Решите диофантовы уравнения:

а) $15x + 21y = 2$; б) $31x - 16y = 9$;

в) $23x + 17y = -3$; г) $19x + 24y = 7$.

Найдите все такие решения этих уравнений, что $33 \le x \le 77$.

**85.** Требуется проложить трассу трубопровода длиной 2007 метров. В распоряжении строителей имеются трубы

длиной 11 и 16 метров. Сколько труб и какой длины понадобится, чтобы проложить трубопровод с наименьшим количеством швов, не разрезая трубы?

**86.** Кузнечик находится в 277 сантиметрах от пищи. Со стороны пищи дует ветер с постоянной скоростью. Кузнечик может прыгать на 25 сантиметров против ветра и на 37 сантиметров по ветру. Сколько раз и в каком направлении он должен прыгнуть, чтобы попасть точно в место расположения пищи? Какое наименьшее количество прыжков ему на это понадобится?

## Дополнительные задания

**87.** Среди чисел вида $7m+3$ найдите наименьшее положительное число, кратное 23.

**88.** Среди чисел вида $8m+5$ найдите наименьшее положительное число, кратное 19.

**89.** Припишите справа к числу 723 две цифры так, чтобы полученное пятизначное число при делении на 31 давало в остатке 7.

**90.** Найдите расстояние между соседними целыми точками прямой $5x-12y=27$.

**91.** Решите в целых числах систему

$$\begin{cases} x-y-3z=1, \\ x+y+2z=1. \end{cases}$$

**92.** Среди чисел вида $3n+1$ найдите пять:

а) наименьших натуральных чисел, кратных пяти;

б) наименьших натуральных чисел, кратных семи;

в) наибольших отрицательных чисел, кратных 8;

г) наибольших отрицательных чисел, кратных 11.

## Контрольная работа №2

*Примерный вариант*

1. Решите сравнение первой степени $24x \equiv 18 \pmod{21}$.

2. Решите систему сравнений первой степени:

$$\begin{cases} x \equiv 5 \pmod{7}, \\ x \equiv 8 \pmod{15}. \end{cases}$$

3. Найдите все целые решения уравнения

$$60x + 21y = 30,$$

удовлетворяющие условию $40 \le x \le 90$.

# *ТЕМА 3.* ЦЕПНЫЕ ДРОБИ

## §1. Конечные цепные дроби

**Определение.** Выражение вида

$$\beta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ldots a_{n-1} + \cfrac{1}{a_n}}}},$$

где $a_i \in \mathbb{Z}$, $a_1, a_2, \ldots a_{n-1} \geq 1$, причём $a_n > 1$, называется *конечной цепной дробью.* Числа $a_i$ называются *неполными частными, $n$ – длиной* цепной дроби. Цепная дробь, как числовое выражение, равна некоторому рациональному числу, которое называется *значением дроби.*

Неполные частные однозначно определяют цепную дробь, поэтому для записи цепной дроби часто используют сокращённую форму записи:

$$\beta = [a_0, a_1, a_2, \ldots, a_n].$$

Для каждой цепной дроби можно рассматривать *подходящие дроби.* А именно, *k-той подходящей дробью* $(k \leq n)$ к данной цепной дроби называется число (цепная дробь)

$$A_k = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ldots a_{k-1} + \cfrac{1}{a_k}}}}.$$

*Бесконечная цепная дробь* – это выражение вида:

$$\beta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ldots a_k + \cfrac{1}{\ldots}}}},$$

где все $a_i$ – целые числа, причём $a_i \geq 1$ начиная с $i = 1$.

**Определение.** *Значением бесконечной цепной дроби* по определению полагается $\lim\limits_{k\to\infty} A_k$ (если он существует).

Многие свойства являются общими для конечных и бесконечных цепных дробей, поэтому в дальнейшем, если не оговорено противное, рассматриваются сразу оба случая.

**Определение.** Определим числа $P_k$ и $Q_k$ по индукции при помощи следующих соотношений:

$$P_0 = a_0, \quad P_1 = a_0 a_1 + 1, \quad P_k = P_{k-1} \cdot a_k + P_{k-2}, \quad k \geq 2;$$

$$Q_0 = 1, \quad Q_1 = a_1, \quad Q_k = Q_{k-1} \cdot a_k + Q_{k-2}, \quad k \geq 2.$$

**Свойства** (подходящих дробей). *Пусть дана цепная дробь* $[a_0, a_1, a_2, \ldots]$, *тогда имеют место следующие свойства.*

*1)* $A_k = \dfrac{P_k}{Q_k}$.

*2)* $P_k \cdot Q_{k-1} - P_{k-1} Q_k = (-1)^{k-1}$.

*3) Числа* $P_k, Q_k$ *взаимно просты.*

*4)* $\dfrac{P_k}{Q_k} - \dfrac{P_{k-1}}{Q_{k-1}} = \dfrac{(-1)^{k-1}}{Q_k Q_{k-1}}, \quad \left|\dfrac{P_k}{Q_k} - \dfrac{P_{k-1}}{Q_{k-1}}\right| = \dfrac{1}{Q_k Q_{k-1}}$.

*5) Числа* $Q_i$ *образуют монотонно возрастающую последовательность:*

$$1 = Q_0 \le Q_1 < Q_2 < Q_3 < \dots .$$

*6)* $P_k \cdot Q_{k-2} - P_{k-2}Q_k = (-1)^k \cdot a_k$ .

*7) Чётные подходящие дроби образуют возрастающую последовательность, нечётные подходящие дроби образуют убывающую последовательность. Всякая чётная подходящая дробь меньше любой нечётной.*

*8) Модуль расстояния между соседними подходящими дробями монотонно уменьшается и стремится к 0, если дробь бесконечна.*

Как простое следствие последних свойств получаем

**Теорему.** *Значение всякой бесконечной цепной дроби существует.*

**Замечание.** Очевидно, что предел $\lim\limits_{k\to\infty} A_k = \lim\limits_{k\to\infty} \dfrac{P_k}{Q_k}$ всегда лежит между числами $\dfrac{P_{2k}}{Q_{2k}}$, $\dfrac{P_{2k+1}}{Q_{2k+1}}$.

**Определение.** Говорят, что *число* $\beta$ *представлено в виде цепной дроби* (конечной или бесконечной), если значение этой цепной дроби равно $\beta$ .

**Теорема.** *Всякое рациональное число представимо в виде конечной цепной дроби, причём такое представление единственно.*

Действительно, пусть $\beta = \dfrac{n}{m}$ – несократимая дробь, $n$ – целое число, $m$ – натуральное число. Составим для чисел $n$ и $m$ алгоритм Евклида и разделим каждое соотношение на делитель.

$$
\begin{aligned}
n &= ma_0 + r_1,\\
m &= r_1a_1 + r_2,\\
r_1 &= r_2a_2 + r_3,\\
&\cdots\cdots\\
r_{n-2} &= r_{n-1}a_{n-1} + r_n,\\
r_{n-1} &= r_na_n.
\end{aligned}
\quad\Rightarrow\quad
\begin{aligned}
\frac{n}{m} &= a_0 + \frac{r_1}{m},\\
\frac{m}{r_1} &= a_1 + \frac{r_2}{r_1},\\
\frac{r_1}{r_2} &= a_2 + \frac{r_3}{r_2},\\
&\cdots\cdots\\
\frac{r_{n-2}}{r_{n-1}} &= a_{n-1} + \frac{r_n}{r_{n-1}},\\
\frac{r_{n-1}}{r_n} &= a_n.
\end{aligned}
$$

Последовательно подставляя каждое равенство в первое равенство, получаем искомую цепную дробь.

$$\frac{n}{m} = a_0 + \frac{r_1}{m} = a_0 + \frac{1}{a_1 + \dfrac{r_2}{r_1}} = a_0 + \frac{1}{a_1 + \dfrac{1}{a_2 + \dfrac{r_3}{r_2}}} = \dots$$

$$\dots = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\dots a_{n-1} + \cfrac{1}{a_n}}}}.$$

Неполные частные цепной дроби равны частным в алгоритме Евклида. Длина цепной дроби равна длине алгоритма Евклида.

**Пример.** Представить в виде цепной дроби число $\beta = \dfrac{18}{7}$.

$$\begin{aligned} 18 &= 7\cdot 2 + 4,\\ 7 &= 4\cdot 1 + 3,\\ 4 &= 3\cdot 1 + 1,\\ 3 &= 1\cdot 3. \end{aligned} \quad \Rightarrow \quad \frac{18}{7} = [2,1,1,3] = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3}}}.$$

Используя рекуррентные соотношения из определения подходящих дробей, можно достаточно быстро вычислять все подходящие дроби. Для этого необходимо составить таблицу следующего вида.

| $k$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $a_k$ | 2 | 1 | 1 | 3 |
| $P_k$ | 2 | 3 | 5 | 18 |
| $Q_k$ | 1 | 1 | 2 | 7 |

В первую строку записываются все значения $k = 0, 1, 2, 3$. Во вторую – все неполные частные $a_k = 2, 1, 1, 3$. В третью и четвёртую строки – значения $P_k$ и $Q_k$, которые последовательно вычисляются по определению.

$$A_0 = a_0 = \frac{a_0}{1} \Rightarrow P_0 = a_0 = 2,\ Q_0 = 1.$$

Записываем эти значения в соответствующие ячейки.

$$A_1 = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} \quad \Rightarrow \quad P_1 = a_0 a_1 + 1 = 3,\ Q_1 = a_1 = 1.$$

Значения $P_2, P_3, P_4$ вычисляем по рекуррентному соотношению $P_k = P_{k-1}\cdot a_k + P_{k-2}$.

$$P_2 = P_1 \cdot a_2 + P_0 = 3\cdot 1 + 2 = 5,$$

$$P_3 = P_2 \cdot a_3 + P_1 = 5\cdot 3 + 3 = 18.$$

Вычисления можно производить чисто механически: *чтобы вычислить значение* $P_k$ *в некоторой клетке нужно взять число из клетки слева (там* $P_{k-1}$*), умножить его на число из клетки выше (там* $a_k$*) и сложить с числом в клетке, расположенной через одну слева (там* $P_{k-2}$*).* Пользуясь этим алгоритмом и двигаясь слева направо, вычисляем все значения $P_k$. Затем аналогично вычисляем все значения $Q_k$.

В результате вычислены все дроби, подходящие к данной цепной дроби:

$$A_0 = \frac{2}{1} = 2,\ A_1 = \frac{3}{1} = 3,\ A_2 = \frac{5}{2},\ A_3 = \frac{18}{7}.$$

Последняя подходящая дробь, естественно, совпадает с исходным числом.

Используя разложение в цепную дробь, подходящие дроби и свойство 2, можно предложить новый способ решения диофантовых уравнений вида

$$ax + by = c.$$

Пусть числа $a, b$ взаимно просты. Разложим число $\frac{a}{b}$ в конечную цепную дробь:

$$\frac{a}{b} = [a_0, a_1, a_2, \ldots, a_n].$$

Согласно определению подходящих дробей $\frac{P_n}{Q_n} = \frac{a}{b}$, причём ввиду несократимости этих дробей

$$P_n = a,\ Q_n = b.$$

Запишем свойство 2:

$$P_n \cdot Q_{n-1} - P_{n-1}Q_n = (-1)^{n-1} = a \cdot Q_{n-1} - P_{n-1} \cdot b .$$

Из последнего равенства несложно получить частное решение диофантова уравнения. Для этого достаточно его умножить на $(-1)^{n-1} c$.

$$a \cdot \left((-1)^{n-1} c \cdot Q_{n-1}\right) + b \cdot \left((-1)^n c \cdot P_{n-1}\right) = (-1)^{2n-2} c = c \;\Rightarrow$$

$$\Rightarrow \; x_0 = (-1)^{n-1} c \cdot Q_{n-1}, \quad y_0 = (-1)^n c \cdot P_{n-1} .$$

Остальные решения диофантовых уравнений находятся по формуле решений:

$$x = x_0 + bt, \; y = y_0 - at, \; t \in \mathbb{Z} .$$

**Пример.** Решить уравнение $18x + 7y = 5$ в целых числах.

Выше было получено, что $\frac{18}{7} = [2, 1, 1, 3]$, $n = 3$ и найдены все подходящие дроби. Предпоследняя подходящая дробь равна $\frac{5}{2}$.

В результате получаем:

$$P_n \cdot Q_{n-1} - P_{n-1}Q_n = (-1)^{n-1} \;\Leftrightarrow\; 18 \cdot 2 - 5 \cdot 7 = (-1)^{3-1} = 1 .$$

Умножаем это равенство на $5$:

$$18 \cdot 2 \cdot 5 - 7 \cdot 5 \cdot 5 = 5 \;\Rightarrow\; 18 \cdot (10) + 7 \cdot (-25) = 5 \;\Rightarrow$$

$$\Rightarrow \; x_0 = 10, \; y_0 = -25 \;\Rightarrow\; x = 10 + 7t, \; y = -25 - 18t, \; t \in \mathbb{Z} .$$

Это общее решение данного диофантова уравнения.

## Занятие 10

**Теоретический материал.** Понятие конечной цепной дроби. Подходящие дроби, их свойства. Представление рационального числа в виде конечной цепной дроби. Применение цепных дробей для решения диофантовых уравнений.

**Основные типы задач.** Вычисление значения цепной дроби и всех подходящих дробей. Разложение рационального числа в цепную дробь. Решение диофантовых уравнений при помощи цепных дробей.

### Задания для практических занятий

**93.** Дайте определение конечной цепной дроби, её подходящих дробей. Сформулируйте простейшие свойства подходящих дробей.

**94.** Вычислите значение цепной дроби и все её подходящие дроби:

а) $[1,2,3,2]$; б) $[-2,2,1,4,3]$;

в) $[1,2,1,5,2]$; г) $[-3,1,1,3,3]$.

**95.** Представьте в виде цепной дроби числа:

а) $\frac{23}{16}$; б) $-\frac{74}{45}$.

в) $\frac{50}{37}$; г) $-\frac{56}{23}$.

**96.** Решите диофантовы уравнения и найдите наименьшие по абсолютной величине решения:

а) $23x+18y=31$; б) $41x-37y=5$;

в) $85x+62y=5$; г) $67x-49y=11$.

ДОПОЛНИТЕЛЬНЫЕ ЗАДАНИЯ

**97.** Вычислите значение цепной дроби и все её подходящие дроби:

а) $[1,1,1,1,1,1,1,1,1,2]$;

б) $[1,2,1,2,1,2,1,2]$.

**98.** Представьте в виде цепной дроби числа:

а) $\frac{144}{89}$; б) $\frac{153}{112}$.

**99.** Решите диофантовы уравнения и найдите наименьшие по абсолютной величине решения:

а) $24x+14y=20$; б) $18x-19y=20$;

в) $144x+89y=1$; г) $153x-112y=3$.

## §2. Бесконечные цепные дроби

Бесконечные цепные дроби являются достаточно удобным и точным инструментом для приближённого представления чисел.

**ОПРЕДЕЛЕНИЕ.** Пусть $\beta=[a_0,a_1,a_2,\ldots]$ – цепная дробь (конечная или бесконечная). *Полными частными* этой дроби называются числа $\beta_0,\beta_1,\beta_2,\ldots$, которые определяются соотношениями

$$\beta=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\ldots a_{k-1}+\cfrac{1}{\beta_k}}}},\quad k>0;\quad \beta_0=\beta\,.$$

**Замечание.** 1) Данные числа определены однозначно, т.к. они однозначно выражаются через числа $\beta, a_0, a_1, \ldots, a_{k-1}$.

2) Для конечных цепных дробей очевидно, что

$$\beta_k = [a_k, a_{k+1}, a_{k+2}, \ldots, a_n] = a_k + \cfrac{1}{a_{k+1} + \cfrac{1}{\ldots a_{n-1} + \cfrac{1}{a_n}}}, \quad k \le n,$$

т.е. $k$-тое полное частное – это часть цепной дроби, начиная с $a_k$.

**Теорема** (о свойствах полных частных). *Пусть* $\beta = [a_0, a_1, a_2, \ldots]$ *– цепная дробь и* $\beta_{k+1}$ *– полное частное, тогда выполняются следующие равенства.*

*1)* $\beta = \dfrac{P_k \cdot \beta_{k+1} + P_{k-1}}{Q_k \cdot \beta_{k+1} + Q_{k-1}}$, $k \ge 1$.

*2)* $\beta_k = [a_k, a_{k+1}, a_{k+2}, \ldots]$.

*3)* $a_k = [\beta_k]$ *(целая часть* $\beta_k$*).*

Если бесконечная цепная дробь является периодической, то её значение можно найти, используя свойства полных частных. Кроме того, это значение можно найти, воспользовавшись периодичностью.

**Пример.** Найти $\beta = [3, 1, 2, 1, 2, 1, 2, \ldots]$.

Рассмотрим первое полное частное, которое является чисто периодическим $\alpha = \beta_1 = [1, 2, 1, 2, 1, \ldots]$. Для него выполняется равенство

$$\beta = 3 + \frac{1}{\alpha}.$$

Воспользовавшись периодичностью $\alpha$, получаем

$$\alpha = 1 + \frac{1}{2 + \frac{1}{\alpha}}.$$

Число $\alpha$ легко находится из этого условия:

$$\alpha = 1 + \frac{1}{2 + \frac{1}{\alpha}} = 1 + \frac{\alpha}{2\alpha + 1} = \frac{3\alpha + 1}{2\alpha + 1} \;\Leftrightarrow\; 2\alpha^2 + \alpha = 3\alpha + 1 \;\Leftrightarrow$$

$$\Leftrightarrow\; 2\alpha^2 - 2\alpha - 1 = 0 \;\Leftrightarrow\; \alpha = \frac{1 \pm \sqrt{3}}{2}.$$

Отрицательное значение не подходит, т.к. по определению $\alpha > 0$, поэтому $\alpha = \frac{1 + \sqrt{3}}{2}$.

Подставляем это число в первую формулу и находим

$$\beta = 3 + \frac{1}{\alpha} = 3 + \frac{2}{1 + \sqrt{3}} = \frac{5 + 3\sqrt{3}}{1 + \sqrt{3}} = \frac{\left(5 + 3\sqrt{3}\right)\left(1 - \sqrt{3}\right)}{\left(1 + \sqrt{3}\right)\left(1 - \sqrt{3}\right)} = 2 + \sqrt{3}.$$

**Теорема.** *Всякое действительное число единственным образом представимо в виде цепной дроби. Если число рациональное, то дробь конечная. Если число иррациональное, то дробь бесконечная.*

**Алгоритм разложения в цепную дробь** состоит в следующем.

Полагаем $a_0 = [\beta]$ и рассматриваем число $x_1 = \frac{1}{\beta - a_0} \;\Rightarrow\; \beta = a_0 + \frac{1}{x_1}$. Согласно определению $\beta_1 = x_1$. Далее продолжаем аналогично.

$$a_1 = [\beta_1], \quad x_2 = \frac{1}{\beta_1 - a_1} \;\Rightarrow\; \beta_1 = a_1 + \frac{1}{x_2} \;\Rightarrow$$

$$\Rightarrow \quad \beta = a_0 + \frac{1}{a_1 + \dfrac{1}{x_2}} \quad \Rightarrow \quad \beta_2 = x_2 ;$$

$$a_2 = [\beta_2], \quad x_3 = \frac{1}{\beta_2 - a_2} \quad \Rightarrow \quad \ldots\ldots .$$

Каждый шаг алгоритма состоит из двух действий.

1) Нахождение $k$-го неполного частного как целой части соответствующего полного частного:

$$\beta_k = [a_k] .$$

2) Нахождение следующего полного частного по формуле

$$\beta_{k+1} = \frac{1}{\beta_k - a_k} .$$

На каждом шаге алгоритма получается равенство вида

$$\beta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ldots a_k + \cfrac{1}{\beta_{k+1}}}}} = [a_0, a_1, a_2, \ldots, a_k, \beta_{k+1}] . \quad (*)$$

Оно даёт начальную часть разложения числа $\beta$ в цепную дробь. Если число $\beta$ является иррациональным, то процесс разложения продолжается бесконечно.

**Пример.** Разложить в цепную дробь число $\beta = 2 + \sqrt{3}$ .

Применяем алгоритм.

1-й шаг.

$$a_0 = [\beta] = \left[2 + \sqrt{3}\right] = 3 ,$$

$$\beta_1 = \frac{1}{\beta - a_0} = \frac{1}{\left(2+\sqrt{3}\right)-3} = \frac{\left(\sqrt{3}+1\right)}{\left(\sqrt{3}-1\right)\left(\sqrt{3}+1\right)} = \frac{\sqrt{3}+1}{2}.$$

2-й шаг.

$$a_1 = [\beta_1] = \left[\frac{\sqrt{3}+1}{2}\right] = 1,$$

$$\beta_2 = \frac{1}{\beta_1 - a_1} = \frac{1}{\frac{\sqrt{3}+1}{2}-1} = \frac{2}{\sqrt{3}-1} = \frac{2\left(\sqrt{3}+1\right)}{\left(\sqrt{3}-1\right)\left(\sqrt{3}+1\right)} = \sqrt{3}+1.$$

3-й шаг.

$$a_2 = [\beta_2] = \left[\sqrt{3}+1\right] = 2,$$

$$\beta_3 = \frac{1}{\beta_2 - a_2} = \frac{1}{\sqrt{3}+1-2} = \frac{1}{\sqrt{3}-1} = \frac{\left(\sqrt{3}+1\right)}{\left(\sqrt{3}-1\right)\left(\sqrt{3}+1\right)} = \frac{\sqrt{3}+1}{2}.$$

Полное частное повторилось: $\beta_1 = \beta_3$, поэтому дальше и полные и неполные частные будут повторяться с периодом 2:

$$1 = a_1 = a_3 = a_5 = \ldots,$$

$$2 = a_2 = a_4 = a_6 = \ldots.$$

В результате $2+\sqrt{3} = [3, 1, 2, 1, 2, \ldots\ldots]$, как было заранее известно из предыдущего примера.

В общем случае числа $\beta_k$ не обязательно будут повторяться. Можно доказать

**Теорему** (Лагранж). *Число $\beta$ представимо в виде периодической цепной дроби тогда и только тогда, когда $\beta$ квадратичная иррациональность (т.е. иррациональный корень некоторого квадратного уравнения с целыми коэффициентами).*

## Занятие 11

**Теоретический материал.** Бесконечные цепные дроби, значение бесконечной цепной дроби. Понятие полного частного, его свойства. Вычисление значения бесконечной периодической цепной дроби. Представление действительного числа в виде цепной дроби. Теорема Лагранжа.

**Основные типы задач.** Вычисление значения бесконечной периодической цепной дроби. Разложение действительного числа в цепную дробь.

### Задания для практических занятий

**100.** Дайте определение бесконечной цепной дроби, значения бесконечной цепной дроби, полных частных, перечислите их свойства.

**101.** Найдите значение цепной дроби:

а) $\left[1,1,1,(1)\right]$; б) $\left[(1,1,2)\right]$;

в) $\left[1,2,(1,3)\right]$; г) $\left[1,2,(1,1,3)\right]$.

**102.** Сформулируйте теорему о представлении иррационального числа бесконечной цепной дробью, опишите алгоритм получения этого представления.

**103.** Представьте в виде цепной дроби числа:

а) $\sqrt{5}$; б) $\dfrac{3+\sqrt{21}}{6}$;

в) $\sqrt{2}$; г) $\dfrac{\sqrt{37}-1}{3}$.

**104.** Сформулируйте теорему Лагранжа о квадратичных иррациональностях.

**105.** Найдите первые несколько неполных частных разложения в цепную дробь чисел:

а) $\log_2 3$; б) $\log_4 3$;

в) $\sqrt[3]{2}$; г) $\sqrt[4]{2}$.

ДОПОЛНИТЕЛЬНЫЕ ЗАДАНИЯ

**106.** Найдите значение цепной дроби:

а) $[1,2,3,(2,1)]$; б) $[1,2,(2,1,3)]$.

**107.** Представьте в виде цепной дроби числа:

а) $\sqrt{10}$; б) $\sqrt{44}$;

в) $\sqrt{7}$; г) $\sqrt{6}$.

**108.** Найдите первые несколько неполных частных разложения в цепную дробь чисел:

а) $\log_3 5$; б) $\sqrt[3]{3}$.

## §3. Приближение чисел цепными дробями

Пусть $\beta$ равно значению (конечной или бесконечной) цепной дроби $[a_0, a_1, a_2, \ldots]$.

**Теорема** (о том, что подходящие дроби монотонно приближаются к значению цепной дроби). *Для двух соседних подходящих дробей* $\frac{P_k}{Q_k}$, $\frac{P_{k-1}}{Q_{k-1}}$ *выполняется неравенство*

$$\left|\beta - \frac{P_k}{Q_k}\right| < \left|\beta - \frac{P_{k-1}}{Q_{k-1}}\right|,$$

*т.е. каждая последующая подходящая дробь ближе к числу* $\beta$ *, чем предыдущая.*

Для достаточно больших значений $k$ дробь $\frac{P_k}{Q_k}$ можно считать приближённым значением числа $\beta$. В доказательстве теоремы о существовании значения дроби получена *оценка точности* этого *приближения:*

$$\left|\beta - \frac{P_k}{Q_k}\right| < \frac{1}{Q_k^2}.$$

Этим можно пользоваться, чтобы найти приблизительное значение цепной дроби.

**Пример.** Вычислить приблизительное значение числа $2+\sqrt{3}$ с точностью до $\frac{1}{1000}$.

Для того, чтобы найти приближение и воспользоваться оценкой, вычисляем подходящие дроби и находим такое $k$, что

$$\frac{1}{Q_k^2} < \frac{1}{1000}.$$

| $a_k$ | 3 | 1 | 2 | 1 | 2 | 1 | 2 | ... |
|---|---|---|---|---|---|---|---|---|
| $P_k$ | 3 | 4 | 11 | 15 | 41 | 56 | 153 | ... |
| $Q_k$ | 1 | 1 | 3 | 4 | 11 | 15 | 41 | ... |

Замечаем, что $41^2 = 1681 > 1000 \Rightarrow \frac{1}{Q_6^2} < \frac{1}{1000}$. В результате

$$2+\sqrt{3} \approx \frac{153}{41} \pm \frac{1}{10^3}.$$

Оценку точности приближения можно несколько улучшить.

**Теорема** (о точности приближения цепной дробью). *Если число* $\beta$ *представлено в виде цепной дроби* $\beta = [a_0, a_1, a_2, \ldots]$ *и* $\frac{P_k}{Q_k}$, $\frac{P_{k+1}}{Q_{k+1}}$ *– две соседние подходящие дроби, то*

$$\left|\beta - \frac{P_k}{Q_k}\right| \le \frac{1}{Q_k \cdot Q_{k+1}}.$$

*Причём, если* $\beta \ne \frac{P_{k+1}}{Q_{k+1}}$, *то неравенство строгое.*

**Теорема** (об ошибке приближения цепной дробью). *Если* $\beta \ne \frac{P_k}{Q_k}$, *то* $\left|\beta - \frac{P_k}{Q_k}\right| > \frac{1}{Q_k \cdot (Q_{k+1} + Q_k)}$.

## Занятие 12

**Теоретический материал.** Приближение действительных чисел цепными дробями, теоремы о точности и ошибке приближения.

**Основные типы задач.** Приближение действительного числа подходящей дробью с заданной точностью.

### Задания для практических занятий

**109.** Дайте определение приближения действительного числа рациональным числом. Сформулируйте теоремы о точности и об ошибке приближения действительного числа подходящей дробью.

**110.** Найдите приближение данного числа подходящей дробью с точностью до $\varepsilon$, оцените ошибку этого приближения:

а) $\frac{1+\sqrt{5}}{2}$, $\varepsilon = \frac{1}{100}$; б) $\frac{3+\sqrt{21}}{6}$, $\varepsilon = \frac{1}{1000}$;

в) $\sqrt{2}$, $\varepsilon = \frac{1}{100}$; г) $\frac{\sqrt{37}-1}{3}$, $\varepsilon = \frac{1}{1000}$.

## Дополнительные задания

**111.** Найдите приближение данного числа подходящей дробью с точностью до $\varepsilon$. Оцените ошибку этого приближения:

а) $\sqrt{10}$, $\varepsilon = \frac{1}{100}$; б) $\sqrt{44}$, $\varepsilon = \frac{1}{100}$;

в) $\sqrt{7}$, $\varepsilon = \frac{1}{1000}$; г) $\sqrt{6}$, $\varepsilon = \frac{1}{1000}$.

**112.** Найдите приближение числа $\pi = 3{,}14159265...$ с точностью до $10^{-4}$ рациональным числом со знаменателем, меньшим 1000.

## Контрольная работа №3

*Примерный вариант*

1. Представьте в виде цепной дроби число $\frac{351}{151}$ и найдите все подходящие дроби.

2. Найдите все целые решения уравнения $351x + 151y = 1$.

3. Найдите значение цепной дроби $[2,(1,3)]$.

4. Найдите приближение числа из предыдущей задачи подходящей дробью с точностью до $\varepsilon = \frac{1}{100}$.

# *ТЕМА 4.* ПЕРВООБРАЗНЫЕ КОРНИ И ИНДЕКСЫ

## §1. Первообразные корни

**N.B.** Если не оговорено противное, то все числа, которые рассматриваются в этой теме, предполагаются взаимно простыми с модулем $m > 1$.

**ОПРЕДЕЛЕНИЕ.** *Порядком* (или *показателем*) числа $a$ по модулю $m$ называется такое наименьшее положительное число $d$, что

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

Обозначение $d = O_m(a)$.

**ПРИМЕР.** Найти $O_{10}(7)$.

Проверяем характеристическое свойство порядка для всех степеней, начиная с самых маленьких.

$7^1 \equiv 7 \not\equiv 1 (\mathrm{mod}\, 10)$,

$7^2 \equiv 9 \not\equiv 1 (\mathrm{mod}\, 10)$,

$7^3 \equiv 63 \equiv 3 \not\equiv 1 (\mathrm{mod}\, 10)$,

$7^4 \equiv 21 \equiv 1 (\mathrm{mod}\, 10)$.

Число $d$ с данным свойством найдено. Так как мы перебирали степени, начиная с 1, то $d = 4$ – наименьшая степень с таким свойством.

**ОТВЕТ:** $O_{10}(7) = 4$.

**ТЕОРЕМА** (о существовании порядка). *Пусть число $a$ взаимно просто с $m$, тогда $O_m(a)$ существует.*

Способы нахождения порядка элемента основаны на его свойствах.

**Свойства** (порядков).

*1) Если* $a \equiv b \pmod m$, *то* $O_m(a) = O_m(b)$.

*2) Если* $O_m(a) = d$, *то числа* $a^1, a^2, \ldots, a^d$ *попарно не сравнимы по модулю* $m$.

*3)* $a^n \equiv 1 \pmod m \Leftrightarrow n \vdots O_m(a)$.

*4)* $\varphi(m) \vdots O_m(a)$.

**Замечание.** Ввиду свойства 4, при нахождении порядка можно перебирать не все степени подряд, начиная с 1, а только натуральные делители $\varphi(m)$. Их конечное число.

**Пример.** Найти $O_{10}(7)$.

Находим $\varphi(10) = 10\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 4$. Делителями числа 4 являются числа 1, 2 и 4. Эти степени и проверяем.

$7^1 \equiv 7 \not\equiv 1 \pmod{10}$,

$7^2 \equiv 9 \not\equiv 1 \pmod{10}$,

$7^4 \equiv (9)^2 = 81 \equiv 1 \pmod{10} \Rightarrow O_{10}(7) = 4$.

*5) Пусть* $d = O_m(a)$, *тогда* $\forall\, s, k$ *выполняется:*

$$a^s \equiv a^k \pmod m \Leftrightarrow s \equiv k \pmod d.$$

*6) Если* $O_m(a), O_m(b)$ *взаимно просты, то*

$$O_m(ab) = O_m(a) \cdot O_m(b).$$

*7) Пусть* $d = O_m(a)$ *и* $НОД(n, d) = k$, *тогда* $O_m\left(a^n\right) = \frac{d}{k}$.

**Следствие.** *Если* $d = O_m(a)$ *и* $d \vdots n$, *то* $O_m\left(a^n\right) = \frac{d}{n}$.

Из свойства 4 следует, что наибольшее возможное значение порядка по модулю $m$ равно $\varphi(m)$. Числа с такими порядками играют большую роль в теории сравнений.

**Определение.** Если порядок по модулю $m$ некоторого числа равен $\varphi(m)$, то это число называется *первообразным корнем по модулю* $m$.

**Замечание.** 1) *Если* $a$ *– первообразный корень, то степени* $a^1, a^2, \ldots, a^{\varphi(m)}$ *образуют приведённую систему вычетов по модулю* $m$.

*2) Если число* $b$ *взаимно просто с* $m$ *и* $a$ *– первообразный корень по модулю* $m$, *то существует* $k \le \varphi(m)$ *такое, что* $a^k \equiv b \pmod m$.

*3) Вместе с каждым первообразным корнем по модулю* $m$ *все элементы класса* $[a]_m$ *также будут первообразными корнями по модулю* $m$.

Ввиду замечания 3, в качестве первообразных корней можно рассматривать классы вычетов целиком. В задачах на нахождение первообразных корней можно ограничиться рассмотрением какой-нибудь приведённой системы по данному модулю.

**Пример.** Найти все первообразные корни по модулю 7.

Вычисляем $\varphi(7) = 6$. Делителями этого числа являются числа 1, 2, 3, 6. Выбираем приведённую систему вычетов по модулю 7, например: 1, 2, 3, 4, 5, 6. Затем вычисляем порядки каждого из этих элементов.

$$O_7(1) = 1,$$

$$2^2 \equiv 4 (\mathrm{mod}\, 7),\ 2^3 \equiv 8 \equiv 1 (\mathrm{mod}\, 7) \ \Rightarrow\ O_7(2) = 3,$$

$$3^2 \equiv 9 (\mathrm{mod}\, 7),\ 3^3 \equiv 27 \equiv 6 (\mathrm{mod}\, 7) \ \Rightarrow\ O_7(3) = 6,$$

$$4^2 \equiv 16 \equiv 2 (\mathrm{mod}\, 7),\ 4^3 \equiv 8 \equiv 1 (\mathrm{mod}\, 7) \ \Rightarrow\ O_7(4) = 3,$$

$$5^2 \equiv 25 \equiv 4 (\mathrm{mod}\, 7),\ 5^3 \equiv 20 \equiv 6 (\mathrm{mod}\, 7) \ \Rightarrow\ O_7(5) = 6,$$

$$6^2 \equiv 36 \equiv 1 (\mathrm{mod}\, 7) \ \Rightarrow\ O_7(6) = 2.$$

В результате первообразными корнями по модулю 7 будут числа 3 и 5 или, точнее, все элементы классов $[3]_7$, $[5]_7$.

**Теорема** (о существовании первообразных корней) П*ервообразные корни по модулю* $m$ *существуют тогда и только тогда, когда* $m = 2, 4, p^k$ *или* $2p^k$, *для некоторого простого числа* $p$.

**Пример.** Наименьшее $m$, не входящее в этот список равно 8. Проверим, что по модулю 8 первообразных корней нет.

$\varphi(8) = 8\left(1 - \frac{1}{2}\right) = 4$. Выбираем приведённую систему вычетов по модулю 8:

$$1, 3, 5, 7.$$

$O_8(1) = 1$,

$3^2 \equiv 5^2 \equiv 7^2 \equiv 1 (\mathrm{mod}\, 8) \ \Rightarrow\ O_8(3) = O_8(5) = O_8(7) = 2 \neq 4$.

Как видим, нет числа, у которого порядок равен 4.

Основным является случай, когда $m = p$ – простое число. Следствие из теоремы ниже даёт точное количество первообразных корней по простому модулю.

**Теорема.** *Пусть $p$ – простое число и $(p-1) \vdots d$. Во всякой приведённой системе вычетов по модулю $p$ есть ровно $\varphi(d)$ чисел, имеющих порядок $d$.*

**Следствие** (о числе первообразных корней по простому модулю). *Число первообразных корней по простому модулю $p$ равно $\varphi(p-1)$.*

**Пример.** Пусть $p = 7$. Так как $\varphi(7-1) = \varphi(6) = 2$, то по модулю 7 существует ровно два первообразных корня. Они оба были найдены в одном из предыдущих примеров.

## Занятие 13

**Теоретический материал.** Порядок числа, класса по некоторому модулю. Свойства порядков. Понятие первообразного корня. Условие существования первообразных корней. Теорема о количестве первообразных корней по простому модулю.

**Основные типы задач.** Вычисление порядков чисел, нахождение первообразных корней.

### Задания для практических занятий

**113.** Дайте определение порядка числа (класса вычетов) по данному модулю. Сформулируйте простейший алгоритм вычисления порядка с использованием некоторых свойств.

**114.** Какие значения может принимать порядок числа (класса вычетов) по модулю 13, 24, 51?

**115.** Вычислите порядок числа $a$ по модулю $m$:

а) $a = 25,\ \ m = 31$; б) $a = 18,\ \ m = 29$;

в) $a = 5,\ \ m = 61$; г) $a = 3,\ \ m = 11$.

**116.** Существуют ли классы вычетов:

а) по модулю 26 порядка 7;

б) по модулю 27 порядка 6?

**117.** Найдите все классы вычетов:

а) по модулю 8 порядка 2;

б) по модулю 11 порядка 4.

**118.** Дайте определение первообразного корня по модулю m. Сформулируйте теорему об условии существования первообразных корней. Существуют ли первообразные корни по модулям 6, 8, 9, 12 ?

**119.** Найдите первообразный корень:

а) по модулю 18; б) по модулю 7.

**120.** Сформулируйте утверждение о количестве первообразных корней по простому модулю. Каково количество первообразных корней по модулю 17, 23, 11?

**121.** Найдите все первообразные корни по модулю 11.

**122.** Найдите два первообразных корня по модулю 13.

## Дополнительные задания

**123.** Докажите, что если $g$ – первообразный корень по модулю $m$ и число $s$ взаимно просто с $\varphi(m)$, то $g^s$ – также первообразный корень по модулю $m$.

**124.** Зная, что 3 является одним из первообразных корней по модулю 29, найдите остальные первообразные корни по этому модулю.

**125.** Вычислите, какое наименьшее количество раз нужно написать цифру 3, чтобы получить многозначное число, делящееся на 13.

**126.** Будет ли первообразным корнем по простому модулю $p > 2$ произведение первообразных корней по этому же модулю?

**127.** Докажите, что если $p = 2^n + 1$ – простое число и $n > 3$, то число 3 является первообразным корнем по модулю $p$.

## §2. Индексы

Пусть $g$ – какой-нибудь фиксированный первообразный корень по модулю $p$. Числа $g^1, g^2, g^3, \ldots, g^{p-1}$ образуют приведённую систему вычетов по модулю $p$, поэтому для любого числа $a$ (взаимно простого с $p$) существует число $k$ такое, что

$$a \equiv g^k \pmod{p}.$$

Это число называется *индексом $a$ по модулю $p$ при основании $g$* и обозначается $ind_g a$.

**Замечание.** *Индекс числа определяется неоднозначно.*

**Свойства** (индексов).

*1)* $a \equiv b \pmod{p} \Leftrightarrow ind_g a \equiv ind_g b \pmod{(p-1)}$.

**Замечание.** Согласно этому свойству, *все числа из некоторого класса вычетов по модулю $p$ имеют одинаковые множества индексов.* Кроме того, *индексы числа или класса вычетов образуют класс вычетов по модулю $(p-1)$.*

Определение индекса аналогично определению логарифма, поэтому они имеют схожие свойства.

*2)* $ind_g ab \equiv ind_g a + ind_g b \left(\mathrm{mod}\left(p-1\right)\right)$.

*3)* $ind_g \left(a^n\right) \equiv n \cdot ind_g a \left(\mathrm{mod}\left(p-1\right)\right)$.

Для работы с индексами удобно брать систему наименьших неотрицательных вычетов.

**Пример.** Пусть $p=5,\ g=3$. Вычислить $ind_3 37$, $ind_3 (-18)$.

$$37 \equiv 2(\mathrm{mod}\,5);\ 3^2 = 9 \equiv 4 \not\equiv 2(\mathrm{mod}\,5),\ 3^3 \equiv 12 \equiv 2(\mathrm{mod}\,5),$$

$$\Rightarrow\ ind_3(37) = ind_3(2) = [3]_4.$$

$$-18 \equiv 2(\mathrm{mod}\,5)\ \Rightarrow\ ind_3(-18) = ind_3(2) = [3]_4.$$

Из примера видно, что для вычисления индексов нужно рассматривать степени первообразного корня по данному модулю. Если индексы нужно вычислять многократно, то это можно сделать заранее, составив *таблицу индексов.*

**Пример.** Составить таблицу индексов по модулю 11 с основанием 7.

Выбираем приведённую систему наименьших неотрицательных вычетов. Пользуясь свойствами сравнений, выясняем, в каком классе вычетов лежит каждая степень 7.

$$7^0 \equiv 1(\mathrm{mod}\,11),\ 7^1 \equiv 7(\mathrm{mod}\,11),\ 7^2 = 49 \equiv 5(\mathrm{mod}\,11),$$

$$7^3 \equiv 35 \equiv 2(\mathrm{mod}\,11),\ 7^4 \equiv 14 \equiv 3(\mathrm{mod}\,11),\ 7^5 \equiv 21 \equiv 10(\mathrm{mod}\,11),$$

$$7^6 \equiv 70 \equiv 4(\mathrm{mod}\,11),\ 7^7 \equiv 28 \equiv 6(\mathrm{mod}\,11),\ 7^8 \equiv 42 \equiv 9(\mathrm{mod}\,11),$$

$$7^9 \equiv 63 \equiv 8(\mathrm{mod}\,11),\ 7^{10} \equiv 56 \equiv 1(\mathrm{mod}\,11).$$

Последнее сравнение подтверждает, что число 7 является первообразным корнем по модулю 11, т.к. $O_{11}(7)=10=\varphi(11)$.

Результаты вычислений можно записать в таблицу.

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $ind_7 a$ | 0 | 3 | 4 | 6 | 2 | 7 | 1 | 9 | 8 | 5 |

Таблицы индексов и свойства индексов применяются для решения задач. При этом в качестве основания можно брать любой первообразный корень.

**Пример.** Решить сравнение $6x \equiv 7 \pmod{11}$.

Применяем свойства 1, 2, а затем таблицу индексов.

$$6x \equiv 7 \pmod{11} \overset{1)}{\Leftrightarrow} ind_7(6x) \equiv ind_7 7 \pmod{10} \overset{2)}{\Leftrightarrow}$$

$$\overset{2)}{\Leftrightarrow} ind_7 6 + ind_7 x \equiv ind_7 7 \pmod{10} \Leftrightarrow \text{(используем таблицу)}$$

$$\Leftrightarrow 7 + ind_2 x \equiv 1 \pmod{10} \Leftrightarrow ind_2 x \equiv 1 - 7 = -6 \equiv 4 \pmod{10} \Leftrightarrow$$

$$\Leftrightarrow \text{(снова таблица и свойство 1)} \Leftrightarrow x \equiv 3 \pmod{11}.$$

**Ответ:** $x \equiv 3 \pmod{11}$.

При помощи индексов можно решать алгебраические сравнения любой степени, т.к. "проиндексировав" сравнение по свойству 1 и применив свойства 2 и 3, мы получаем сравнения первой степени относительно $ind_g x$. Для наглядности можно вводить новую неизвестную $y = ind_g x$.

Применим этот способ для решения так называемых *двучленных сравнений* вида

$$ax^n \equiv b \pmod{p}.$$

**Алгоритм решения двучленных сравнений.**

1) Индексируем обе части сравнения:

$$ax^n \equiv b \pmod{p} \Leftrightarrow ind_g\left(ax^n\right) \equiv ind_g b \pmod{(p-1)} \Leftrightarrow$$

$$\Leftrightarrow ind_g a + n \cdot ind_g x \equiv ind_g b \pmod{(p-1)} \Leftrightarrow$$

$$\Leftrightarrow n \cdot ind_g x \equiv ind_g b - ind_g a \pmod{(p-1)}.$$

2) Делаем замену $y = ind_g x$:

$$ny \equiv \left(ind_g b - ind_g a\right) \pmod{(p-1)}.$$

3) Решаем полученное сравнение первой степени одним из способов. Решения существуют, если

$$\left(ind_g b - ind_g a\right) \vdots \text{НОД}(n,\ p-1).$$

В результате получится $k = НОД(n,\ p-1)$ решений:

$$y \equiv c_1,\ y \equiv c_2,\ \ldots,\ y \equiv c_k \pmod{(p-1)}.$$

4) Делаем обратную замену и находим $x$:

$$x \equiv g^{c_1},\ x \equiv g^{c_2},\ \ldots,\ x \equiv g^{c_k} \pmod{p}.$$

Чтобы найти представителей этих классов вычетов в приведённой системе наименьших неотрицательных вычетов, используем таблицу индексов. Предполагается, что таблица индексов по модулю $p$ с основанием $g$ уже составлена.

**Пример.** Решить сравнение $5x^6 \equiv 4 \pmod{11}$.

$$5x^6 \equiv 4 \pmod{11} \Leftrightarrow 6 \cdot ind_7 x \equiv ind_7 4 - ind_7 5 \pmod{10} \Leftrightarrow$$

$$\Leftrightarrow\ 6y \equiv 6-2=4 \pmod{10}\ \Leftrightarrow\ 3y \equiv 2 \pmod{5}.$$

Решая последнее сравнение, находим $y \equiv 4 \pmod{5}$. По свойству классов вычетов с кратными модулями

$$y \equiv 4, 4+5 \pmod{10}.$$

Делаем обратную замену:

$$ind_2 x \equiv 4, 9 \pmod{10}.$$

По таблице индексов находим, что

$$x \equiv 3, 8 \pmod{11}.$$

Таким образом, решениями оказались два класса вычетов по модулю 11.

## Занятие 14

**Теоретический материал.** Индекс числа, класса вычетов. Свойства индексов. Таблицы индексов. Применение индексов к решению сравнений.

**Основные типы задач.** Вычисление индексов, составление таблиц индексов, решение сравнений при помощи индексов.

### Задания для практических занятий

**128.** Дайте определение индекса числа или класса вычетов по модулю $m$ с основанием $g$. Что такое таблица индексов?

**129.** Составьте таблицу индексов по модулю $m$ с основанием $g$:

а) $m=7,\ \ g=3$;

б) $m=11,\ \ g=2$;

в) $m=13,\ \ g=6$;

г) $m=19,\ \ g=3$.

**130.** Пользуясь таблицей индексов, найдите:

а) $ind_3(345)$ по модулю 7;

б) $ind_2(-611)$ по модулю 11;

в) $ind_{32}(-218)$ по модулю 13;

г) $ind_{22}\left(3^{333}\right)$ по модулю 19.

**131.** Сформулируйте свойства индексов. Как могут применяться эти свойства для решения сравнений?

**132.** Пользуясь таблицей индексов, решите сравнения:

а) $5x^4 \equiv 3 (\mathrm{mod}\, 7)$; б) $3x^5 \equiv 7 (\mathrm{mod}\, 11)$;

в) $2x^5 \equiv 9 (\mathrm{mod}\, 13)$; г) $5x^3 \equiv 3 (\mathrm{mod}\, 19)$.

**133.** Пользуясь таблицей индексов, найдите остаток от деления:

а) $374^{386}$ на 7; б) $376^{386}$ на 11;

в) $372^{386}$ на 13; г) $373^{386}$ на 19.

## Дополнительные задания

**134.** Докажите, что если $g_1, g_2$ – первообразные корни по простому модулю *p,* то

$$ind_{g_1}(a) \equiv ind_{g_2}(a) \cdot ind_{g_1}(g_2) (\mathrm{mod}\, p-1).$$

**135.** Решите сравнения:

а) $x^2 \equiv 3 (\mathrm{mod}\, 13)$; б) $3x^4 \equiv 2 (\mathrm{mod}\, 13)$;

в) $2x^5 \equiv -5 (\mathrm{mod}\, 13)$; г) $12x^5 \equiv 1 (\mathrm{mod}\, 13)$.

**136.** Решите сравнения:

а) $7^x \equiv 11 (\mathrm{mod} 19)$; б) $7^x \equiv 17 (\mathrm{mod} 19)$;

в) $7x^4 \equiv 11 (\mathrm{mod} 19)$; г) $5x^7 \equiv 2 (\mathrm{mod} 19)$.

## §3. Квадратичные вычеты и невычеты

Рассмотрим сравнения второй степени по простому модулю $p$:

$$ax^2 + bx + c \equiv 0 (\mathrm{mod}\, p),\ a \not\equiv 0 (\mathrm{mod}\, p). \qquad (1)$$

Случай $p = 2$ можно считать тривиальным, т.к. сравнение можно легко решить методом перебора. В дальнейшем будем считать, что $p > 2$.

**Предложение 1.** *Сравнение (1) можно свести к решению сравнения вида*

$$x^2 \equiv a (\mathrm{mod}\, p). \qquad (2)$$

**Предложение 2.** *Сравнение (2) либо не имеет решений, либо имеет два решения.*

**Замечание.** Если $x^2 \equiv a (\mathrm{mod}\, p)$ и $a \equiv b (\mathrm{mod}\, p)$, то $x^2 \equiv b (\mathrm{mod}\, p)$. Поэтому, решая сравнение (2), можно рассматривать в качестве коэффициентов не отдельные числа $a$, а классы их содержащие целиком.

**Определение.** Класс вычетов по модулю $p$ называется *квадратичным вычетом* (*квадратичным невычетом*), если для чисел $a$ из этого класса сравнение $x^2 \equiv a (\mathrm{mod}\, p)$ имеет ровно два решения (соответственно, не имеет решений). Элементы этих классов также называются соответственно квадратичными вычетами или квадратичными невычетами.

**Теорема** (признак квадратичного вычета). *Число* $a$ *является квадратичным вычетом по простому модулю* $p$ $\left(p>2,\ a\not\vdots p\right)$ *тогда и только тогда, когда*

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

**Теорема** (признак квадратичного невычета). *Число* $a$ *является квадратичным невычетом по простому модулю* $p$ $\left(p>2,\ a\not\vdots p\right)$ *тогда и только тогда, когда*

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

**Теорема** (о количестве вычетов). *Количество вычетов по простому модулю* $p>2$ *равно количеству невычетов по этому же модулю и равно* $\frac{p-1}{2}$.

**Определение.** *Символом Лежандра* называется выражение $\left(\frac{a}{p}\right)$, значение которого определяется следующим образом:

$\left(\frac{a}{p}\right) = +1$, если $a$ – квадратичный вычет по модулю $p$;

$\left(\frac{a}{p}\right) = -1$, если $a$ – квадратичный невычет по модулю $p$.

Использование символа Лежандра упрощает запись некоторых свойств, связанных с существованием решений у квадратичного сравнения.

**Пример.** $\left(\frac{2}{3}\right) = -1$, т.к. сравнение $x^2 \equiv 2 (\mathrm{mod}\, 3)$ не имеет решений.

$\left(\frac{4}{5}\right)=1$, т.к. сравнение $x^2 \equiv 4 \pmod 5$ имеет два решения $[\pm 2]_5$.

**Свойства** (символа Лежандра).

*1) Если* $a \equiv b \pmod p$, *то* $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$.

*2)* $\left(\frac{a^2}{p}\right)=1$.

*3) (критерий Эйлера)* $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$.

*4)* $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=\begin{cases}+1, & при \quad p \equiv 1 \pmod 4,\\ -1, & при \quad p \equiv 3 \pmod 4.\end{cases}$

*5)* $\left(\frac{a_1 a_2 \cdot \ldots \cdot a_n}{p}\right)=\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\ldots\left(\frac{a_n}{p}\right)$.

*6)* $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}+1, & при \quad p \equiv 1 \pmod 8, \quad p \equiv 7 \pmod 8,\\ -1, & при \quad p \equiv 3 \pmod 8, \quad p \equiv 5 \pmod 8.\end{cases}$

*7)* (закон взаимности)

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}, \quad \left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right).$$

После этого можно предложить способ вычисления символа Лежандра для любых $a$ и $p$ ($a \nmid p$, $p>2$ – простое), т.е. способ определения, имеет ли решения сравнение $x^2 \equiv a \pmod p$.

**Алгоритм проверки разрешимости квадратичного сравнения** $x^2 \equiv a \pmod p$**.**

1) Вычисляя символ Лежандра $\left(\frac{a}{p}\right)$, можно считать, что $0 < a < p$, т.к. в противном случае, пользуясь свойством 1, можно заменить $a$ на его остаток от деления на $p$.

2) Если $a = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_s^{\beta_s}$, то можно воспользоваться свойством 5:

$$\left(\frac{a}{p}\right) = \left(\frac{q_1}{p}\right)^{\beta_1} \cdot \left(\frac{q_2}{p}\right)^{\beta_2} \cdot \ldots \cdot \left(\frac{q_s}{p}\right)^{\beta_s},$$

Причём, пользуясь тем, что каждое из чисел $\left(\frac{q_i}{p}\right)$ равно $+1$ или $-1$, можно из произведения выбросить сомножители с чётными степенями, а нечётные показатели степеней заменить на 1.

3) Значение $\left(\frac{2}{p}\right)$ вычисляется по свойству 6.

4) Величину $\left(\frac{q}{p}\right)$, $q > p$, $q$, $p$ – простые числа, пользуясь свойством 7, заменяем на $\left(\frac{p}{q}\right)$ (возможно со знаком минус).

В результате применения этого алгоритма числа в числителях символа Лежандра будут уменьшаться до тех пор, пока мы не дойдём до $\left(\frac{1}{p'}\right) = 1$.

**Пример.** Не решая сравнение $x^2 \equiv 20 \pmod{23}$, выяснить, имеет ли оно решения.

$$\left(\frac{20}{23}\right) \overset{5)}{=} \left(\frac{2}{23}\right)^2 \cdot \left(\frac{5}{23}\right) = \left(\frac{5}{23}\right) \overset{7)}{=} (-1)^{\frac{5-1}{2}\cdot\frac{23-1}{2}} \left(\frac{23}{5}\right) = +\left(\frac{23}{5}\right) \overset{1)}{=}$$

$$= \left(\frac{3}{5}\right) \overset{7)}{=} (-1)^{\frac{3-1}{2}\cdot\frac{5-1}{2}} \left(\frac{5}{3}\right) = + \left(\frac{5}{3}\right) \overset{1)}{=} \left(\frac{2}{3}\right) \overset{6)}{=} (-1)^{\frac{3^2-1}{8}} = -1.$$

Сравнение решений не имеет.

## Занятие 15

**Теоретический материал.** Квадратичные вычеты и невычеты. Признаки квадратичного вычета и квадратичного невычета. Символ Лежандра, его свойства. Алгоритм проверки разрешимости сравнения второй степени.

**Основные типы задач.** Вычисление символа Лежандра.

### Задания для практических занятий

**137.** Дайте определение квадратичного вычета и квадратичного невычета по простому модулю. Сформулируйте признаки квадратичного вычета и невычета.

**138.** Проверьте являются ли квадратичным вычетами:

а) по модулю 7 числа 2, 3, 4, 5;

б) по модулю 11 числа 6, 7, 8, 9;

в) по модулю 13 числа 3, 5, 7, 9.

**139.** Дайте определение символа Лежандра. Сформулируйте свойства символа Лежандра.

**140.** Используя свойства символа Лежандра, определите, имеют ли решения сравнения:

а) $x^2 \equiv 7 \pmod{19}$; б) $x^2 \equiv 18 \pmod{23}$;

в) $x^2 \equiv 5 \pmod{29}$; г) $x^2 \equiv 10 \pmod{31}$.

## Дополнительные задания

**141.** Используя свойства символа Лежандра, определите, имеют ли решения сравнения:

а) $x^2 \equiv 8 \pmod{19}$; б) $x^2 \equiv 19 \pmod{23}$;

в) $x^2 \equiv 6 \pmod{29}$; г) $x^2 \equiv 11 \pmod{31}$.

## Контрольная работа №4

*Примерный вариант*

1. Вычислите порядок числа $a = 21$ по модулю $m = 17$.

2. Пользуясь таблицей индексов, решите сравнение

$$9x^7 \equiv 7 \pmod{13}.$$

3. Используя свойства символа Лежандра, определите, имеет ли решения сравнение $x^2 \equiv 17 \pmod{23}$.

# *ТЕМА 5.* АРИФМЕТИЧЕСКИЕ ПРИЛОЖЕНИЯ

## §1. Позиционные системы счисления

Целые и дробные числа постоянно используются. Для того чтобы устно передавать друг другу численную информацию, в языке должна существовать система числительных. Для того чтобы письменно передавать численную информацию, должна быть разработана система записи чисел. Для того чтобы выполнять действия над числами, должны быть разработаны алгоритмы, позволяющие по записи чисел определять результат действия. Всё это входит в *систему счисления*.

Ниже будет рассмотрена $g$*-ичная позиционная система счисления*. В нашей практике используются системы с основанием $g = 10, 2, 8, 16$.

**ОПРЕДЕЛЕНИЕ.** Пусть $g$ – целое число, большее единицы, которое в дальнейшем будет называться *основанием системы счисления*. $g$*-ичным представлением* натурального числа $n$ называется представление вида

$$n = a_k g^k + a_{k-1} g^{k-1} + \ldots + a_1 g + a_0 ,$$

где $a_i$ – целые числа, удовлетворяющие неравенству $0 \le a_i < g$ и $a_k \ne 0$.

**ТЕОРЕМА** (о $g$-ичном представлении натуральных чисел). *Всякое натуральное число $n$ имеет единственное $g$-ичное представление.*

Доказательство теоремы о $g$-ичном представлении даёт один из

**Алгоритмов получения $g$-ичного представления.** *Делим число $n$ на $g$ с остатком, затем частное делим на $g$ и т.д. делим на $g$ каждое последующее частное до тех пор, пока частное не получится равным 0. Остатки от деления, взятые в обратном порядке, дают коэффициенты (цифры) искомого $g$-ичного представления.*

Действительно, если

$$n = g \cdot h_0 + a_0,\ 0 \le a_0 < g,$$

$$h_0 = g \cdot h_1 + a_1,\ 0 \le a_1 < g,$$

$$h_1 = g \cdot h_2 + a_2,\ 0 \le a_2 < g,$$

$$h_2 = g \cdot h_3 + a_3,\ 0 \le a_3 < g,$$

$$\cdots\cdots$$

$$h_{k-1} = g \cdot h_k + a_k,\ 0 \le a_k < g,\ h_k = 0,$$

то, последовательно подставляя выражение для $h_i$ в первое равенство, получим требуемое представление:

$$n = gh_0 + a_0 = g\left(gh_1 + a_1\right) + a_0 = g^2 h_1 + \underline{ga_1 + a_0} =$$

$$= g^2\left(gh_2 + a_2\right) + ga_1 + a_0 = g^3 h_2 + \underline{g^2 a_2 + ga_1 + a_0} = \ldots$$

$$\ldots = g^k a_k + g^{k-1} a_{k-1} + \ldots + ga_1 + a_0 =$$

$$= a_k g^k + a_{k-1} g^{k-1} + \ldots + a_1 g + a_0,$$

причём $0 \le a_i < g$.

Эта теорема лежит в основе *..$g$-ичной позиционной системы счисления,* которая включает в себя следующие составные части

1) *Цифры,* т.е. некоторые символы для записи чисел от 0 до $(g-1)$.

Так как в $g$-ичном представлении коэффициенты $a_i$ удовлетворяют условию $0 \le a_i < g$, то каждый из них может быть записан одной цифрой. Будем считать, то $\overline{a_i}$ – это запись коэффициента $a_i$ цифрой.

2) $g$-ичная позиционная форма записи.

Всякое представление $n = a_k g^k + a_{k-1} g^{k-1} + \ldots + a_1 g + a_0$ можно сокращённо записывать в виде

$$n = \overline{a_k a_{k-1} \ldots a_1 a_0} .$$

Или, чтобы подчеркнуть величину $g$, пишут так:

$$n = \left(\overline{a_k a_{k-1} \ldots a_1 a_0}\right)_g .$$

$g$-ичное представление по такой записи однозначно восстанавливается. Форма записи называется *позиционной,* т.к. "вес" каждой цифры определяется её положением (позицией) в записи: *$s$-тая, считая с конца, цифра записи $\overline{a_{s-1}}$ входит в $g$-ичное представление в составе слагаемого $a_{s-1} g^{s-1}$*.

3) *Алгоритмы*, позволяющие по $g$-ичным записям чисел находить ($g$-ичную запись) их суммы, разности, произведения, частные и остатки, т.е. результаты арифметических действий.

Такие алгоритмы хорошо нам известны по 10-тичной системе счисления. Для системы счисления с другим основанием они аналогичны. В качестве примера разберём 8-ричную систему счисления.

Цифры (и их названия) удобно взять те же, что и в 10-тичной системе:

$$0, 1, 2, 3, 4, 5, 6, 7 .$$

**Пример.** Найти 8-ричную запись числа 1000000.

```
1000000 | 8
   8    |------
------  | 125000
  20
  16
  40
  40
------
   0

125000 | 8
   8   |------
-------| 15625
  45
  40
  50
  48
  20
  16
  40
  40
------
   0

15625 | 8
   8  |------
------| 1953
  76
  72
  42
  40
  25
  24
------
   1
```

```
1953 | 8
 16  |------
-----| 244
  35
  32
  33
  32
------
   1

244 | 8
 24 |------
----| 30
   4
   0
------
   4

30 | 8
24 |------
---| 3
 6
 0
---
 6

3 | 8
0 |------
--| 0
 3
```

В результате $1000000 = (3641100)_8$.

Полученное равенство можно проверить.

$$(3641100)_8 = 3 \cdot 8^6 + 6 \cdot 8^5 + 4 \cdot 8^4 + 1 \cdot 8^3 + 1 \cdot 8^2 + 0 \cdot 8^1 + 0 =$$

$$= 3 \cdot 262144 + 6 \cdot 32768 + 4 \cdot 4096 + 1 \cdot 512 + 1 \cdot 64 + 0 \cdot 8 + 0 =$$

$$= 786432 + 196608 + 16384 + 512 + 64 = 1000000.$$

Для арифметических вычислений в 8-ричной системе имеет смысл составить *таблицу сложения* и *таблицу умножения*, т.е. таблицы, в которых даны соответственно

результаты сложения и умножения однозначных (т.е. записанных одной цифрой) чисел. 8-ричную запись чисел в ячейках таблицы находим при помощи алгоритма, продемонстрированного в предыдущем примере.

**Таблица сложения**

| + | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** |
|---|---|---|---|---|---|---|---|---|
| **0** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **1** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 10 |
| **2** | 2 | 3 | 4 | 5 | 6 | 7 | 10 | 11 |
| **3** | 3 | 4 | 5 | 6 | 7 | 10 | 11 | 12 |
| **4** | 4 | 5 | 6 | 7 | 10 | 11 | 12 | 13 |
| **5** | 5 | 6 | 7 | 10 | 11 | 12 | 13 | 14 |
| **6** | 6 | 7 | 10 | 11 | 12 | 13 | 14 | 15 |
| **7** | 7 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

**Таблица умножения**

| x | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** |
|---|---|---|---|---|---|---|---|---|
| **0** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **1** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **2** | 0 | 2 | 4 | 6 | 10 | 12 | 14 | 16 |
| **3** | 0 | 3 | 6 | 11 | 14 | 17 | 22 | 25 |
| **4** | 0 | 4 | 10 | 14 | 20 | 24 | 30 | 34 |
| **5** | 0 | 5 | 12 | 17 | 24 | 31 | 36 | 43 |
| **6** | 0 | 6 | 14 | 22 | 30 | 36 | 44 | 52 |
| **7** | 0 | 7 | 16 | 25 | 34 | 43 | 52 | 61 |

**Пример.** Сложить в восьмеричной системе $(567136)_8$ и $(75637)_8$.

Как и в алгоритме сложения для 10-ичной системы, цифры складываются поразрядно. Если при сложении получается двузначное число, то его первая цифра идёт "в ум", т.е. переходит в следующий разряд. Ниже выполнено

сложение "столбиком" данных чисел. Справа даны пояснения для каждого шага.

$$\begin{array}{r} 5\,6\,7\,1\,3\,6 \\ +\quad 7\,5\,6\,3\,7 \\ \hline 6\,6\,4\,7\,7\,5 \end{array}$$

$6+7=15_8$; 5 пишем, 1 "в уме";

$3+3+1$ "в уме" $=7$;

$1+6=7$;

$7+5=14_8$; 4 пишем, 1 "в уме";

$6+7+1$ "в уме" $=16_8$; 6 пишем, 1 "в уме";

$5+1$ "в уме" $=6$.

При сложении цифр использовалась таблица сложения.

Пример. Вычислить в восьмеричной системе разность

$$(567136)_8-(75637)_8.$$

При вычитании, если из большей цифры нужно вычесть меньшую, занимают единицу в следующем разряде.

$$\begin{array}{r} 5\,6\,7\,1\,3\,6 \\ -\quad 7\,5\,6\,3\,7 \\ \hline 4\,7\,1\,2\,7\,7 \end{array}$$

$16-7=7$;

$12-3=7$;

$10-6=2$;

$6-5=1$;

$16-7=7$;

$5-1=4$.

Вычитание цифр можно выполнять также при помощи таблицы сложения. Например, согласно таблице, 16 получается как $7+7$. В результате:

$$16=7+7 \Rightarrow 16-7=7.$$

Иногда случается, что занимать в следующем разряде нечего, тогда нужно занимать единицу в следующих двух, трёх и т.д. разрядах. Для того чтобы выполнять это быстро,

имеет смысл проделать следующие предварительные вычисления.

$10-1=07,\ 20-1=17,\ 30-1=27,\ \ldots;$

$100-1=077,\ 200-1=177,\ 300-1=277,\ \ldots;$

$1000-1=0777,\ 2000-1=1777,\ 3000-1=2777,\ \ldots.$

И так далее.

**Пример.** Вычислить в восьмеричной системе

$$(1002000304)_8-(123456717)_8.$$

```
  077  1777  27
 1002000304
-  123456717
 ------------
  656321365
```

Занимаем: $30-1=27$;

$14-7=5$;

$7-1=6$;

Занимаем: $2000-1=1777$;

$12-7=3$;

$7-6=1;\ 7-5=2;\ 7-4=3$;

Занимаем: $100-1=077$;

$11-3=6;\ 7-2=5;\ 7-1=6$.

При умножении столбиком нужно пользоваться таблицей умножения.

**Пример.** Умножить в восьмеричной системе $(567)_8$ на $(643)_8$.

```
   567
 x 643
 -----
  2145
+ 2734
  4312
 -----
 462705
```

$7\cdot3=25$; 5 пишем, 2 "в уме";

$6\cdot3+2$ "в уме" $=22+2=24$;

4 пишем, 2 "в уме";

$5 \cdot 3 + 2$ "в уме" $= 17 + 2 = 21$;

21 пишем;

$7 \cdot 4 = 34$; 4 пишем, 3 "в уме";

$6 \cdot 4 + 3$ "в уме" $= 33$; 3 пишем, 3 "в уме";

$5 \cdot 4 + 3$ "в уме" $= 27$; 27 пишем.... .

Далее действуем аналогично. Полученные три числа складываем.

В алгоритме деления, чтобы подобрать наибольшую цифру, произведение которой на делитель меньше или равно соответствующей части делимого, необходимо выполнять умножение. Алгоритм сравнения чисел в 8-ричной системе аналогичен алгоритму сравнения в 10-ичной системе.

**Пример.** Разделить в $(341567)_8$ на $(25)_8$.

| 341567 | 25 |
|---|---|
| 25 | 12577 |
| 71 | |
| 52 | |
| 175 | |
| 151 | |
| 246 | |
| 223 | |
| 237 | |
| 223 | |
| 14 | |

Первая цифра частного равна 1, т.к.

$25 \cdot 1 = 25 < 34,\ 25 \cdot 2 = 52 > 34$.

Вторая цифра равна 2, т.к.

$25 \cdot 2 = 52 < 71,\ 25 \cdot 3 = 77 > 71$.

Третья цифра равна 5, т.к.

$25 \cdot 5 = 151 < 175,\ 25 \cdot 6 = 176 > 175$.

Четвёртая цифра равна 7, т.к.

$25 \cdot 7 = 223 < 246$.

Пятая цифра равна 7.

**Ответ:** $(341567)_8 = (25)_8 \cdot (12577)_8 + (14)_8$; частное равно $(12577)_8$, остаток равен $(14)_8$.

При изучении делимости чисел, которые записаны в $g$-ичной системе счисления, полезно использовать *признаки делимости*. Целый список признаков делимости можно получить на основе следующей

**Теоремы.** *Пусть дано число* $m > 1$ *и для каждой степени* $g$ *известны такие числа* $b_i$, *что* $g^i \equiv b_i \pmod{m}$. *Пусть дано* $g$*-ичное представление числа* $n$*:*

$$n = a_k g^k + a_{k-1} g^{k-1} + \ldots + a_1 g + a_0 .$$

*Тогда* $n \equiv a_k b_k + a_{k-1} b_{k-1} + \ldots + a_1 b_1 + a_0 b_0 \pmod{m}$.

**Следствие** (обобщённый признак делимости Паскаля). *Число* $n$ *делится на* $m$ *тогда и только тогда, когда число* $(a_k b_k + a_{k-1} b_{k-1} + \ldots + a_1 b_1 + a_0 b_0)$ *делится на* $m$.

Сформулируем для примера несколько признаков делимости.

**Признак делимости на 3, 9 в десятичной системе счисления.** *Натуральное число сравнимо с суммой своих цифр по модулю 3, 9. Оно делится на 3, 9 тогда и только тогда, когда делится соответственно на 3, 9 сумма его цифр.*

Аналогично можно получить известные признаки делимости в десятичной системе на 2, 4, 5, 7, 8, 10, 11 и т.д.

Согласно свойству делимости, если числа $m_1$ и $m_2$ взаимно просты, то

$$a \vdots m_1 m_2 \;\Leftrightarrow\; a \vdots m_1,\ a \vdots m_2 .$$

На основе этого можно получить признаки делимости на 6, 12, 14, 15 и т.д.

**Обобщённый рекуррентный признак делимости на** $m = 7, 11, 13, 1001$. Для любых целых чисел $a, b$

$$1000a + b \equiv r \pmod{m} \;\Leftrightarrow\; a - b \equiv -r \pmod{m}.$$

При помощи признаков делимости и свойств сравнений можно проверять правильность выполнения арифметических действий. Проверка основывается на следующем

**Свойстве.** *Для любых целых чисел* $a, b$

$$a = b \;\Leftrightarrow\; (\forall m > 1)\big(a \equiv b \pmod{m}\big).$$

Ясно, что проверить сравнимость данных чисел по всем модулям $m > 1$ невозможно. Однако, проверка по нескольким различным (взаимно простым) модулям существенно сокращает вероятность ошибки.

**Пример.** Проверить правильность выполнения действия:

$$562 \cdot 56 = 32372.$$

Обозначим левую часть равенства буквой $A$, а правую – буквой $B$. Воспользуемся признаком делимости на 9.

$$562 \equiv 5 + 6 + 2 = 13 \equiv 1 + 3 = 4 \pmod{9};$$

$$56 \equiv 5 + 6 = 11 \equiv 2 \pmod{9};$$

$$32372 \equiv 3 + 2 + 3 + 7 + 2 = 17 \equiv 8 \pmod{9}.$$

В результате получается, что

$$A \equiv 4 \cdot 2 = 8 \equiv B \pmod{9}.$$

С точки зрения делимости на 9 всё сходится.

Проверим равенство с точки зрения делимости на 11.

$$562 \equiv 5 - 6 + 2 = 1 \pmod{11};$$

$$56 \equiv -5 + 6 = 1 \pmod{11};$$

$$32372 \equiv 3 - 2 + 3 - 7 + 2 = -1 \pmod{11}.$$

В результате получается, что

$$A \equiv 1 \cdot 1 = 1 \not\equiv -1 \equiv B \pmod{11}.$$

Следовательно, $A \neq B$ и в вычислениях где-то допущена ошибка (легко определить, что полученный ответ на 900 больше правильного).

## Занятие 16

**Теоретический материал.** Позиционные системы счисления. Теорема о g-ичном представлении чисел. Алгоритм получения g-ичного представления. Вычисления в g-ичной системе счисления. Признаки делимости. Признак делимости Паскаля.

**Основные типы задач.** Вычисление g-ичного представления целого числа для различных g, выполнение арифметических операций в g-ичной системе счисления.

### Задания для практических занятий

**142.** Дайте определение g-ичной позиционной системы записи. Сформулируйте теорему g-ичном представлении чисел, алгоритм получения g-ичной записи.

**143.** Найдите 2-ичное представление чисел:

а) 1000; б) 1783.

**144.** Найдите 8-ричное представление чисел:

а) 2009; б) 11111;

в) 465378; г) 8276151.

**145.** Составьте таблицы сложения и умножения для:

а) 2-ичной системы счисления;

б) 8-ричной системы счисления;

в) 16-ричной системы счисления.

**146.** Вычислите, используя таблицы сложения:

а) $(1001011010)_2 + (101100011)_2$;

б) $(567356)_8 + (62425)_8$;

в) $(51674346)_8 + (46031424)_8$;

г) $(5A73F6)_{16} + (B24D25)_{16}$;

д) $(ABCD754)_{16} + (756FFDA)_{16}$.

**147.** Сформулируйте алгоритм вычитания. Для выполнения процедуры «заёма в старшем разряде» докажите, что

а) $\left(1\underbrace{00...0}_{n}\right)_2 - 1 = \left(\underbrace{11...1}_{n}\right)_2$;

б) $\left(1\underbrace{00...0}_{n}\right)_8 - 1 = \left(\underbrace{77...7}_{n}\right)_8$;

в) $\left(1\underbrace{00...0}_{n}\right)_{16} - 1 = \left(\underbrace{FF...F}_{n}\right)_{16}$.

**148.** Вычислите, используя таблицы сложения:

а) $(1001011010)_2 - (101100011)_2$;

б) $(511356)_8 - (162475)_8$;

в) $(110001032)_8 - (33162475)_8$;

г) $(15A72F1)_{16} - (AB2D25)_{16}$;

д) $(1001700306)_{16} - (AB4DA2FC5)_{16}$.

**149.** Сформулируйте алгоритм умножения в g-ичной системе счисления.

**150.** Вычислите, используя таблицы сложения и умножения:

а) $(1011)_2 \cdot (1011)_2$;

б) $(453)_8 \cdot (64)_8$;

в) $(2164)_8 \cdot (357)_8$;

г) $(A1C)_{16} \cdot (9E)_{16}$;

д) $(4B2D)_{16} \cdot (A7)_{16}$.

**151.** Сформулируйте алгоритм деления в g-ичной системе счисления. Для подбора подходящей цифры, докажите правило сравнения чисел в g-ичной системе.

**152.** Вычислите частное и остаток от деления $n$ на $m$:

а) $n = (10010110)_2$, $m = (1011)_2$;

б) $n = (234164)_8$, $m = (57)_8$;

в) $n = (7354226)_8$, $m = (325)_8$;

г) $n = (234164)_{16}$, $m = (57)_{16}$;

д) $n = (A26BC97)_{16}$, $m = (AA)_{16}$.

**153.** Сформулируйте обобщённый признак делимости Паскаля. Как применять этот признак для нахождения остатков от деления?

**154.** Докажите признаки делимости на 3, 9, 11, 2, 4, $2^n$, 5, 25, $5^n$ в десятичной системе счисления.

**155.** Проверьте правильность выполнения арифметических действий:

а) $71187 + 83762 = 158549$; б) $9642 \cdot 5735 = 55395870$;

в) $8376245 - 7400862 = 965383$;

г) $\sqrt[4]{456876} = 26$; д) $3912862 : 29193 = 134$.

## Дополнительные задания

**156.** Найдите 16-ричное представление чисел:

а) 2009; б) 11111;

в) 465378; г) 8276151.

**157.** Вычислите, используя таблицы сложения:

а) $(512737)_8 + (265474)_8$;

б) $(4166246)_8 + (4375107)_8$;

в) $(4A902D1)_{16} + (CB8E79)_{16}$;

г) $(ABCDABC)_{16} + (F1F2D3A)_{16}$.

**158.** Вычислите, используя таблицы сложения:

а) $(622467)_8 - (314137)_8$;

б) $(100101052)_8 - (44273506)_8$;

в) $(23A32D1)_{16} - (BAB2DF9)_{16}$;

г) $(102170105)_{16} - (B4DA88C5)_{16}$.

**159.** Вычислите, используя таблицы сложения и умножения:

а) $(725)_8 \cdot (43)_8$; б) $(5442)_8 \cdot (573)_8$;

в) $(91C)_{16} \cdot (FE)_{16}$; г) $(4123)_{16} \cdot (97)_{16}$.

**160.** Вычислите частное и остаток от деления $n$ на $m$:

а) $n = (321446)_8$, $m = (75)_8$;

б) $n = (3752462)_8$, $m = (253)_8$;

в) $n = (321446)_{16}$, $m = (75)_{16}$;

г) $n = (6A2B7C9)_{16}$, $m = (A1)_{16}$.

**161.** Найти десятичное представление числа:

а) $(1001110101001010)_2$; б) $(2763541)_8$;

в) $(76255435)_8$; г) $(A41FD2)_{16}$.

**162.** Первая цифра некоторого четырёхзначного числа равна 7. Если эту цифру переставить на последнее место, то число уменьшается на 414. Найдите это число.

**163.** Если некоторое число разделить на сумму его цифр, то в частном получится 6, а в остатке 3. Если же из него вычесть утроенную сумму его цифр, то получится 39. Найдите это число.

**164.** Если между цифрами некоторого двузначного числа записать это же двузначное число, то полученное четырёхзначное число будет больше первоначального в 99 раз. Найдите это число.

**165.** Найдите все числа вида:

а) $\overline{x43y}$, делящиеся на 45;

б) $\overline{13xy43z}$, делящиеся на 792;

в) $\overline{7x36y5}$, делящиеся на 1375;

г) $\overline{4x87y6}$, делящиеся на 56.

## §2. g-ичное представление дробных чисел

**Определение.** *g-ичным представлением* дробного числа $\frac{n}{m}$ называется представление вида

$$\frac{n}{m} = a_k g^k + a_{k-1} g^{k-1} + \ldots + a_1 g + a_0 + \frac{b_1}{g} + \frac{b_2}{g^2} + \frac{b_3}{g^3} + \ldots ,$$

где все коэффициенты $a_i, b_j$ – целые числа в пределах от 0 до $(g-1)$. Слагаемых может быть как конечное, так и бесконечное количество. Во втором случае сумма в правой части – это сумма ряда.

$g$-ичная запись будет выглядеть так:

$$\frac{n}{m} = \overline{a_k a_{k-1} \ldots a_1 a_0},\ \overline{b_1 b_2 b_3} \ldots .$$

Выражение в правой части равенства будет называться *g-ичной дробью*. Запятая в записи отделяет целую часть от дробной.

Если последовательность цифр в правой части начинает повторяться с некоторым периодом, то говорят, что $g$-ичная дробь является *периодической*. Запись вида

$$\overline{a_k a_{k-1} \ldots a_1 a_0},\ \overline{b_1 b_2 b_3 \ldots b_s}\ \left(\overline{c_1 c_2 \ldots c_t}\right)$$

расшифровывается как сокращение записи

$$\overline{a_k a_{k-1} \ldots a_1 a_0},\ \overline{b_1 b_2 \ldots b_s}\ \overline{c_1 c_2 \ldots c_t}\ \overline{c_1 c_2 \ldots c_t} \ldots ,$$

в которой, начиная с $(s+1)$-ой цифры, цифры дробной части повторяются с периодом $t$.

$\overline{b_1 b_2 \ldots b_s}$ – это *непериодическая часть* или *предпериод* дроби, а число $s$ длина предпериода. $\left(\overline{c_1 c_2 \ldots c_t}\right)$ – это *периодическая часть* или *период* дроби, а $t$ – его длина.

Дробь называется *чисто периодической*, если $s = 0$, т.е. непериодической части нет.

Например, $\frac{1}{3} = 0,33333\ldots = 0,(3)$, т.е. число $\frac{1}{3}$ представлено в виде чисто периодической десятичной дроби с длиной периода 1.

Каждое рациональное число имеет $g$-ичное представление. Основным является случай, когда дробь несократима и её знаменатель взаимно прост с основанием системы счисления $g$.

**Теорема.** *Всякая несократимая дробь* $\frac{n}{m}$, *знаменатель которой взаимно прост с* $g$, *представима в виде чисто периодической* $g$*-ичной дроби:*

$$\frac{n}{m} = A + 0,\ \left(c_1 c_2 \ldots c_t\right),$$

*где* $A$ *– целая часть, а длина периода* $t = O_m(g)$.

**Алгоритм получения g-ичной дроби** аналогичен алгоритму деления $n$ на $m$. Как только цифры числа $n$ закончатся, мы начинаем, умножая каждый остаток на $m$, получать цифры после запятой.

Рассмотрим общий случай.

Для простоты будем считать, что $g = 10$. Рассмотрим несократимую дробь $\frac{n}{m}$, и пусть числа 10 и $m$ не являются взаимно простыми. Число $g = 10$ имеет два простых делителя

– 2 и 5, поэтому $m = 2^{\alpha} \cdot 5^{\beta} \cdot m_1$, где число $m_1$ взаимно просто с $g = 10$.

Пусть $\gamma = \max(\alpha, \beta)$, тогда можно сделать следующее преобразование:

$$\frac{n}{m} = \frac{n}{2^{\alpha} \cdot 5^{\beta} \cdot m_1} = \frac{1}{10^{\gamma}} \left( \frac{2^{\gamma-\alpha} \cdot 5^{\gamma-\beta} \cdot n}{m_1} \right).$$

Первый случай: $m_1 = 1$. Число в скобках является целым. Пусть его 10-тичное представление имеет вид $\overline{a_k a_{k-1} \ldots a_1 a_0}$, тогда

$$\frac{n}{m} = \frac{1}{10^{\gamma}} \left( \overline{a_k a_{k-1} \ldots a_1 a_0} \right) = \overline{a_k a_{k-1} \ldots a_{\gamma}}, \ \overline{a_{\gamma-1} \ldots a_1 a_0}.$$

Это случай, когда получается конечная десятичная дробь.

Второй случай: $m_1 \neq 1$. Применяя к числу в скобках алгоритм из теоремы, получаем:

$$\frac{2^{\gamma-\alpha} \cdot 5^{\gamma-\beta} \cdot n}{m_1} = \overline{a_k a_{k-1} \ldots a_1 a_0} + 0, \ \left( \overline{c_1 c_2 \ldots c_t} \right), \ t = O_{m_1}(10).$$

Отсюда

$$\frac{n}{m} = \overline{a_k a_{k-1} \ldots a_{\gamma}}, \ \overline{a_{\gamma-1} \ldots a_1 a_0} \ \left( \overline{c_1 c_2 \ldots c_t} \right).$$

В этом случае получилась периодическая дробь, длина предпериода которой равна $\gamma = \max(\alpha, \beta)$, а длина периода равна $t = O_{m_1}(10)$.

В случае другого основания $g$ все выкладки сохраняются, только вместо 2 и 5 нужно рассматривать все простые делители основания $g$.

**Пример.** Найти 10-тичное представление чисел $\frac{5}{13}, \frac{17}{8}, \frac{5}{12}$.

Алгоритм разложения в 10-ичную дробь может оказаться длинным и можно пропустить тот момент, когда остатки начнут повторяться. Поэтому сначала выясним, какой вид будет иметь десятичная дробь.

Так как $\text{НОД}(10,13)=1$, то в первом случае дробь будет чисто периодической. Вычислим длину периода. Для этого нужно вычислить $O_{13}(10)$. Так как $\varphi(13)=12$, то порядок может быть равен $1, 2, 3, 4, 6, 12$ (это натуральные делители числа 12).

```
50 | 13
39 | 0,384615...
110
104
 60
 52
  80
  78
   20
   13
    70
    65
     5      Повтор.
```

$$10^1 \equiv -3 \pmod{13},$$

$$10^2 \equiv 9 \equiv -4 \pmod{13},$$

$$10^3 \equiv 12 \equiv -1 \pmod{13},$$

$$10^4 \equiv 16 \equiv 3 \pmod{13},$$

$$10^6 \equiv 1 \pmod{13}.$$

Длина периода равна 6. Следовательно, в алгоритме седьмое число совпадёт с первым. После этого применяем алгоритм.

**Ответ:** $\frac{5}{13} = 0,(384615)$.

Рассмотрим число $\frac{17}{8}$. Так как $8 = 2^3 = 2^3 \cdot 5^0$, то

```
1   50 | 12
    48 | 0,4166...
2    20
     12
3    80
     72
     8      Повтор.
```

дробь будет конечной, причём длина дробной части будет равна $\max(3,0)=3$.

$$\frac{17}{8}=\frac{17\cdot 5^3}{2^3\cdot 5^3}=\frac{17\cdot 5^3}{10^3}=$$

$$=\frac{2125}{1000}=2{,}125.$$

Рассмотрим число $\frac{5}{12}$. Так как $12=2^2\cdot 5^0\cdot 3$ и $O_3(10)=1$, то должна получиться бесконечная периодическая дробь, длина непериодической части которой равна $\max(2,0)=2$, а длина периода равна 1. В алгоритме числа начнут повторяться начиная с третьего.

| | | | |
|---|---|---|---|
| 1 | 30 | 12 | |
| | 24 | 0,2(3146)... | |
| 2 | 40 | | |
| | 36 | | |
| 3 | 20 | | |
| | 12 | | |
| 4 | 60 | | |
| | 50 | | |
| 5 | 100 | | |
| | 74 | | |
| 6 | 40 | Повтор. | |

**Ответ:** $\frac{5}{12}=0{,}41(6)$.

**Пример.** Найти 8-ричное представление числа $\frac{3}{10}$.

Так как $10=2^1\cdot 5$ и $\text{НОД}(8,5)=1$, то должна получиться бесконечная 8-ричная дробь с непериодической частью длины 1. Так как $8^1\equiv 3(\mathrm{mod}\,5)$, $8^2\equiv 9\equiv -1(\mathrm{mod}\,5)$, $8^4\equiv 1(\mathrm{mod}\,5)$, то $O_5(8)=4$ и длина периода будет равна 4. Запишем числитель и знаменатель в 8-ричной системе, все вычисления будем делать также в 8-

ричной системе. Умножение на $g=8$ в 8-ричной системе сводится к дописыванию нуля.

$$10=8+2=(12)_8 .$$

**Ответ:** $\left(\frac{3}{12}\right)_8 = 0,2(3146)_8 .$

Таким образом, всякое рациональное число имеет $g$-ичное представление. Кроме того, *$g$-ичное представление всякого рационального числа единственно.*

Разберём обратную задачу: как данную бесконечную периодическую дробь преобразовать в обыкновенную? .

Это делается следующим образом. Пусть

$$A=\overline{a_k a_{k-1}\dots a_0},\ \overline{b_1\dots b_s}\ \left(\overline{c_1 c_2\dots c_t}\right)_g .$$

Рассмотрим числа $A\cdot g^s$, $A\cdot g^{s+t}$:

$$A\cdot g^s=\overline{a_k a_{k-1}\dots a_0}\ \ \overline{b_1\dots b_s},\ \left(\overline{c_1 c_2\dots c_t}\right)_g ,$$

$$A\cdot g^{s+t}=\overline{a_k a_{k-1}\dots a_0}\ \ \overline{b_1\dots b_s}\ \ \overline{c_1 c_2\dots c_t},\ \left(\overline{c_1 c_2\dots c_t}\right)_g .$$

Если из второго вычесть первое, то дробные части сократятся и можно выразить $A$:

$$A=\frac{\overline{a_k a_{k-1}\dots a_0}\ \ \overline{b_1\dots b_s}\ \ \overline{c_1 c_2\dots c_t}-\overline{a_k a_{k-1}\dots a_0}\ \ \overline{b_1\dots b_s}}{g^{s+t}-g^s} .$$

**Пример.** Преобразовать десятичную дробь $0,41(6)$ в обыкновенную.

Применяем формулу, полученную выше.

$$0,41(6)=\frac{416-41}{10^3-10^2}=\frac{375}{900}=\frac{75}{180}=\frac{15}{36}=\frac{5}{12} .$$

## Занятие 17

**Теоретический материал.** g-ичное представление дробных чисел. Теорема о разложении дробного числа в g-ичную дробь. Длина периода g-ичной дроби. Условия получения конечных g-ичных дробей, дробей с непериодической частью. Обращение бесконечных периодических g-ичных дробей в обыкновенные.

**Основные типы задач.** Представление дробного числа в виде g-ичной дроби, представление бесконечной периодической дроби в виде обыкновенной дроби.

### Задания для практических занятий

**166.** Какие десятичные дроби могут получиться при разложении рационального числа? Как вычислить предпериод и период этих дробей? В чём состоит алгоритм разложения рационального числа в десятичную дробь?

**167.** Разложите рациональное число в десятичную дробь, предварительно определив тип дроби и вычислив её период и предпериод:

а) $\frac{7}{11}$; б) $\frac{7}{13}$;

в) $\frac{33}{125}$; г) $\frac{351}{256}$;

д) $\frac{533}{875}$; е) $\frac{137}{208}$.

**168.** Найдите все положительные правильные несократимые дроби, которые обращаются в чисто периодические дроби с периодом 1.

**169.** При каких значениях знаменателя положительная правильная несократимая дробь обращается в чисто

периодическую десятичную дробь с периодом 2 ? Сколько таких дробей?

**170.** Запишите в виде обыкновенных дробей следующие десятичные дроби:

а) $0,265$; б) $1,(26)$;

в) $12,37(739)$; г) $2,48906$;

д) $0,(344)$; е) $34,2(8573)$.

### Дополнительные задания

**171.** Разложите рациональное число в 8-ричную дробь, предварительно определив тип дроби и вычислив её период и предпериод:

а) $\frac{7}{11}$; б) $\frac{7}{13}$;

в) $\frac{33}{125}$; г) $\frac{351}{256}$.

## Контрольная работа №5

*Примерный вариант*

1. Найдите десятичное представление числа $(36275311)_8$.

2. Вычислите $(5324)_8 \cdot (435)_8$.

3. Представьте число $\frac{211}{224}$ в виде десятичной дроби, предварительно определив тип дроби и вычислив её период и предпериод.

# ЛИТЕРАТУРА

1. *Казачек, Н.А.* Алгебра и теория чисел: учебное пособ. для студ.-заочников II курса физ.-мат. факультетов пед.инст. /Н.А.Казачек, Г.Н.Перлатов, Н.Я.Виленкин, А.И.Бородин; под ред. Н.Я.Виленкина. – М.: Просвещение, 1984.

2. *Бухштаб, А.А.* Теория чисел / А.А.Бухштаб. – М.: Просвещение, 1966.

3. *Иванов, А.М.* Делимость в кольце целых чисел: учебно-дидактический комплекс/ А.М.Иванов, А.И.Кузьмичёв. – Новосибирск: Изд. НГПУ, 1996.

4. *Кочева, А.А.* Задачник-практикум по алгебре и теории чисел. Ч.III. Для студентов-заочников II курса физ.-мат. фак. пед. ин-тов/ А.А.Кочева. – М.:Просвещение, 1984.

5. *Кузьмичёв, А.И.* Теория сравнений: учебно-дидактический комплекс/ А.И.Кузьмичёв, В.И.Стрига. – Новосибирск: Изд. НГПУ, 2002.

6. *Куликов, Л.Я.* Алгебра и теория чисел/ Л.Я.Куликов. – М.: Высшая школа, 1979.

7. *Куликов, Л.Я.* Сборник задач по алгебре и теория чисел/ Л.Я.Куликов и др. – М.: Просвещение, 1993.

8. *Ляпин, Е.С.* Алгебра и теория чисел. Ч.I. Числа/ Е.С.Ляпин, А.Е. Евсеев. – М.: Просвещение, 1974.

9. *Нестеренко, Ю.В.* Теория чисел: учебник для студ. высш. учеб. заведений/ Ю.В.Нестеренко. – М.: Издательский центр «Академия», 2008.

10. Практические занятия по алгебре и теории чисел: методическая разработка для студентов математического факультета педуниверситета/ Сост. А.П.Бирюков и др. – Новосибирск: Изд. НГПУ, 1994.

11. *Сизый, С.В.* Лекции по теории чисел: учеб. пособие для студентов вузов/ С.В.Сизый. – М.:ФИЗМАТЛИТ, 2007.

12. *Тропин, М.П.* Теория чисел: курс лекций для студентов математического факультета/ М.П.Тропин. – Новосибирск: Изд. НГПУ, 2006.

13. *Хинчин, А.Я.* Цепные дроби/А.Я.Хинчин. – М., 1978.

14. *Шнеперман, Л.Б.* Сборник задач по алгебре и теории чисел/ Л.Б.Шнеперман. – Минск, 1982.

# ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

# СОДЕРЖАНИЕ

Учебное издание

**Кузьмичёв Анатолий Иванович**

**Тропин Михаил Петрович**

**ТЕОРИЯ ЧИСЕЛ**

задачник-практикум для студентов 3-го курса

В авторской редакции

Компьютерная вёрстка М.П.Тропин

---

Подписано к печати 23.09.09. Формат бумаги 60x84/16

Печать RISO. Уч.-изд.л. 7,5. Усл.печ.л. 6,97. Тираж 100 экз.

Заказ №

---

Педуниверситет, 630126, Новосибирск, 126, Вилюйская, 28