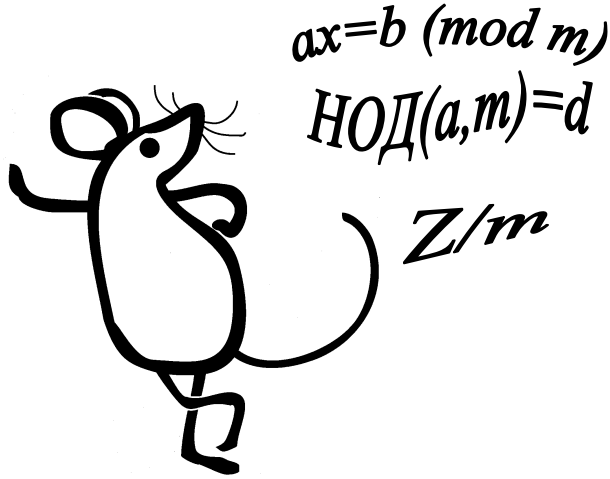
ГОУВПО «Воронежский государственный
технический университет»

Кафедра высшей математики и физико-математического
моделирования

ЭЛЕМЕНТЫ ТЕОРИИ СРАВНЕНИЙ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
для организации самостоятельной работы
по курсу «Алгебра» для студентов
специальностей 090102, 090105
очной формы обучения



Воронеж 2008

Составитель канд. физ.-мат. наук С.П. Майорова

УДК 512.8

Элементы теории сравнений: методические указания для организации самостоятельной работы по курсу «Алгебра» для студентов специальностей 090102, 090105 очной формы обучения/ ГОУВПО «Воронежский государственный технический университет»; сост. С.П. Майорова. Воронеж, 2008. 44 с.

В методических указаниях содержатся краткие основные сведения по разделу «Элементы теории сравнений», примеры решения типовых задач, задачи для самостоятельного решения и тестовые задания для итогового контроля.

Издание соответствует требованиям Государственного образовательного стандарта высшего профессионального образования по направлению 090100 «Информационная безопасность», специальностям 090102 «Компьютерная безопасность» и 090105 «Комплексное обеспечение информационной безопасности автоматизированных систем», дисциплине «Алгебра».

Библиогр.: 6 назв.

Рецензент канд. физ.-мат. наук, доц. М.Г. Завгородний

Ответственный за выпуск зав. кафедрой
д-р физ.-мат. наук, проф. И.Л. Батаронов

Печатается по решению редакционно-издательского совета Воронежского государственного технического университета

§ 1. ДЕЛИМОСТЬ В КОЛЬЦЕ ЦЕЛЫХ ЧИСЕЛ. ТЕОРЕМА О ДЕЛЕНИИ С ОСТАТКОМ. НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ

1.1. Отношение делимости в кольце целых чисел

Рассмотрим множество целых чисел $\mathbb{Z}$:

$$\mathbb{Z} = \{0,\ \pm 1,\ \pm 2,\ \pm 3,\ ...\}.$$

Целые числа относительно операций сложения и умножения образуют кольцо. Это означает, что сумма, разность и произведение двух целых чисел также является целым числом. Частное же от деления двух целых чисел может и не быть целым числом.

Определение. Пусть $a, b \in \mathbb{Z}$. Говорят, что число a *делится* на число b, или b *делит* a, если существует такое целое число c, что $a = bc$.

Обозначение: a *делится* на b записывают в виде $a \vdots b$; b *делит* a - в виде $b \mid a$.

Таким образом, по определению

$$a \vdots b \ \Leftrightarrow\ \exists c \in \mathbb{Z} \mid\ a = bc.$$

Из определения отношения делимости вытекает:
1) любое число, отличное от нуля, не делится на нуль;
2) нуль делится на любое число, в том числе и на нуль;
3) любое целое число a делится на $\pm a$, ± 1.

Свойства отношения делимости:

1) Если $a \vdots b$ и $a \neq 0$, то $|a| \geq |b|$.

2) Если $a \vdots b$, то $(\pm a) \vdots (\pm b)$.

3) Если $a \vdots c$ и $b \vdots c$, то $(au + bv) \vdots c$ для любых $u, v \in \mathbb{Z}$.

4) Если $a \vdots b$, то $(ka) \vdots b$ при любом $k \in \mathbb{Z}$.

5) Если $a \vdots b$ и $b \vdots a$, то $a = \pm b$.

1.2. Деление целых чисел с остатком

Определение. *Разделить с остатком* целое число a на целое число b - это значит найти целые числа q и r, которые удовлетворяют условиям:

1) $a = bq + r$,

2) $0 \le r < |b|$.

Числа q и r называются соответственно *неполным частным* и *остатком* от деления a на b.

Теорема (о делении с остатком). *Если* $a, b \in \mathbb{Z}$ *и* $b \neq 0$, *то число* a *можно разделить на число* b *с остатком, причем неполное частное и остаток определяются однозначно.*

Обращаем внимание на то, что остаток всегда - число *неотрицательное*: $r \ge 0$.

Остаток от деления a на b будем обозначать $r_b(a)$.

Сравнивая определение отношения делимости (п.1.1) и определение деления с остатком (п.1.2) и учитывая единственность неполного частного и остатка, получим:

Следствие. *Если* $a, b \in \mathbb{Z}$ *и* $b \neq 0$, *то* $a \vdots b \Leftrightarrow r_b(a) = 0$.

1.3. Наибольший общий делитель целых чисел, алгоритм Евклида его вычисления

Пусть a и b - два целых числа, из которых, по крайней мере, одно отлично от нуля.

Определение. *Наибольшим общим делителем* чисел a и b называется наибольшее натуральное число d, которое является делителем как для a, так и для b.

Если оба числа a, b равны нулю, то их наибольший общий делитель равен нулю.

Наибольший общий делитель чисел a и b обозначается $НОД(a, b)$.

Заметим, что в силу определения число $d = НОД(a,b)$ удовлетворяет двум условиям:

1) $a \vdots d$, $b \vdots d$;

2) для любого $d_1 \in \mathbb{Z}$ из условий $a \vdots d_1$, $b \vdots d_1$ следует $d \geq d_1$.

Для нахождения НОД двух целых чисел используют *алгоритм Евклида*. Опишем его.

Пусть $a,b \in \mathbb{Z}$ и $b \neq 0$. Разделим с остатком a на b, получим:

$$a = bq_1 + r_1, \quad 0 \leq r_1 < |b|.$$

Если $r_1 = 0$, то алгоритм окончен. В этом случае $a \vdots b$ и $НОД(a,b) = |b|$. Если же $r_1 \neq 0$, то делим с остатком b на r_1:

$$b = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1.$$

Если $r_2 = 0$, то алгоритм окончен; в противном случае делим с остатком r_1 на r_2, и так далее до тех пор, пока не получим остаток, равный нулю. Запишем алгоритмом Евклида символически:

$$\begin{array}{lll}
a : b & a = bq_1 + r_1, & 0 < r_1 < |b|; \\
b : r_1 & b = r_1q_2 + r_2, & 0 < r_2 < r_1; \\
r_1 : r_2 & r_1 = r_2q_3 + r_3, & 0 < r_3 < r_2; \\
\ldots & \ldots, & \ldots; \\
r_{k-2} : r_{k-1} & r_{k-2} = r_{k-1}q_k + r_k, & 0 < r_k < r_{k-1}; \\
r_{k-1} \vdots r_k & r_{k-1} = r_kq_{k+1}. &
\end{array}$$

Последний, отличный от нуля остаток в алгоритме Евклида есть наибольший общий делитель чисел a и b, т.е. $НОД(a,b) = r_k$.

Наибольший общий делитель обладает следующим важным свойством.

Теорема (о линейном представлении НОД). *Если* $a,b\in\mathbb{Z}$ *и* $d=НОД(a,b)$, *то существуют такие числа* $u_0,v_0\in\mathbb{Z}$, *что выполняется равенство*

$$d=au_0+bv_0.$$

Наибольший общий делитель нескольких чисел ищется следующим образом. Сначала находят НОД любых двух чисел, затем НОД - для полученного общего делителя и третьего числа и так далее. Последнее, полученное таким образом число и будет НОД для всех данных чисел. Так, для трех чисел имеем:

$$НОД(a,b,c)=НОД(НОД(a,b),c).$$

1.4. Взаимно простые числа

Определение. Целые числа a и b называются *взаимно простыми*, если $НОД(a,b)=1$.

Свойства взаимно простых чисел:

1) Целые числа a и b взаимно просты тогда и только тогда, когда существуют целые числа u, v такие, что $au+bv=1$.

2) Если $НОД(a,b)=1$, $НОД(a,c)=1$, то $НОД(a,bc)=1$.

3) Если $(ab)\vdots c$ и $НОД(a,c)=1$, то $b\vdots c$.

4) Если $НОД(a,b)=d$, $d\neq 0$, то $НОД\left(\frac{a}{d},\frac{b}{d}\right)=1$, т.е. числа $\frac{a}{d}$ и $\frac{b}{d}$ являются взаимно простыми.

5) Если $a\vdots b$ и $a\vdots c$, причем $НОД(b,c)=1$, то $a\vdots(bc)$.

1.5. Наименьшее общее кратное целых чисел

Определение. *Наименьшим общим кратным* целых чисел a и b называется такое наименьшее натуральное число, которое делится как на a, так и на b.

Наименьшее общее кратное чисел a и b обозначают $НОК(a,b)$.

Теорема. *Если целые числа a, b отличны от нуля, то*

$$НОК(a,b)=\frac{|ab|}{НОД(a,b)}.$$

1.6. Простые числа. Каноническое разложение целых чисел

Определение. Натуральное число $p>1$ называется *простым,* если оно не имеет натуральных делителей, отличных от 1 и p; в противном случае число называется *составным*.

Теорема (основная теорема арифметики). *Любое натуральное число $n>1$ либо является простым, либо разлагается в произведение простых чисел, причем такое разложение единственно с точностью до перестановки сомножителей.*

Из теоремы следует, что любое целое число $a\neq 0;1$ можно однозначно представить в виде

$$a=\varepsilon p_1^{k_1}p_2^{k_2}...p_m^{k_m},$$

где $\varepsilon=\pm 1$; $p_1, p_2,\ldots, p_m$ - различные простые числа, $p_1<p_2<...<p_m$; $k_1,\ k_2,\ldots,\ k_m$ - натуральные числа. Такое представление числа a называется его *каноническим разложением*.

Канонические разложения целых чисел можно использовать для нахождения *НОД* и *НОК*.

Рассмотрим два целых числа a и b. Дополним их канонические разложения сомножителями вида p_i^0. Получим:

$$a = \varepsilon_1 p_1^{t_1} p_2^{t_2} \dots p_k^{t_k}, \qquad b = \varepsilon_2 p_1^{s_1} p_2^{s_2} \dots p_k^{s_k},$$

где $\varepsilon_1, \varepsilon_2 \in \{1, -1\}$; $t_i \geq 0$, $s_i \geq 0$, $i = \overline{1,k}$; $p_1 < p_2 < \dots < p_k$. Тогда

$$НОД(a,b) = p_1^{\min(t_1,s_1)} \dots p_k^{\min(t_k,s_k)},$$

$$НОК(a,b) = p_1^{\max(t_1,s_1)} \dots p_k^{\max(t_k,s_k)}.$$

Заметим, что задача нахождения канонического разложения целого числа сама является в общем случае сложной. Поэтому на практике *НОД* и *НОК* больших чисел находят с помощью алгоритма Евклида.

При нахождении простых делителей натурального числа полезно иметь в виду следующее. Наименьший $(\neq 1)$ делитель p числа n является числом простым и $p^2 \leq n$, если n - число составное.

Решение типовых задач

Задача 1. Найти частное и остаток от деления числа a на число b, если:

а) $a = 764$, $b = 13$;
б) $a = 764$, $b = -13$;
в) $a = -764$, $b = 13$;
г) $a = -764$, $b = -13$.

Решение. Воспользуемся теоремой о делении с остатком. Число a запишем в виде

$$a = bq + r, \qquad \text{где} \quad 0 \leq r < |b|.$$

а) Обычным делением находим

$$764 = 13 \cdot 58 + 10, \quad \text{т.е. } q = 58,\ r = 10.$$

б) В равенстве (а) одновременно поменяем знаки у делителя и частного:

$$764 = (-13) \cdot (-58) + 10, \quad \text{т.е. } q = -58,\ r = 10.$$

в) Обе части равенства (а) умножим на (-1):

$$-764 = 13 \cdot (-58) - 10.$$

Затем, чтобы получить *неотрицательный* остаток, в правой части равенства проибавим и вычтем 13. Получим:

$$-764 = 13 \cdot (-59) + 3, \quad \text{т.е. } q = -59,\ r = 3.$$

г) Поступим так же, как в случае (в), но знак минус отнесем к делителю:

$$-764 = (-13) \cdot 58 - 10 = (-13) \cdot 59 + 3, \quad \text{т.е. } q = 59,\ r = 3.$$

Задача 2. Для чисел $a = 1068$, $b = 309$ найти наибольший общий делитель.

Решение. Применяя алгоритм Евклида к данным числам, получим цепочку равенств:

$a : b$ $\quad 1068 = 309 \cdot 3 + 141, \quad r_1 = 141;$

$b : r_1$ $\quad 309 = 141 \cdot 2 + 27, \quad r_2 = 27;$

$r_1 : r_2$ $\quad 141 = 27 \cdot 5 + 6, \quad r_3 = 6;$

$r_2 : r_3$ $\quad 27 = 6 \cdot 4 + 3, \quad r_4 = 3;$

$r_3 : r_4$ $\quad 6 = 3 \cdot 2.$

Последний, отличный от нуля остаток в алгоритме Евклида есть $НОД(a, b)$, т.е. $НОД(1068, 309) = r_4 = 3$.

Задача 3. Для чисел $a = 1068$, $b = 309$ получить линейное представление *НОД*.

Решение. Алгоритм Евклида для данных чисел a и b указан в задаче 2; там же найдено, что $НОД(a,b) = 3$.

Найдем линейное представление *НОД*, т.е. найдем числа $u_0, v_0 \in \mathbb{Z}$ такие, что выполняется равенство $НОД(a,b) = au_0 + bv_0$.

Для этого из равенств в алгоритме Евклида выразим остатки, начиная с последнего:

$$r_4 = 3 = 27 - 6 \cdot 4, \quad (1)$$

$$r_3 = 6 = 141 - 27 \cdot 5, \quad (2)$$

$$r_2 = 27 = 309 - 141 \cdot 2, \quad (3)$$

$$r_1 = 141 = 1068 - 309 \cdot 3. \quad (4)$$

Из правых частей полученных равенств (1)-(4) будем последовательно исключать остатки. Сначала в равенство (1) подставим выражение для остатка $r_3 = 6$ - см. равенство (2). Получим:

$$НОД(a,b) = r_4 = 3 = 27 - 6 \cdot 4 =$$

$$= 27 - (141 - 27 \cdot 5) \cdot 4 = 27 \cdot 21 - 141 \cdot 4.$$

В полученное равенство подставим выражение для остатка $r_2 = 27$ - см. равенство (3). Получим:

$$НОД(a,b) = 27 \cdot 21 - 141 \cdot 4 =$$

$$= (309 - 141 \cdot 2) \cdot 21 - 141 \cdot 4 = 309 \cdot 21 - 141 \cdot 46.$$

Наконец, в последнее равенство подставим выражение для остатка $r_1 = 141$ - см. равенство (4). Получим:

$$НОД(a,b) = 309 \cdot 21 - 141 \cdot 46 =$$

$$= 309 \cdot 21 - (1068 - 309 \cdot 3) \cdot 46 = 309 \cdot 159 - 1068 \cdot 46 .$$

Таким образом, для данных чисел $a = 1068$ и $b = 309$ линейное представление *НОД* найдено, а именно:

$$НОД(a,b) = 3 = a \cdot (-46) + b \cdot 159 .$$

Задача 4. Для чисел $a = 1068$, $b = 309$ найти наименьшее общее кратное.

Решение. Для нахождения $НОК(a,b)$ воспользуемся формулой $НОК(a,b) = \dfrac{|ab|}{НОД(a,b)}$.

Наибольший общий делитель данных чисел a и b уже найден в задаче 2: $НОД(1068,309) = 3$. Тогда

$$НОК(1068,309) = \frac{1068 \cdot 309}{3} = 110004 .$$

Задача 5. Вычислить $НОД(588,2058,2849)$ двумя способами – с помощью алгоритма Евклида и с помощью разложения чисел на простые множители.

Решение. *Первый способ*. Воспользуемся равенством

$$НОД(a,b,c) = НОД(НОД(a,b),c) .$$

Сначала применим алгоритм Евклида к числам $a = 588$ и $b = 2058$. Имеем:

$b : a$ $\quad 2058 = 588 \cdot 3 + 294$,

$a : r_1$ $\quad 588 = 294 \cdot 2$.

Отсюда находим $НОД(588,2058) = 294$.

Теперь вычислим $НОД(НОД(a,b),c) = НОД(294,2849)$. С помощью алгоритма Евклида имеем:

$$2849 = 294 \cdot 9 + 203,$$
$$294 = 203 \cdot 1 + 91,$$
$$203 = 91 \cdot 2 + 21,$$
$$91 = 21 \cdot 4 + 7,$$
$$21 = 7 \cdot 3.$$

Отсюда находим $НОД(294, 2849) = 7$. Окончательно получаем: $НОД(588, 2058, 2849) = НОД(294, 2849) = 7$.

Второй способ. Разложим данные числа на простые множители:

588	2	2058	2	2849	7
294	2	1029	3	407	11
147	3	343	7	37	37
49	7	49	7	1	
7	7	7	7		
1		1			

Итак, $588 = 2^2 \cdot 3 \cdot 7^2$, $2058 = 2 \cdot 3 \cdot 7^3$, $2849 = 7 \cdot 11 \cdot 37$.

Для нахождения *НОД* трех данных чисел выбираем общие простые множители в наименьшей встречающейся степени (см. п.1.6). Окончательно получим:

$$НОД(588, 2058, 2849) = 2^0 \cdot 3^0 \cdot 7^1 \cdot 11^0 \cdot 37^0 = 7.$$

Задача 6. Выяснить, простым или составным является число 1001.

Решение. Пусть 1001 - число составное. Тогда наименьший простой делитель p этого числа удовлетворяет неравенству (см. п.1.6): $p^2 \le n$, или $p \le \sqrt{n}$. В данном случае $\sqrt{n} = \sqrt{1001} \approx 31,6$; тогда $p \le 31$. Этому неравенству удовлетворяют простые числа 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31. Проверка показывает, что $1001 \vdots 7$, поэтому 1001 - число составное.

Задачи для самостоятельного решения

Задача 1. Докажите, что для любых $a, b, k \in \mathbb{Z}$ справедливы равенства:

1) $НОД(a,b) = НОД(a-kb,b) = НОД(a,b-ka)$;

2) $НОД(ka,kb) = k \cdot НОД(a,b)$;

3) $НОД(a,b) = НОД(b,r)$, где r - остаток от деления a на b;

4) если $НОД(a,b) = 1$, то $НОД(a,bc) = НОД(a,c)$.

Задача 2. Дано каноническое разложение натурального числа $a = p_1^{k_1} \ldots p_m^{k_m}$. Докажите, что числа вида $d = p_1^{t_1} \ldots p_m^{t_m}$, где $0 \le t_i \le k_i$, $t_i \in \mathbb{Z}$, и только они являются делителями числа a.

Задача 3. Для данных чисел a, b найти *НОД* двумя способами – с помощью алгоритма Евклида и с помощью разложения чисел на простые множители; получить линейное представление *НОД*; найти $НОК(a,b)$:

1) $a = 285$, $b = 363$; Ответ: $НОД(a,b) = 3 = -14a + 11b$

2) $a = 12103$, $b = 1425$; Ответ: $НОД(a,b) = 19 = -2a + 17b$

3) $a = 2237$, $b = 1021$. Ответ: $НОД(a,b) = 1 = 466a - 1021b$

Задача 4. Вычислить $НОД(279,372,1395)$ двумя способами – с помощью алгоритма Евклида и с помощью разложения чисел на простые множители. Ответ: 93

§ 2. СРАВНЕНИЯ ЦЕЛЫХ ЧИСЕЛ ПО МОДУЛЮ. РЕШЕНИЕ СРАВНЕНИЙ

2.1. Сравнения целых чисел и их свойства

Пусть m - данное натуральное число, условимся называть его *модулем*.

Определение. Два целых числа a и b называются *сравнимыми по модулю* m, если при делении на m они дают одинаковые остатки.

Обозначение: $a \equiv b (\mathrm{mod}\, m)$.

На практике сравнимость двух чисел удобно проверять с помощью следующего критерия.

Теорема (критерий сравнимости). *Целые числа* a, b *сравнимы по модулю* m *тогда и только тогда, когда разность* $(a-b)$ *делится на* m, *т.е.*

$$a \equiv b (\mathrm{mod}\, m) \Leftrightarrow (a-b) \vdots m.$$

Из теоремы вытекает, что сравнение $a \equiv b (\mathrm{mod}\, m)$ равносильно возможности представить число a в виде $a = b + mk$ при некотором $k \in \mathbb{Z}$.

Простейшие свойства сравнений:

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

2) Если $a \equiv b (\mathrm{mod}\, m)$, то $b \equiv a (\mathrm{mod}\, m)$.

3) Если $a \equiv b (\mathrm{mod}\, m)$ и $b \equiv c (\mathrm{mod}\, m)$, то $a \equiv c (\mathrm{mod}\, m)$.

4) Если $a \equiv b (\mathrm{mod}\, m)$ и $c \equiv d (\mathrm{mod}\, m)$,
то $a + c \equiv b + d (\mathrm{mod}\, m)$, т.е. сравнения можно почленно складывать.

Следствие. К одной части сравнения можно прибавить число, кратное модулю, т.е. $a \equiv b(\mathrm{mod}\, m) \Leftrightarrow a \equiv b + mk(\mathrm{mod}\, m)$, $k \in \mathbb{Z}$.

5) Если $a \equiv b(\mathrm{mod}\, m)$ и $c \equiv d(\mathrm{mod}\, m)$, то $ac \equiv bd(\mathrm{mod}\, m)$, т.е. сравнения можно почленно перемножать.

Следствие 1. Обе части сравнения можно умножить на одно и то же целое число, т.е. $a \equiv b(\mathrm{mod}\, m) \Rightarrow ka \equiv kb(\mathrm{mod}\, m)$, $k \in \mathbb{Z}$.

Следствие 2. Обе части сравнения можно возвести в одну и ту же степень, т.е. $a \equiv b(\mathrm{mod}\, m) \Rightarrow a^k \equiv b^k(\mathrm{mod}\, m)$.

6) Если d - общий делитель чисел a, b и $НОД(d, m) = 1$, то $a \equiv b(\mathrm{mod}\, m) \Leftrightarrow \frac{a}{d} \equiv \frac{b}{d}(\mathrm{mod}\, m)$, т.е обе части сравнения можно делить на число, взаимно простое с модулем.

7) Если d - общий делитель чисел a, b, m, то $a \equiv b(\mathrm{mod}\, m) \Leftrightarrow \frac{a}{d} \equiv \frac{b}{d}(\mathrm{mod}\, \frac{m}{d})$, т.е обе части сравнения и модуль можно разделить на их общий делитель.

2.2. Сравнения первой степени с одним неизвестным

Определение. Сравнение вида $ax \equiv b(\mathrm{mod}\, m)$, где a, b - целые числа, m - натуральное число, называется *сравнением первой степени с одним неизвестным*.

Определение. *Решением сравнения* $ax \equiv b(\mathrm{mod}\, m)$ называется любое целое число, при подстановке которого вместо x сравнение превращается в верное числовое сравнение.

Определение. Два сравнения называются *равносильными*, если они имеют одно и то же множество решений.

Прежде чем решать сравнения, сделаем следующие замечания.

1) Если в сравнении $ax \equiv b(\mathrm{mod}\, m)$ любой из коэффициентов a, b заменить сравнимым с ним по модулю m числом, то получится сравнение, равносильное исходному.

2) Если некоторое целое число x_0 является решением сравнения, то его решениями являются все числа класса $x \equiv x_0(\mathrm{mod}\, m)$. Поэтому весь этот класс называют *одним* решением модулю m, а число различных классов целых чисел, удовлетворяющих данному сравнению, называют *числом решений* по модулю m.

Приведем условия разрешимости сравнений первой степени.

Теорема 1. *Если* $НОД(a,m)=1$, *то сравнение* $ax \equiv b(\mathrm{mod}\, m)$ *имеет единственное решение по модулю* m.

Теорема 2. *Пусть* $НОД(a,m)=d$. *Сравнение* $ax \equiv b(\mathrm{mod}\, m)$ *имеет решения тогда и только тогда, когда* $b \vdots d$. *Если* $b \vdots d$, *то сравнение имеет ровно* d *решений по модулю* m.

2.3. Решение сравнений первой степени с помощью рекуррентной формулы

Рассмотрим сравнение $ax \equiv b\ (\mathrm{mod}\, m)$. Если его коэффициенты a, b и модуль m являются большим числами, то нахождение решения этого сравнения с помощью простейших свойств затруднительно. Тогда для решения сравнения применяют другой способ – используют рекуррентную формулу. Опишем этот способ.

Заметим, что в силу теоремы 2 п.2.2 нахождение решений сравнения $ax \equiv b\ (\mathrm{mod}\, m)$ всегда можно свести к случаю, когда $НОД(a,m)=1$. Действительно, если

$НОД(a,m)=d\neq 1$ и $b\vdots d$, то разделив обе части данного сравнения и модуль на число d, получим сравнение $a_1x\equiv b_1 \pmod{m_1}$, где числа $a_1=\frac{a}{d}$ и $m_1=\frac{m}{d}$ - взаимно простые.

Пусть дано сравнение

$$ax\equiv b \pmod{m}, \quad \text{где} \quad НОД(a,m)=1.$$

Это сравнение имеет единственное решение (в силу теоремы 1 п.2.2). Для отыскания этого решения применим алгоритм Евклида к числам a и m, а затем воспользуемся формулой

$$x\equiv bV \pmod{m},$$

где число V находят из таблицы

k	0	1	2	…	i	…	n
q_k	–	q_1	q_2	…	q_i	…	q_n
V_k	$V_0=1$	$V_1=-q_1$	V_2	…	V_i	…	$V_n=V$

Здесь $q_1,q_2,\ldots,q_n$ - последовательность неполных частных в алгоритме Евклида для чисел a и m; все числа V_2, … , V_n вычисляются по рекуррентной формуле:

$$V_k=V_{k-2}-V_{k-1}q_k, \quad k=\overline{2,n}.$$

2.4. Системы сравнений

Рассмотрим системы сравнений первой степени с одним неизвестным. При этом ограничимся системами, состоящими из сравнений вида $x\equiv a(\bmod m)$, так как к таким системам может быть сведена всякая система сравнений с одним неизвестным.

Теорема (китайская теорема об остатках). *Если натуральные числа* m_1, m_2, … , m_k *попарно взаимно просты, то система сравнений*

$$\begin{cases} x \equiv a_1 (\mathrm{mod}\, m_1) \\ x \equiv a_2 (\mathrm{mod}\, m_2) \\ \quad \ldots \\ x \equiv a_k (\mathrm{mod}\, m_k) \end{cases}$$

имеет единственное решение по модулю $M = m_1 m_2 ... m_k$ *при любых* a_1, a_2, … , $a_k \in \mathbb{Z}$.

Алгоритм решения указанной системы сравнений следующий:

1) Сначала решим систему из первых двух сравнений. Для этого из первого сравнения системы находим

$$x = a_1 + m_1 y, \quad \text{где} \quad y \in \mathbb{Z}.$$

2) Подставим во второе сравнение вместо x выражение $a_1 + m_1 y$. Решим полученное сравнение $a_1 + m_1 y \equiv a_2 (\mathrm{mod}\, m_2)$ относительно y. Получим

$$y = b_1 + m_2 t, \quad \text{где} \quad t \in \mathbb{Z}.$$

Подставив найденные значения y в равенство $x = a_1 + m_1 y$, получим все решения системы из первых двух сравнений:

$$x = a_1 + m_1 y = a_1 + m_1 (b_1 + m_2 t) = a_1 + m_1 b_1 + m_1 m_2 t.$$

Они образуют единственное решение по модулю $m_1 m_2$.

3) Подставим найденные значения $x = a_1 + m_1 b_1 + m_1 m_2 t$ в третье сравнение системы и найдем t, и т.д.

4) Продолжая этот процесс, мы найдем все решения данной системы сравнений, которые будут составлять один класс чисел по модулю $M = m_1 m_2 ... m_k$.

2.5. Функция Эйлера, ее применение к решению сравнений

Определение. *Функцией Эйлера* называется функция φ, определенная на множестве натуральных чисел следующим образом: значение $\varphi(n)$ равно количеству натуральных чисел, не превосходящих n и взаимно простых с n.

Приведем формулу для вычисления $\varphi(n)$.

Если натуральное число n имеет каноническое разложение $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, то

$$\varphi(n) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \ldots p_k^{\alpha_k - 1}(p_1 - 1)(p_2 - 1) \ldots (p_k - 1).$$

Теорема (Эйлера). *Если числа a, m взаимно просты, то*

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

Следствие. Если p - простое число и $a \in \mathbb{Z}$, то:

1) $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$ при $НОД(a, p) = 1$;

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

Утверждение 1) следствия называют *малой теоремой Ферма*.

Теорема Эйлера позволяет указать формулу для нахождения решения сравнений первой степени.

Теорема. *Решение сравнения $ax \equiv b (\mathrm{mod}\, m)$, где $НОД(a, m) = 1$, имеет вид*

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

Решение типовых задач

Задача 1. Выясните, какие из данных чисел сравнимы по модулю $m = 6$; проверьте, можно ли из данных чисел составить полную систему вычетов по модулю $m = 6$:

259, -87, 165, 348, -16, 503, -124, 52.

Решение. Найдем остатки от деления данных чисел на модуль $m = 6$:

$259 = 6 \cdot 43 + 1$; $\quad -16 = 6 \cdot (-3) + 2$;

$-87 = 6 \cdot (-15) + 3$; $\quad 503 = 6 \cdot 83 + 5$;

$165 = 6 \cdot 27 + 3$; $\quad -124 = 6 \cdot (-21) + 2$;

$348 = 6 \cdot 58 + 0$; $\quad 52 = 6 \cdot 8 + 4$.

Замечаем, что числа -87 и 165, а также -16 и -124 дают одинаковые остатки, поэтому эти числа сравнимы:

$$-87 \equiv 165 \pmod 6,$$

$$-16 \equiv -124 \pmod 6.$$

Выясним, можно ли из данных чисел составить полную систему вычетов. Замечаем, что в результате деления чисел на модуль $m = 6$ получены *всевозможные* остатки, которые можно получить при делении на 6 – это 0, 1, 2, 3, 4, 5. Поэтому полную систему вычетов составить можно. Она должна состоять из шести чисел. Например,

259, -87, 348, -16, 503, 52.

Задача 2. Найдите количество натуральных чисел, не превышающих данного числа $n = 1584$ и взаимно простых с числом n.

Решение. Искомое количество натуральных чисел равно значению функции Эйлера $\varphi(n)$. Для нахождения $\varphi(n)$ получим каноническое разложение данного числа $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, а затем воспользуемся формулой

$$\varphi(n) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \ldots p_k^{\alpha_k - 1} (p_1 - 1)(p_2 - 1) \ldots (p_k - 1).$$

Разложение данного числа $n = 1584$ на простые множители имеет вид: $1584 = 2^4 \cdot 3^2 \cdot 11$.

Тогда количество натуральных чисел, не превышающих числа 1584 и взаимно простых с этим числом равно

$$\varphi(1584) = \varphi(2^4 \cdot 3^2 \cdot 11) = 2^3 \cdot 3^1 \cdot 11^0 \cdot (2-1)(3-1)(11-1) = 480.$$

Задача 3. Найдите остаток $r_m(a)$ от деления числа $a = 23^{48} + 48^{23}$ на число $m = 7$.

Решение. Сначала каждое слагаемое заменим на сравнимое с ним число. Заметим, что

$$23 \equiv 2 (\mathrm{mod}\, 7), \quad 48 \equiv -1 (\mathrm{mod}\, 7).$$

Отсюда в силу свойств числовых сравнений (см. п.2.1, следствие 2 свойства 5) получим:

$$23^{48} \equiv 2^{48} (\mathrm{mod}\, 7), \qquad 48^{23} \equiv (-1)^{23} (\mathrm{mod}\, 7).$$

Тогда $a = 23^{48} + 48^{23} \equiv 2^{48} + (-1)^{23} = (2^3)^{16} - 1.$

Теперь замечаем, что $2^3 \equiv 1 (\mathrm{mod}\, 7)$, тогда

$$a = 23^{48} + 48^{23} \equiv 1^{16} - 1 \equiv 0 (\mathrm{mod}\, 7).$$

Таким образом, остаток от деления числа $a = 23^{48} + 48^{23}$ на число $m = 7$ найден, а именно: $r_7(a) = 0$, значит число a делится на 7.

Задача 4. Исследуйте и решите сравнения, используя простейшие свойства сравнений; сделайте проверку:

а) $22x \equiv 7(\mathrm{mod}19)$;

б) $28x \equiv 8(\mathrm{mod}12)$;

в) $26x \equiv 10(\mathrm{mod}13)$.

Решение. а) Рассмотрим первое сравнение

$$22x \equiv 7(\mathrm{mod}19).$$

Исследуем его. Здесь $НОД(a,m) = НОД(22,19) = 1$, следовательно, в силу теоремы 1 п.2.2 сравнение имеет единственное решение.

Найдем это решение. Используя простейшие свойства сравнений, получим:

$22x \equiv 7(\mathrm{mod}19)$,

$22x - 19x \equiv 7(\mathrm{mod}19)$,

$3x \equiv 7(\mathrm{mod}19)$,

$3x \equiv 7 + 2 \cdot 19(\mathrm{mod}19)$,

$3x \equiv 45(\mathrm{mod}19) \ \vdots 3, \ НОД(3,19) = 1$,

$x \equiv 15(\mathrm{mod}19)$.

Сделаем проверку. Найденное значение $x = 15$ подставим в исходное сравнение: $22 \cdot 15 \equiv 7(\mathrm{mod}19)$. Выясним, верно ли полученное числовое сравнение. Для этого воспользуемся критерием сравнимости (см. п.2.1); проверим, делится ли разность $22 \cdot 15 - 7$ на 19. Имеем: $22 \cdot 15 - 7 = 323$ и 323:19=17. Таким образом, $(22 \cdot 15 - 7) \vdots 19$, следовательно, числовое сравнение $22 \cdot 15 \equiv 7(\mathrm{mod}19)$ - верно.

Ответ: $x \equiv 15(\mathrm{mod}19)$.

б) Рассмотрим второе сравнение $28x \equiv 8(\mathrm{mod}12)$. Исследуем его. Здесь $НОД(a,m) = НОД(28,12) = 4$, причем $b = 8$ делится на 4; следовательно, в силу теоремы 2 п.2.2 сравнение имеет четыре решения.

Найдем эти решения. Разделим обе части данного сравнения и модуль на 4, получим:

$$28x \equiv 8(\mathrm{mod}12) \ \big| : 4,$$

$$7x \equiv 2(\mathrm{mod}3),$$

$$7x - 6x \equiv 2(\mathrm{mod}3),$$

$$x \equiv 2(\mathrm{mod}3).$$

Отсюда находим четыре решения исходного сравнения по модулю 12: x_1, $x_1 + m_1$, $x_1 + 2m_1$, $x_1 + 3m_1$, где $x_1 = 2$, $m_1 = 3$:

$$x_1 \equiv 2(\mathrm{mod}12),$$

$$x_2 \equiv 5(\mathrm{mod}12),$$

$$x_3 \equiv 8(\mathrm{mod}12),$$

$$x_4 \equiv 11(\mathrm{mod}12).$$

Сделаем проверку. Значение $x = 2$ подставим в исходное сравнение: $28 \cdot 2 \equiv 8(\mathrm{mod}12)$ и выясним, верно ли полученное числовое сравнение. Воспользуемся критерием сравнимости (см. п.2.1); разность $28 \cdot 2 - 8 = 48$ делится на 12, следовательно, числовое сравнение $28 \cdot 2 \equiv 8(\mathrm{mod}12)$ - верно.
Ответ: $x \equiv 2,\ 5,\ 8,\ 11\ (\mathrm{mod}12)$.

в) Рассмотрим третье сравнение $26x \equiv 10(\mathrm{mod}13)$. Исследуем его. Здесь $d = НОД(a,m) = НОД(26,13) = 13$. Так как $b = 10$ не делится на $d = 13$, то данное сравнение решений не имеет. Ответ: решений нет.

Задача 5. Решите сравнение $6x \equiv 15(\mathrm{mod}\,45)$ с помощью функции Эйлера.

Решение. Так как $НОД(a,m) = НОД(6,45) = 3$ и $b = 15$ делится на 3, то сравнение имеет три решения по $\mathrm{mod}\,45$. Найдем их. Данное сравнение равносильно сравнению $2x \equiv 5(\mathrm{mod}15)$, в котором $НОД(a,m) = НОД(2,15) = 1$. Поэтому последнее сравнение имеет единственное решение по $\mathrm{mod}15$, которое найдем с помощью функции Эйлера. В силу теоремы п.2.5 имеем:

$$x \equiv 5 \cdot 2^{\varphi(15)-1}(\mathrm{mod}15).$$

Так как $\varphi(15) = 8$, то $x \equiv 5 \cdot 2^7(\mathrm{mod}15)$.
Упростим найденное решение:

$$x \equiv 5 \cdot 2^7 = 10 \cdot 2^6 = 10 \cdot 64 \equiv 10 \cdot 4 = 40 \equiv 10(\mathrm{mod}15).$$

Таким образом, $x \equiv 10(\mathrm{mod}15)$. Этот класс разбивается на три класса решений по исходному модулю 45:

$$x_1 \equiv 10(\mathrm{mod}\,45), \quad x_2 \equiv 25(\mathrm{mod}\,45), \quad x_3 \equiv 40(\mathrm{mod}\,45).$$

Ответ: $x \equiv 10,\ 25,\ 40\ (\mathrm{mod}\,45)$.

Задача 6. Исследуйте и решите сравнение, используя рекуррентную формулу; сделайте проверку:

$$729x \equiv 33\ (\mathrm{mod}\ 321).$$

Решение. Сначала упростим сравнение, заменив в нем коэффициент 729 остатком от деления на модуль 321. Получим сравнение, равносильное данному:

$$87x \equiv 33\ (\mathrm{mod}\ 321). \qquad (1)$$

Исследуем полученное сравнение, для этого проверим условия теоремы 2 п.2.2. С помощью алгоритма Евклида найдем *НОД* чисел $a = 87$ и $m = 321$. Имеем:

$m : a \qquad 321 = 87 \cdot 3 + 60;$

$a : r_1 \qquad 87 = 60 \cdot 1 + 27;$

$r_1 : r_2 \qquad 60 = 27 \cdot 2 + 6;$

$r_2 : r_3 \qquad 27 = 6 \cdot 4 + 3;$

$r_3 \vdots r_4 \qquad 6 = 3 \cdot 2.$

Следовательно, $d = НОД(87, 321) = 3$. Так как правая часть сравнения $b = 33$ делится на $d = 3$, то сравнение разрешимо и имеет ровно 3 решения по модулю 321.

Решим сравнение (1). Сначала поделим обе его части на число $d = 3$, получим равносильное сравнение

$$29x \equiv 11 \pmod{107}, \qquad (2)$$

имеющее единственное решение по модулю 107. Для отыскания решения сравнения (2) используем рекуррентную формулу (см. п.2.3). Применим алгоритм Евклида к числам $a = 29$ и $m = 107$. Имеем

$m : a \qquad 107 = 29 \cdot 3 + 20;$

$a : r_1 \qquad 29 = 20 \cdot 1 + 9;$

$r_1 : r_2 \qquad 20 = 9 \cdot 2 + 2;$

$r_2 : r_3 \qquad 9 = 2 \cdot 4 + 1;$

$r_3 \vdots r_4 \qquad 2 = 1 \cdot 2.$

Отсюда получаем последовательность неполных частных: $q_1 = 3$, $q_2 = 1$, $q_3 = 2$ и $q_4 = 4$. По ним, пользуясь рекуррентной формулой $V_k = V_{k-2} - V_{k-1} q_k$ $(k = 2, 3, 4)$, найдем число $V = V_4$:

$$\left.\begin{array}{l} V_0 = 1 \\ V_1 = -q_1 = -3 \end{array}\right\}$$ начальные условия

$V_2 = V_0 - V_1 q_2 = 4$,

$V_3 = V_1 - V_2 q_3 = -11$,

$V_4 = V_2 - V_3 q_4 = 48$.

Весь процесс вычисления удобно записать в виде таблицы:

k	0	1	2	3	4
q_k	–	3	1	2	4
V_k	1	–3	4	–11	$48 = V$

Теперь по формуле $x \equiv bV \pmod{m}$ находим решение сравнения (2) по модулю 107:

$$x \equiv 48 \cdot 11 \equiv 100 \pmod{107}.$$

Отсюда найдем все три решения данного сравнения (1) по модулю 321:

$x_1 \equiv 100 \pmod{321}$,

$x_2 \equiv 100 + 107 \equiv 207 \pmod{321}$,

$x_3 \equiv 100 + 107 \cdot 2 \equiv 314 \pmod{321}$.

Сделаем проверку. Значение $x = 100$ подставим в исходное сравнение: $729 \cdot 100 \equiv 33 \pmod{321}$. С помощью критерия сравнимости (см. п.2.1) выясним, верно ли полученное числовое сравнение. Имеем: $729 \cdot 100 - 33 = 72867$ и $72867 : 321 = 227$, т.е $(729 \cdot 100 - 33) \vdots 321$; следовательно, числовое сравнение $729 \cdot 100 \equiv 33 \pmod{321}$ - верно.

Ответ: $x \equiv 100,\ 207,\ 314 \pmod{321}$.

Задача 7. Решите систему сравнений:

$$\begin{cases} x \equiv 16 \pmod 5 \\ x \equiv 27 \pmod 4 \\ x \equiv 2 \pmod{13} \end{cases}.$$

Решение. В данной системе модули $m_1 = 5$, $m_2 = 4$ и $m_3 = 13$ являются попарно взаимно простыми числами, тогда в силу китайской теоремы об остатках (см. п.2.4) система имеет единственное решение по модулю $M = m_1 m_2 m_3 = 5 \cdot 4 \cdot 13 = 260$. Найдем это решение. Предварительно упростим правые части каждого из сравнений. Имеем:

$$\begin{cases} x \equiv 1 \pmod 5 \\ x \equiv 3 \pmod 4 \\ x \equiv 2 \pmod{13} \end{cases}.$$

1) Сначала решим систему, состоящую из первых двух сравнений:

$$\begin{cases} x \equiv 1 \pmod 5 \\ x \equiv 3 \pmod 4 \end{cases}.$$

Первое сравнение определяет целые числа, представимые в виде

$$x = 5k + 1, \quad k \in \mathbb{Z}.$$

Найдем все значения k, при которых x удовлетворяет и второму сравнению системы. Для этого подставим во второе сравнение вместо x выражение $5k + 1$ и решим полученное сравнение:

$$5k + 1 \equiv 3 \pmod 4.$$

Имеем:

$$5k+1\equiv 3 \pmod 4 \;\Leftrightarrow\; 5k\equiv 2 \pmod 4 \;\Leftrightarrow\; k\equiv 2 \pmod 4;$$

значит $k=4t+2$, $t\in\mathbb{Z}$. Подставим найденное выражение для k в равенство $x=5k+1$, получим:

$$x=5k+1=5(4t+2)+1=20t+11.$$

Последнее означает, что $x\equiv 11 \pmod{20}$. Тем самым все решения системы из первых двух сравнений найдены.

2) Заменим теперь первые два сравнения исходной системы на их решение $x\equiv 11 \pmod{20}$. Получим новую систему, равносильную исходной:

$$\begin{cases} x\equiv 11 \pmod{20} \\ x\equiv 2 \pmod{13} \end{cases}.$$

Решим ее аналогичным способом. Из первого сравнения имеем:

$$x=20t+11;$$

подставим это значение x во второе сравнение:

$$20t+11\equiv 2 \pmod{13},$$

Откуда находим

$$20t\equiv -9 \pmod{13};\quad 7t\equiv -9 \pmod{13};\quad 7t\equiv -35 \pmod{13};$$

$$t\equiv -5 \pmod{13};\quad t\equiv 8 \pmod{13}.$$

Тогда $t=13q+8$, и поэтому

$$x=20t+11=20(13q+8)+11=260q+171.$$

Следовательно, все решения исходной системы образуют один класс чисел по модулю 260:

$$x\equiv 171 \pmod{260}.$$

Ответ: $x\equiv 171 \pmod{260}$.

Задача 8. Решите сравнение, используя простейшие свойства сравнений:

$$381x \equiv 3 \pmod{71}.$$

Решение. Сначала упростим сравнение, заменив в нем коэффициент 381 остатком от деления на модуль 71. Получим сравнение, равносильное данному:

$$26x \equiv 3 \pmod{71}.$$

Здесь $НОД(a,m) = НОД(26,71) = 1$, следовательно, сравнение имеет единственное решение. Найдем его:

$$26x - 71x \equiv 3 \pmod{71},$$

$$-45x \equiv 3 \pmod{71} \mid :3,$$

$$-15x \equiv 1 \pmod{71},$$

$$-15x \equiv 1 - 71 \pmod{71},$$

$$-15x \equiv -70 \pmod{71} \mid :(-5),$$

$$3x \equiv 14 - 71 \pmod{71},$$

$$3x \equiv -57 \pmod{71} \mid :3,$$

$$x \equiv -19 \pmod{71}.$$

Упростим полученный ответ:

$$x \equiv -19 + 71 \pmod{71},$$

$$x \equiv 52 \pmod{71}.$$

Ответ: $x \equiv 52 \pmod{71}$.

Задача 9. Решите сравнение, используя простейшие свойства сравнений:

$$47x \equiv 56 \pmod{93}.$$

Решение. Обе части сравнения умножим на число 2. Обращаем внимание на то, что это число взаимно просто с модулем $m = 93$, поэтому получим сравнение, равносильное данному:

$$47x \equiv 56 \pmod{93} \ |\times 2, \quad НОД(2,93) = 1,$$

$$94x \equiv 112 \pmod{93},$$

$$94x - 93x \equiv 112 \pmod{93},$$

$$x \equiv 112 \pmod{93},$$

$$x \equiv 112 - 93 \pmod{93},$$

$$x \equiv 19 \pmod{93}.$$

Ответ: $x \equiv 19 \pmod{93}$.

Задачи для самостоятельного решения

Задача 1. Выясните, какие из следующих сравнений являются верными:

1) $1 \equiv -6 \pmod{7}$;

2) $572 \equiv 0 \pmod{13}$;

3) $2^5 \equiv 1 \pmod{4}$;

4) $325 \equiv 762 \pmod{19}$;

5) $3m \equiv -1 \pmod{m}$.

Задача 2. Докажите, что следующие сравнения являются верными:

1) $121 \equiv 13145 \pmod{2}$;

2) $121347 \equiv 92817 \pmod{10}$;

3) $52 \equiv -8 \pmod{10}$;

4) $(m-1)^2 \equiv 1 \pmod{m}$;

5) $2m+1 \equiv (m+1)^2 \pmod{m}$.

Задача 3. Докажите, что если $3^k \equiv -1 \pmod{10}$, где $k \in \mathbb{N}$, то $3^{k+4} \equiv -1 \pmod{10}$.

Задача 4. Известно, что $a^{100} \equiv 5 \pmod{7}$ и $a^{101} \equiv 45 \pmod{7}$. Найдите остаток от деления числа a на 7.

Задача 5. Найдите остаток от деления:

1) 3^{20} на 10;

2) 5^{32} на 9;

3) 3^{812} на 25;

4) 13^{479} на 15;

5) 19^{400} на 78.

Задача 6. Найдите значение функции Эйлера $\varphi(n)$ для $n = 81,\ 97,\ 125,\ 226,\ 4356$.

Задача 7. Выясните, какие из сравнений имеют решения, и решите их, используя лишь простейшие свойства сравнений:

1) $5x \equiv 3 \pmod{17}$;

2) $7x \equiv 15 \pmod{9}$;

3) $8x \equiv 7 \pmod{14}$;

4) $18x \equiv 15 \pmod{69}$;

5) $27x \equiv 9 \pmod{15}$;

6) $21x + 5 \equiv 0 \pmod{29}$.

Задача 8. Исследуйте и решите сравнения, используя рекуррентную формулу:

1) $5286x \equiv 225 \pmod{849}$;

2) $4172x \equiv 344 \pmod{676}$;

3) $4305x \equiv 935 \pmod{830}$.

4) $23579x \equiv 365 \pmod{1275}$.

Задача 9. Решите системы сравнений:

1) $\begin{cases} x \equiv 2 \pmod{15} \\ x \equiv 18 \pmod{22} \end{cases}$;

2) $\begin{cases} x \equiv 38 \pmod{5} \\ x \equiv 17 \pmod{4} \\ x \equiv 2 \pmod{11} \end{cases}$;

3) $\begin{cases} x \equiv 5 \pmod{26} \\ x \equiv 12 \pmod{35} \\ x \equiv 14 \pmod{69} \end{cases}$;

4) $\begin{cases} 4x \equiv 3 \pmod{7} \\ 5x \equiv 4 \pmod{6} \end{cases}$;

5) $\begin{cases} 5x \equiv 20 \pmod{6} \\ 6x \equiv 6 \pmod{5} \\ 4x \equiv 5 \pmod{77} \end{cases}$;

6) $\begin{cases} 7x \equiv 10 \pmod{26} \\ 9x \equiv 17 \pmod{35} \\ 5x \equiv 13 \pmod{69} \end{cases}$.

Задача 10. Известно, что $12 \equiv a \pmod{10}$. Укажите верные и неверные утверждения:

1) $12 = 10a + r$, $0 \le r < 10$;

2) $2 \equiv a \pmod{10}$;

3) $(a-2) \vdots 5$;

4) $a \vdots 2$;

5) $\exists t \in \mathbb{Z} \mid 12 = 10t + a$.

§ 3. КОЛЬЦА И ПОЛЯ КЛАССОВ ВЫЧЕТОВ

3.1. Классы вычетов по модулю m

Пусть m - данное натуральное число.

Определение. Класс всех целых чисел, сравнимых с числом a по модулю m, называют *классом вычетов по модулю* m и обозначают $[a]_m$ или $\overline{a}$.

В силу определения верно:

$$[a]_m = [b]_m \quad \Leftrightarrow \quad a \equiv b (\mathrm{mod}\, m).$$

Множество всех классов вычетов по модулю m обозначают $\mathbb{Z}/m$. Так как различные остатки при делении на m исчерпываются числами 0, 1, 2, … , $m-1$, то получим m классов:

$$\mathbb{Z}/m = \{[0]_m, [1]_m, [2]_m, \ldots, [m-1]_m\}.$$

3.2. Кольцо классов вычетов

Определим на множестве $\mathbb{Z}/m$ операции сложения и умножения следующим образом. Положим:

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

Введенные операции обладают свойствами:

1) $([a]_m + [b]_m) + [c]_m = [a]_m + ([b]_m + [c]_m)$

2) $[a]_m + [b]_m = [b]_m + [a]_m$

3) Класс $[0]_m$ является нейтральным элементом относительно операции сложения.

4) Для любого $[a]_m$ класс $[-a]_m$ является противоположным элементом.

5) $([a]_m \cdot [b]_m) \cdot [c]_m = [a]_m \cdot ([b]_m \cdot [c]_m)$

6) $[a]_m \cdot [b]_m = [b]_m \cdot [a]_m$

7) $([a]_m + [b]_m) \cdot [c]_m = [a]_m \cdot [c]_m + [b]_m \cdot [c]_m$

8) Класс $[1]_m$ является нейтральным элементом относительно операции умножения.

В силу свойств 1-8 верно следующее утверждение.

Теорема. *Множество $\mathbb{Z}/m$ всех классов вычетов по модулю m с определенными выше операциями сложения и умножения является коммутативным кольцом с единицей.*

Кольцо $\mathbb{Z}/m$ называют *кольцом классов вычетов по модулю m.*

Замечание. На практике в целях упрощения записей часто вместо кольца классов вычетов $\mathbb{Z}/m$ используют изоморфное ему кольцо $\mathbb{Z}_m$, элементами которого являются наименьшие неотрицательные представители $0, 1, 2, \ldots, m-1$ каждого класса. При этом под операциями сложения и умножения понимают обычные арифметические операции над числами с последующей заменой результата остатком от деления на m. Кольцо $\mathbb{Z}_m$ называют *кольцом вычетов по модулю m.*

3.3. Поля классов вычетов

Укажем условия, при которых кольцо $\mathbb{Z}/m$ является полем. Для этого сначала опишем обратимые элементы этого кольца.

Теорема. *В кольце $\mathbb{Z}/m$ элемент $[a]_m \neq [0]_m$ обратим тогда и только тогда, когда $НОД(a, m) = 1$, т.е. когда класс $[a]_m$ взаимно прост с модулем m.*

Следствие. *Ненулевой элемент* $[a]_m$ *кольца* $\mathbb{Z}/m$ *является делителем нуля тогда и только тогда, когда* $НОД(a,m) \neq 1$.

Выше (см. п.3.2) было показано, что множество $\mathbb{Z}/m$ всех классов вычетов по модулю m является коммутативным кольцом с единицей. Укажем, когда это кольцо будет полем.

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

Это поле называют *полем вычетов по модулю* m.

Решение типовых задач

Задача 1. Укажите, из каких элементов состоит кольцо $\mathbb{Z}/10$. Выпишите множества всех обратимых элементов и всех делителей нуля этого кольца. Для каждого обратимого элемента найдите обратный.

Решение. Кольцо $\mathbb{Z}/10$ состоит из 10 классов, которые соответствуют различным остаткам от деления целых чисел на модуль 10:

$$\mathbb{Z}/10 = \left\{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3}, \ldots,\ \overline{9}\right\}.$$

Выясним, какие из этих классов обратимы. В силу теоремы п.3.3 класс $\overline{a}$ обратим тогда и только тогда, когда он взаимно прост с модулем $m = 10$. Следовательно, имеется $\varphi(10) = 4$ таких класса и множество всех обратимых элементов кольца $\mathbb{Z}/10$ имеет вид:

$$\mathbb{Z}_{10}^{*} = \left\{\overline{1},\ \overline{3}, \overline{7}, \overline{9}\right\}.$$

Тогда все остальные классы, кроме нулевого, являются делителями нуля: $\left\{\overline{2},\ \overline{4}, \overline{5}, \overline{6}, \overline{8}\right\}$.

Для каждого обратимого класса найдем обратный. Для отыскания класса $\overline{a}^{-1}=\overline{x}$ надо решить уравнение $\overline{a}\cdot\overline{x}=\overline{1}$ в кольце $\mathbb{Z}/10$. Или, в терминах сравнений, найти $\overline{a}^{-1}$ - это значит решить сравнение $ax\equiv 1\ (\mathrm{mod}\ 10)$.

Для класса $\overline{1}$ имеем:

$$1\cdot x\equiv 1\ (\mathrm{mod}\ 10)\ \Rightarrow\ \left(\overline{1}\right)^{-1}=\overline{1}.$$

Для класса $\overline{3}$:

$$3x\equiv 1(\mathrm{mod}\ 10)\ \Rightarrow\ 3x\equiv 1-10(\mathrm{mod}\ 10)\ \Big|\ :3\ \Rightarrow$$

$$\Rightarrow x\equiv -3(\mathrm{mod}\ 10)\ \Rightarrow\ x\equiv 7(\mathrm{mod}\ 10)\ \Rightarrow$$

$$\Rightarrow\left(\overline{3}\right)^{-1}=\overline{7}.$$

Последнее равенство означает, что $\overline{3}\cdot\overline{7}=\overline{1}$. Следовательно,

$$\left(\overline{7}\right)^{-1}=\overline{3}.$$

Для класса $\overline{9}$ имеем:

$$9x\equiv 1(\mathrm{mod}\ 10)\ \Rightarrow\ 9x\equiv 1-10(\mathrm{mod}\ 10)\ \Big|\ :9\ \Rightarrow$$

$$\Rightarrow\ x\equiv -1(\mathrm{mod}\ 10)\ \Rightarrow\ x\equiv 9\ (\mathrm{mod}\ 10)\ \Rightarrow$$

$$\Rightarrow\left(\overline{9}\right)^{-1}=\overline{9}\quad\text{(элемент обратен себе).}$$

Ответ: множество обратимых элементов $\mathbb{Z}_{10}^{*}=\left\{\overline{1},\ \overline{3},\overline{7},\overline{9}\right\}$,

множество делителей нуля $\left\{\overline{2},\ \overline{4},\overline{5},\overline{6},\overline{8}\right\}$;

$\left(\overline{1}\right)^{-1}=\overline{1}$, $\left(\overline{3}\right)^{-1}=\overline{7}$, $\left(\overline{7}\right)^{-1}=\overline{3}$, $\left(\overline{9}\right)^{-1}=\overline{9}$.

Задача 2. В кольце классов вычетов $\mathbb{Z}/117$ найдите сумму, произведение и обратные (если они существуют) для классов $\overline{a} = \overline{248}$ и $\overline{b} = \overline{-416}$.

Решение. Сначала упростим данные классы:

$$\overline{a} = \overline{248} = \overline{248 - 2 \cdot 117} = \overline{14},$$

$$\overline{b} = \overline{-416} = \overline{-416 + 4 \cdot 117} = \overline{52}.$$

Найдем сумму классов:

$$\overline{a} + \overline{b} = \overline{14} + \overline{52} = \overline{66}.$$

Найдем произведение классов:

$$\overline{a} \cdot \overline{b} = \overline{14} \cdot \overline{52} = \overline{728} = \overline{728 - 6 \cdot 117} = \overline{26}.$$

Выясним, существуют ли для данных классов обратные. Так как

$$\text{НОД}(a, m) = \text{НОД}(14, 117) = 1$$

и

$$\text{НОД}(b, m) = \text{НОД}(52, 117) = 13,$$

то класс $\overline{a}$ взаимно прост с модулем, а класс $\overline{b}$ не является взаимно простым с модулем. Следовательно, в силу теоремы п.3.3 класс вычетов $\overline{a}$ обратим, а класс $\overline{b}$ не имеет обратного.

Для класса $\overline{a} = \overline{14}$ найдем обратный элемент $\overline{a}^{-1}$. Для этого решим сравнение $ax \equiv 1 \pmod{117}$, т. е.

$$14x \equiv 1 \pmod{117}.$$

Воспользуемся рекуррентной формулой (см. п.2.3). Применим алгоритм Евклида к числам 14, 117 и найдем последовательность неполных частных: $q_1 = 8$, $q_2 = 2$, $q_3 = 1$. По ним,

пользуясь формулой $V_k = V_{k-2} - V_{k-1}q_k \quad (k = 2,3)$, найдем число $V = V_3$. Результаты вычислений запишем в таблицу:

k	0	1	2	3
q_k	–	8	2	1
V_k	1	–8	17	$-25 = V$

Теперь по формуле $x \equiv bV \pmod m$ найдем решение сравнения $14x \equiv 1 \pmod{117}$:

$$x \equiv -25 \pmod{117},$$

или после упрощения: $x \equiv -25 + 117 \pmod{117}$,

$$x \equiv 92 \pmod{117}.$$

Таким образом, для класса $\overline{a} = \overline{14}$ найден обратный элемент $(\overline{a})^{-1} = \overline{92}$.

Ответ: $\overline{a} + \overline{b} = \overline{66}$, $\overline{a}\overline{b} = \overline{26}$, $(\overline{a})^{-1} = \overline{92}$, $\overline{b}^{-1}$ не существует.

Задача 3. В кольце $\mathbb{Z}/5$ решить уравнение $\overline{3} \cdot x = \overline{4}$.

Решение. Решение данного уравнения $\overline{3} \cdot x = \overline{4}$ имеет вид $x = \overline{4} \cdot (\overline{3})^{-1}$, причем класс $x = (\overline{3})^{-1}$ существует, так как кольцо $\mathbb{Z}/5$ является полем и поэтому все его ненулевые элементы обратимы.

Найдем элемент $(\overline{3})^{-1}$. Для этого решим сравнение $3x \equiv 1 (\mathrm{mod}\, 5)$. Используя свойства сравнений, имеем:

$$3x \equiv 1 (\mathrm{mod}\, 5), \qquad 3x \equiv 6 (\mathrm{mod}\, 5), \qquad x \equiv 2 (\mathrm{mod}\, 5).$$

Следовательно, $(\overline{3})^{-1} = \overline{2}$. Теперь найдем решение данного уравнения: $x = \overline{4} \cdot (\overline{3})^{-1} = \overline{4} \cdot \overline{2} = \overline{8} = \overline{8-5} = \overline{3}$.

Ответ: $x = \overline{3}$.

Задача 4. Для матрицы $A=\begin{pmatrix}3 & 2\\ 1 & 6\end{pmatrix}$ над полем $\mathbb{Z}_7$ найдите обратную матрицу A^{-1}. Сделайте проверку.

Решение. Для нахождения обратной матрицы воспользуемся формулой $A^{-1}=\frac{1}{|A|}\tilde{A}$, где $\tilde{A}=\begin{pmatrix}A_{11} & A_{21}\\ A_{12} & A_{22}\end{pmatrix}$.

Найдем определитель данной матрицы:

$$|A|=\begin{vmatrix}3 & 2\\ 1 & 6\end{vmatrix}=18-2=16\equiv 2(\mathrm{mod}\,7).$$

Вычислим алгебраические дополнения к элементам матрицы:

$$A_{11}=6,\quad A_{12}=-1\equiv 6(\mathrm{mod}\,7),$$

$$A_{21}=-2\equiv 5(\mathrm{mod}\,7),\quad A_{22}=3.$$

Тогда

$$A^{-1}=\frac{1}{|A|}\tilde{A}=\frac{1}{2}\begin{pmatrix}6 & 5\\ 6 & 3\end{pmatrix}=\begin{pmatrix}3 & 5\cdot 2^{-1}\\ 3 & 3\cdot 2^{-1}\end{pmatrix}.$$

Найдем элемент 2^{-1}. Для этого решим сравнение $2x\equiv 1(\mathrm{mod}\,7)$. Имеем:

$$2x\equiv 1(\mathrm{mod}\,7)\Leftrightarrow 2x\equiv 1+7(\mathrm{mod}\,7)\,|:2\Leftrightarrow x\equiv 4(\mathrm{mod}\,7).$$

Таким образом, $2^{-1}=4$; откуда находим

$$5\cdot 2^{-1}=20\equiv 6(\mathrm{mod}\,7),\quad 3\cdot 2^{-1}=12\equiv 5(\mathrm{mod}\,7).$$

Окончательно получаем:

$$A^{-1}=\begin{pmatrix}3 & 5\cdot 2^{-1}\\ 3 & 3\cdot 2^{-1}\end{pmatrix}=\begin{pmatrix}3 & 6\\ 3 & 5\end{pmatrix}.$$

Сделаем проверку, т. е. покажем, что $AA^{-1} = E$. Имеем

$$AA^{-1} = \begin{pmatrix} 3 & 2 \\ 1 & 6 \end{pmatrix} \cdot \begin{pmatrix} 3 & 6 \\ 3 & 5 \end{pmatrix} = \begin{pmatrix} 15 & 28 \\ 21 & 36 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 7.$$

Ответ: $A^{-1} = \begin{pmatrix} 3 & 6 \\ 3 & 5 \end{pmatrix}$.

Задачи для самостоятельного решения

Задача 1. Выпишите множества всех элементов, всех обратимых элементов и всех делителей нуля кольца $\mathbb{Z}/28$. Для каждого обратимого элемента найдите обратный.

Задача 2. В кольце классов вычетов $\mathbb{Z}/91$ найдите сумму, произведение и обратные (если они существуют) для классов:

1) $\overline{a} = \overline{496}$, $\overline{b} = \overline{205}$;
2) $\overline{a} = \overline{508}$, $\overline{b} = \overline{327}$;
3) $\overline{a} = \overline{-306}$, $\overline{b} = \overline{417}$;
4) $\overline{a} = \overline{251}$, $\overline{b} = \overline{473}$.

Задача 3. Для данной матрицы A над заданым полем вычетов $\mathbb{Z}_p$ найдите обратную матрицу A^{-1}. Сделайте проверку.

1) $A = \begin{pmatrix} 5 & 3 \\ 4 & 6 \end{pmatrix}$ над $\mathbb{Z}_7$;
2) $A = \begin{pmatrix} 2 & 5 \\ 1 & 4 \end{pmatrix}$ над $\mathbb{Z}_{11}$;
3) $A = \begin{pmatrix} 8 & 7 \\ 3 & 5 \end{pmatrix}$ над $\mathbb{Z}_{13}$;
4) $A = \begin{pmatrix} 7 & 5 \\ 1 & 3 \end{pmatrix}$ над $\mathbb{Z}_{11}$.

Задача 4. Вычислите $f(3)$ для многочлена

$$f(x) = x^{214} + 3x^{152} + 2x^{47} + 2 \in \mathbb{Z}_5[x].$$

Тестовые задания для итогового контроля

Вариант 1

1. Сравнение $x \equiv 2 \pmod 9$ равносильно равенству (при любом $k \in \mathbb{Z}$):

1) $x = 2k + 9$; 2) $x = 9k + 2$; 3) $x = 9k$; 4) $x = 2k + 7$.

2. Решение сравнения $25x \equiv 1 (\mathrm{mod} 19)$ имеет вид:

1) $x \equiv 16 (\mathrm{mod}\, 38)$; 2) $x \equiv 8 (\mathrm{mod} 19)$;

3) $x \equiv 16 (\mathrm{mod} 19)$; 4) $x \equiv 2 (\mathrm{mod} 19)$.

3. Укажите, сколько решений имеет сравнение

$$2871x \equiv 231 \pmod{258}$$

1) 2; 2) 3; 3) 1; 4) нет решений.

4. Обратимыми элементами кольца вычетов $\mathbb{Z}_{26}$ являются:

1) 3, 9, 12; 2) 1, 2, 13; 3) 7, 9, 15; 4) 1, 16, 25.

5. В кольце классов вычетов $\mathbb{Z}/91$ для класса [508] укажите обратный:

1) [12]; 2) [6]; 3) [79]; 4) [72].

6. Укажите, какие из колец вычетов являются полями:

$$\mathbb{Z}_8,\ \mathbb{Z}_{15},\ \mathbb{Z}_{19},\ \mathbb{Z}_{53},\ \mathbb{Z}_{103}.$$

7. Для матрицы $A = \begin{pmatrix} 2 & 5 \\ 1 & 4 \end{pmatrix}$ над полем $\mathbb{Z}_{11}$ обратная матрица A^{-1} имеет вид:

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

8. Укажите верные и неверные утверждения ($a, q \in \mathbb{Z}$):

1) Если $a = 6q - 3$, то остаток при делении a на 6 равен 3.

2) Если $a = 6q - 2$, то остаток при делении a на 6 равен 2.

3) Если $a = 6q - 10$, то остаток при делении a на 6 равен 2.

Вариант 2

1. Сравнение $x \equiv 2 \pmod 7$ равносильно равенству (при любом $k \in \mathbb{Z}$):

1) $x = 2k + 7$; 2) $x = 7k + 2$; 3) $x = 9k$; 4) $x = 5k + 2$.

2. Решение сравнения $13x \equiv 4 (\mathrm{mod} 17)$ имеет вид:

1) $x \equiv 8 (\mathrm{mod} 17)$; 2) $x \equiv 16 (\mathrm{mod}\, 34)$;

3) $x \equiv 16 (\mathrm{mod} 17)$; 4) $x \equiv 4 (\mathrm{mod} 17)$.

3. Укажите, сколько решений имеет сравнение

$$2415x \equiv 114 \pmod{429}$$

1) 1; 2) 2; 3) 3; 4) нет решений.

4. Обратимыми элементами кольца вычетов $\mathbb{Z}_{28}$ являются:

1) 1, 9, 17; 2) 1, 4, 7; 3) 2, 7, 16; 4) 1, 8, 27.

5. В кольце классов вычетов $\mathbb{Z}/91$ для класса $[-306]$ укажите обратный:

1) [17]; 2) [46]; 3) [89]; 4) [11].

6. Укажите, какие из колец вычетов являются полями:

$$\mathbb{Z}_6,\ \mathbb{Z}_{17},\ \mathbb{Z}_{29},\ \mathbb{Z}_{35},\ \mathbb{Z}_{97}.$$

7. Для матрицы $A = \begin{pmatrix} 4 & 5 \\ 2 & 3 \end{pmatrix}$ над полем $\mathbb{Z}_7$ обратная матрица A^{-1} имеет вид:

1) $\begin{pmatrix} 6 & 2 \\ 1 & 4 \end{pmatrix}$; 2) $\begin{pmatrix} 3 & 4 \\ 2 & 1 \end{pmatrix}$; 3) $\begin{pmatrix} 2 & 6 \\ 1 & 3 \end{pmatrix}$; 4) $\begin{pmatrix} 5 & 1 \\ 6 & 2 \end{pmatrix}$.

8. Пусть $НОД(a+b, 2a) = d$, где a и b - данные натуральные числа. Укажите верные и неверные утверждения:

1) $d = НОД(a, b)$;

2) $d = НОД(2a, a - b)$;

3) $d = 2НОД(a, b)$.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Глухов М.М.* Алгебра / М.М. Глухов, В.П. Елизаров, А.А. Нечаев. В 2 т. – М.: Гелиос АРВ, 2003.

2. *Глухов М.М.* Алгебра и аналитическая геометрия / М.М. Глухов. – М.: Гелиос АРВ, 2005.

3. *Куликов Л.Я.* Алгебра и теория чисел / Л.Я. Куликов. – М.: Высш. шк., 1979.

4. *Виноградов И.М.* Основы теории чисел / И.М. Виноградов. – М.: Наука, 1965.

5. *Майорова С.П.* Алгебра: учеб. пособие / С.П. Майорова, М.Г. Завгородний. – Воронеж: ГОУВПО «Воронежский государственный технический университет», 2007. Часть 2.

6. *Майорова С.П.* Практикум по алгебре / С.П. Майорова, М.Г. Завгородний. – Воронеж: ВГТУ, 2006.

СОДЕРЖАНИЕ

ЭЛЕМЕНТЫ ТЕОРИИ СРАВНЕНИЙ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
для организации самостоятельной работы
по курсу «Алгебра» для студентов
специальностей 090102, 090105
очной формы обучения

Составитель
Майорова Светлана Павловна

В авторской редакции

Компьютерный набор С.П. Майоровой

Подписано в печать 2.12.2008.
Формат 60x84/16. Бумага для множительных аппаратов.
Усл. печ. л. 2,9. Уч.-изд. л. 2,7. Тираж 60 экз. «С»
Заказ №

ГОУВПО «Воронежский государственный
технический университет»
394026 Воронеж, Московский просп., 14