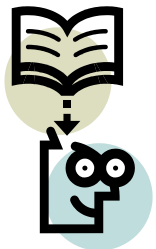
Федеральное государственное бюджетное образовательное
учреждение высшего профессионального образования
«Сахалинский государственный университет»

О. А. Гущина, Т. А. Неешпапа

СРАВНЕНИЯ В КОЛЬЦЕ ЦЕЛЫХ ЧИСЕЛ

Учебно-методическое пособие



Южно-Сахалинск
Издательство СахГУ
2012

УДК 512(075.4)
ББК 22.144я78
Г 98

Печатается по решению учебно-методического совета Сахалинского государственного университета, 2012 г.

Рецензент:
Федоров О. А., *кандидат педагогических наук, доцент, декан факультета математики, физики и информатики СахГУ.*

Г 98 **Гущина, О. А. Сравнения в кольце целых чисел** : учебно-методическое пособие / О. А. Гущина, Т. А. Неешпапа. – Южно-Сахалинск : изд-во СахГУ, 2012. – 96 с.
ISBN 978-5-88811-412-4

Учебно-методическое пособие представляет собой специальный курс по одному из разделов теории чисел – теории сравнений. Пособие рекомендовано для студентов математических специальностей и направлений высших учебных заведений, в частности специальностей «Прикладная математика и информатика», «Педагогическое образование: профиль – математика». Приводятся задания для самоконтроля и самостоятельного решения. Данное учебно-методическое пособие может служить для проведения практических занятий, организации самостоятельной работы и дистанционного обучения студентов.

УДК 512(075.4)
ББК 22.144я78

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

Теория чисел – это наука о целых числах. Целые числа и операции над ними известны еще с древнейших времен и являются одними из первых математических абстракций. Теория сравнений в кольце целых чисел – один из разделов теории чисел. Существуют различные учебные пособия по теории чисел, но ни одно из них не содержит достаточно подробно изложенной теории сравнений. Практика работы в высшем учебном заведении показала потребность в учебном пособии, которое помогло бы студенту более подробно и доступно познакомиться с теорией сравнений в кольце целых чисел как под руководством преподавателя, так и самостоятельно. Данное издание – одна из попыток создания такого пособия.

Предлагаемое учебно-методическое пособие знакомит читателя с важнейшими понятиями теории сравнений в кольце целых чисел.

Цель данного пособия – просто и доходчиво на конкретных примерах изложить основные методы и приемы теории сравнений в кольце целых чисел.

В пособии рассмотрены такие темы, как свойства сравнений, функция Эйлера, линейные сравнения, системы линейных сравнений, степенные сравнения, квадратичные вычеты, арифметические приложения теории сравнений.

Весь материал пособия разбит на отдельные темы. Каждый факт теории проиллюстрирован примерами. По каждой теме приведены вопросы для самоконтроля. В конце пособия приведены задания для самостоятельного решения. Доказательства теорем завершаются знаком ■.

Авторы

1. СРАВНЕНИЯ В КОЛЬЦЕ ЦЕЛЫХ ЧИСЕЛ

Рассмотрим множество $\boldsymbol{Z}$ целых чисел. Известно, что при делении любого целого числа на натуральное число n получается в остатке одно из чисел множества $A_n = \{0;1;2;...;n-1\}$. Все множество целых чисел можно разбить на следующие подмножества $Z_0 = \{n \cdot t / t \in Z\}$, $Z_1 = \{n \cdot t + 1 / t \in Z\}$,..., $Z_{n-1} = \{n \cdot t + (n-1) / t \in Z\}$. Т. к. полученные множества являются непустыми, попарно не пересекаются и в объединении дают множество $\boldsymbol{Z}$, то они образуют разбиение множества $\boldsymbol{Z}$ целых чисел на классы. Причем эти множества обладают одним замечательным свойством: разность любых двух чисел, принадлежащих одному классу, делится на n. Действительно, если $a \in Z_k, b \in Z_k$, т. е. $a = nt + k$ $(t \in Z)$ и $b = nl + k$ $(l \in Z)$, то $a - b = n(t - l)$, что означает $(a-b) \vdots n$ (символ $\vdots$ означает, что разность $(a-b)$ делится на n).

ОПРЕДЕЛЕНИЕ. Целые числа a и b называются сравнимыми по модулю n $(n \geq 2)$, если разность их делится на n.

Запись $a \equiv b (\mathrm{mod}\, n)$ или $a \equiv b (n)$ называют сравнением и читают: a сравнимо с b по модулю n. Здесь a – левая часть сравнения, b – правая часть сравнения, n – модуль сравнения.

Из определения следует, что $a \equiv 0 (\mathrm{mod}\, n) \Leftrightarrow a \vdots n$.

Примеры.

Следующие сравнения истинны: $4 \equiv 13 (\mathrm{mod}\, 3)$, т. к. $4 - 13 = -9 = 3 \cdot (-3)$;

$21 \equiv -34 (\mathrm{mod}\, 11)$, т. к. $21 - (-34) = 55 \vdots 11$;

$28 \equiv 67 (\mathrm{mod}\, 13)$, т. к. $28 = 13 \cdot 2 + 2, 67 = 13 \cdot 5 + 2$ и $2 = 2$.

Следующие сравнения ложны:

$12 \equiv 134 (\mathrm{mod}\, 4)$, т. к. $12 - 134 = -122 = 4 \cdot (-30{,}5)$ и $-30{,}5 \notin Z$;

$-35 \equiv 68 (\mathrm{mod}\, 17)$, т. к. $-35 = 17 \cdot (-3) + 16$, $68 = 17 \cdot 4$ и $16 \neq 0$.

Как показано выше, $(a-b):n$, если числа a и b принадлежат одному классу Z_k. Следовательно, числа a и b сравнимы по модулю n, если при делении чисел a и b на n получаются равные остатки.

Действительно, пусть $a=nq+r_a, 0\le r_a\le n-1$ и $b=np+r_b, 0\le r_b\le n-1$. Т. к. из того, что $a\equiv b(\mathrm{mod}\,n)$, следует по определению $(a-b):n$ и $n(q-p):n$, то $(r_a-r_b):n$. Из условий для остатков r_a, r_b получаем: $-(n-1)\le(r_a-r_b)\le n-1$, т. е. (r_a-r_b) – целое число из промежутка $(1-n;n-1)$. Причем $(r_a-r_b):n$, а это возможно только, если $(r_a-r_b)=0$. В итоге имеем $r_a=r_b$.

Верно и обратное утверждение: остатки при делении двух целых чисел на n равны, если $a\equiv b(\mathrm{mod}\,n)$.

Свойства сравнений.

СВОЙСТВО 1. Для любого целого числа a и любого $n\ge 2$ справедливо $a\equiv a(\mathrm{mod}\,n)$.

Доказательство. Т. к. $a-a=0$ и $0:n, n\ne 0$, то $(a-a):n\Rightarrow a\equiv a(\mathrm{mod}\,n)$.

Примеры.

$5\equiv 5(\mathrm{mod}\,6); 5\equiv 5(\mathrm{mod}1367); -354\equiv -354(\mathrm{mod}1786); 0\equiv 0(\mathrm{mod}\,56)$.

СВОЙСТВО 2. Для любых целых чисел a и b, любого $n\ge 2$ из того, что $a\equiv b(\mathrm{mod}\,n)$, следует $b\equiv a(\mathrm{mod}\,n)$.

Доказательство. Т. к. $a\equiv b(\mathrm{mod}\,n)$, по определению имеем $(a-b):n$, т. е. существует такое целое число $t\in Z$, что справедливо равенство $a-b=nt$. Тогда $b-a=-(a-b)=-(nt)=n(-t)$, что означает $(b-a):n$, следовательно, $b\equiv a(\mathrm{mod}\,n)$.

СВОЙСТВО 3. Для любых целых чисел a, b и c, любого $n\ge 2$ из справедливости сравнений $a\equiv b(\mathrm{mod}\,n)$ и $b\equiv c(\mathrm{mod}\,n)$ следует справедливость сравнения $a\equiv c(\mathrm{mod}\,n)$.

Доказательство. Рассмотрим разность $a-c=a-b+b-c=(a-b)+(b-c)$. В силу того, что $a\equiv b(\mathrm{mod}\,n)$, имеем $(a-b):n$, аналогично из сравнения $b\equiv c(\mathrm{mod}\,n)$ следует $(b-c):n$. По свойству делимости имеем $(a-c):n$, откуда $a\equiv c(\mathrm{mod}\,n)$.

СВОЙСТВО 4. Для любых целых чисел a,b,c,d и любого $n \geq 2$ из того, что истинны сравнения $a \equiv b(\mathrm{mod}\, n)$ и $c \equiv d(\mathrm{mod}\, n)$, следует истинность сравнения $a+c \equiv b+d(\mathrm{mod}\, n)$.

Доказательство. Разность $(a+c)-(b+d)$ делится на n, т. к. $(a+c)-(b+d)=(a-b)+(c-d)$ – сумма двух целых чисел, делящихся на n.

Следствие 1. Если $a \equiv b(\mathrm{mod}\, n)$ и $c \equiv d(\mathrm{mod}\, n)$, то $a-c \equiv b-d(\mathrm{mod}\, n)$.

Следствие 2. Из того, что $a \equiv b(\mathrm{mod}\, n)$, следует $a-b \equiv 0(\mathrm{mod}\, n)$.

Следствие 3. Если $a \equiv b(\mathrm{mod}\, n)$ и $c \in Z$, то $a \pm c \equiv b \pm c(\mathrm{mod}\, n)$.

Следствие 4. Если $a \equiv b(\mathrm{mod}\, n)$ и $k,t \in Z$, то $a \pm k \cdot n \equiv b \pm t \cdot n(\mathrm{mod}\, n)$.

Пример.

$$\begin{cases} 137 \equiv 46(\mathrm{mod}13) \\ -214 \equiv -45(\mathrm{mod}13) \end{cases} \Rightarrow (137+(-214)) \equiv (46+(-45))(\mathrm{mod}13) \Rightarrow -77 \equiv 1(\mathrm{mod}13).$$

СВОЙСТВО 5. Для любых целых чисел a,b,c,d и любого $n \geq 2$ из того, что истинны сравнения $a \equiv b(\mathrm{mod}\, n)$ и $c \equiv d(\mathrm{mod}\, n)$, следует истинность сравнения $ac \equiv bd(\mathrm{mod}\, n)$.

Доказательство. Имеем $ac-bd = ac-bc+bc-bd = c(a-b)+b(c-d)$.

Следовательно, $(ac-bd) \vdots n$, т. е. $ac \equiv bd(\mathrm{mod}\, n)$.

Следствие 1. Из того, что $a \equiv b(\mathrm{mod}\, n)$ и k – целое число, следует $ak \equiv bk(\mathrm{mod}\, n)$.

Следствие 2. Из того, что $a \equiv b(\mathrm{mod}\, n)$ и k – натуральное число, следует $a^k \equiv b^k(\mathrm{mod}\, n)$.

Пример.

$$\begin{cases} 12 \equiv -13(\mathrm{mod}5) \\ -14 \equiv 16(\mathrm{mod}5) \end{cases} \Rightarrow (12 \cdot (-14)) \equiv ((-13) \cdot 16)(\mathrm{mod}13) \Rightarrow -168 \equiv -208(\mathrm{mod}5).$$

СВОЙСТВО 6. Для любых целых чисел a и b, любого $n \geq 2$ из того, что $a \equiv b(\mathrm{mod}\, n)$ и $n \vdots n_1$, $n_1 \geq 2$, следует $a \equiv b(\mathrm{mod}\, n_1)$.

Доказательство. Из сравнения $a \equiv b(\mathrm{mod}\, n)$ по определению имеем, $(a-b) \vdots n$. Т. к. $n \vdots n_1$, то $(a-b) \vdots n_1$, следовательно, $a \equiv b(\mathrm{mod}\, n_1)$.

Пример.

$$\begin{cases} 143 \equiv 353 (\mathrm{mod}\, 210) \\ 210 = 2 \cdot 3 \cdot 5 \cdot 7 \end{cases} \Rightarrow 143 \equiv 353 (\mathrm{mod}\, 2),\ 143 \equiv 353 (\mathrm{mod}\, 3),\ 143 \equiv 353 (\mathrm{mod}\, 5),$$
$$143 \equiv 353 (\mathrm{mod}\, 7),\ 143 \equiv 353 (\mathrm{mod}\, 6),\ 143 \equiv 353 (\mathrm{mod}\, 10),\ 143 \equiv 353 (\mathrm{mod}\, 14),$$
$$143 \equiv 353 (\mathrm{mod}\, 15),\ 143 \equiv 353 (\mathrm{mod}\, 21),\ 143 \equiv 353 (\mathrm{mod}\, 35),\ 143 \equiv 353 (\mathrm{mod}\, 30),$$
$$143 \equiv 353 (\mathrm{mod}\, 42),\ 143 \equiv 353 (\mathrm{mod}\, 105),\ 143 \equiv 353 (\mathrm{mod}\, 70)\ .$$

СВОЙСТВО 7. Для любых целых чисел a и b, любого $n \geq 2$ из того, что $a \equiv b (\mathrm{mod}\, n)$ и $a \vdots k, b \vdots k, n \vdots k,\ k \in N$, следует $\frac{a}{k} \equiv \frac{b}{k} \left(\mathrm{mod} \frac{n}{k} \right)$.

Доказательство. По условию и определению делимости имеем $a = k \cdot \frac{a}{k}, b = k \cdot \frac{b}{k}, n = k \cdot \frac{n}{k}$. Тогда $a - b = nt,\ k \cdot \left(\frac{a}{k} - \frac{b}{k} \right) = k \cdot \frac{n}{k} \cdot t$. После сокращения на k получаем $\left(\frac{a}{k} - \frac{b}{k} \right) = \frac{n}{k} \cdot t$, т. е. $\frac{a}{k} \equiv \frac{b}{k} \left(\mathrm{mod} \frac{n}{k} \right)$.

Пример.

$$\begin{cases} 273 \equiv 78 (\mathrm{mod} 195) \\ 273 = 39 \cdot 7,\ 78 = 39 \cdot 2,\ 195 = 39 \cdot 5 \end{cases} \Rightarrow 7 \equiv 2 (\mathrm{mod}\, 5).$$

СВОЙСТВО 8. Для любых целых чисел a и b, любого $n \geq 2$ из того, что $a \equiv b (\mathrm{mod}\, n)$ и $a \vdots k,\ b \vdots k,\ (n;k) = 1$, следует $\frac{a}{k} \equiv \frac{b}{k} (\mathrm{mod}\, n)$.

Доказательство. По условию и определению делимости имеем $a = k \cdot \frac{a}{k}, b = k \cdot \frac{b}{k}$, причем $\frac{a}{k} \in Z, \frac{b}{k} \in Z$. Тогда $a - b = k \cdot \left(\frac{a}{k} - \frac{b}{k} \right)$ и по условию $k \cdot \left(\frac{a}{k} - \frac{b}{k} \right) \vdots n$, т. к. $(n;k) = 1$, то по свойству делимости получим $\left(\frac{a}{k} - \frac{b}{k} \right) \vdots n$, следовательно, $\frac{a}{k} \equiv \frac{b}{k} (\mathrm{mod}\, n)$.

Пример.

$$\begin{cases} 799 \equiv 1457 (\mathrm{mod}\, 211) \\ 799 = 47 \cdot 17, 1457 = 47 \cdot 31 \\ (211;47) = 1 \end{cases} \Rightarrow 17 \equiv 31 (\mathrm{mod}\, 211).$$

СВОЙСТВО 9. Для любых целых чисел a и b, любых $n \geq 2$, $m \geq 2$ из того, что $a \equiv b(\mathrm{mod}\, n)$, $a \equiv b(\mathrm{mod}\, m)$ и $(m;n)=1$, следует, что истинно сравнение $a \equiv b(\mathrm{mod}\, n \cdot m)$.

Доказательство. Из условия имеем $(a-b) \vdots n$ и $(a-b) \vdots m$, откуда получаем равенство $a-b=nt=mk$. Т. к. $(m;n)=1$, то $nt \vdots m \Leftrightarrow t \vdots m$, $t = m \cdot l,\ l \in Z$. В результате имеем $a-b=nt=nml$, что означает истинность сравнения $a \equiv b(\mathrm{mod}\, n \cdot m)$.

Замечание. Справедливо и свойство, обратное свойству 9.

Примеры.

$$\begin{cases} 15 \equiv 39(\mathrm{mod}\, 8) \\ 15 \equiv 39(\mathrm{mod}\, 3) \end{cases} \Rightarrow 15 \equiv 39(\mathrm{mod}\, 24);$$

$$\begin{cases} 41 \equiv -141(\mathrm{mod}\, 91) \\ 91 = 7 \cdot 13,\ (7;13)=1 \end{cases} \Rightarrow \begin{cases} 41 \equiv -141(\mathrm{mod}\, 7) \\ 41 \equiv -141(\mathrm{mod}\, 13) \end{cases}.$$

СВОЙСТВО 10. Для любых целых чисел a и b, любых $n \geq 2$, $m \geq 2$ из того, что $a \equiv b(\mathrm{mod}\, n)$, $a \equiv b(\mathrm{mod}\, m)$ и $[m;n]$ – наименьшее общее кратное чисел *m*, *n*, следует истинность сравнения $a \equiv b(\mathrm{mod}[m;n])$.

Доказательство. Пусть $d=(m;n)$ – наибольший общий делитель чисел *m* и *n*. Тогда по свойству наибольшего общего делителя имеем $m = d \cdot m_1,\ n = d \cdot n_1$ и $(m_1;n_1)=1$. Из сравнений $a \equiv b(\mathrm{mod}\, n)$ и $a \equiv b(\mathrm{mod}\, m)$ по определению получаем, что $(a-b) \vdots n$ и $(a-b) \vdots m$, т. е. $a-b=nt=mk$. Следовательно, верно равенство $m_1 k = n_1 t$. А т. к. $(m_1;n_1)=1$, то $k \vdots n_1$ и $a-b=mn_1k_1$. По формуле вычисления наименьшего общего кратного получаем $[m;n]=\dfrac{m \cdot n}{(m;n)}=\dfrac{m \cdot d \cdot n_1}{d}=m \cdot n_1$. Окончательно имеем $a-b=[m;n]k_1$, т. е. $(a-b) \vdots [m;n]$ и $a \equiv b(\mathrm{mod}[m;n])$.

Пример.

$$\begin{cases} 32 \equiv -38(\mathrm{mod}\, 14) \\ 32 \equiv -38(\mathrm{mod}\, 35) \end{cases} \Rightarrow \begin{cases} 32 \equiv -38(\mathrm{mod}\, 70) \\ [14;35]=70 \end{cases}.$$

ОПРЕДЕЛЕНИЕ.

Множества $Z_0 = \{nt / t \in Z\}$, $Z_1 = \{nt+1 / t \in Z\}$,..., $Z_{n-1} = \{nt+(n-1) / t \in Z\}$ (при $n \geq 2$) называют классами вычетов по модулю *n*. Числа, входящие в эти множества, называют представителями или образующими этих классов.

Если целое число *a* является представителем класса вычетов Z_i, то имеем $a = n \cdot t + i = n \cdot t + r_a$, $0 \leq r_a \leq n-1$. Данное равенство показывает, что и само число *a*, и остаток от деления *a* на модуль *n* принадлежат одному классу вычетов. Поэтому в качестве образующего элемента класса вычетов, содержащего число *a*, удобно рассматривать остаток r_a. Класс вычетов Z_{r_a} по модулю *n* будем обозначать $[r_a]_n$, читается «класс вычетов, порожденный числом r_a по модулю *n*». Тогда имеем, что класс вычетов $[r_a]_n$ – это множество всех целых чисел, сравнимых с r_a по модулю *n*, т. е. $[r_a]_n = \{b \in Z \mid b \equiv r_a (\mathrm{mod}\, n)\}$.

Пример.

Найдем все классы вычетов по модулю 5. При делении на 5 остаток *r* удовлетворяет условию $0 \leq r \leq 4$, поэтому имеем следующие классы вычетов по модулю 5:

$[0]_5 = Z_0 = \{5t / t \in Z\}$, $[1]_5 = Z_0 = \{5t+1 / t \in Z\}$, $[2]_5 = Z_0 = \{5t+2 / t \in Z\}$,

$[3]_5 = Z_0 = \{5t+3 / t \in Z\}$, $[4]_5 = Z_0 = \{5t+4 / t \in Z\}$.

Т. к. любое целое число *a* можно разделить на 5 с остатком, $a = 5q + r_a$, $r_a \in \{0;1;2;3;4\}$, то *a* попадет в какой-то класс вычетов $[r_a]_5$. В силу определения класса вычетов и свойства 3 любой вычет *x* класса $[r_a]_5$ сравним с r_a по модулю 5, а следовательно, и с *a*, т. е. истинно сравнение $b \equiv r_a \equiv a (\mathrm{mod}\, 5)$. Данный факт означает, что любое целое число может быть рассмотрено в качестве образующего элемента класса вычетов, его содержащего. Следовательно, справедливо следующее свойство.

СВОЙСТВО 11. Если целое число *a* принадлежит классу вычетов $[b]_n$, то класс вычетов $[a]_n$ совпадает с классом $[b]_n$.

Доказательство. Для доказательства равенства классов $[a]_n = [b]_n$ докажем взаимное включение классов: $[a]_n \subset [b]_n$ и $[b]_n \subset [a]_n$.

Выберем из класса $[a]_n$ любой элемент x. По определению класса вычетов $x \equiv a(\mathrm{mod}\, n)$. Из условия $a \in [b]_n$ имеем $a \equiv b(\mathrm{mod}\, n)$. Тогда по свойству 3 справедливо сравнение $x \equiv b(\mathrm{mod}\, n)$, откуда следует, что x является элементом класса $[b]_n$. Следовательно, $[a]_n \subset [b]_n$.

Возьмем в классе $[b]_n$ любой элемент $[y]_n$. По свойству 2 из сравнения $a \equiv b(\mathrm{mod}\, n)$ следует сравнение $b \equiv a(\mathrm{mod}\, n)$. Из сравнений $y \equiv b(\mathrm{mod}\, n)$ и $b \equiv a(\mathrm{mod}\, n)$ по свойству 3 получим $y \equiv a(\mathrm{mod}\, n)$. Имеем $[b]_n \subset [a]_n$.

В зависимости от решаемой задачи бывает удобно в качестве представителей классов выбирать вычеты с особыми условиями: наименьшие положительные вычеты, наименьшие неотрицательные вычеты, наименьшие по абсолютной величине вычеты, наибольшие отрицательные вычеты, наибольшие неположительные вычеты, вычеты, принадлежащие данному интервалу, и т. д.

Пример.

Вычеты 23, –46, 63, 4, 732, –127 по модулю 7 заменить на:

1) наименьшие по абсолютной величине вычеты;
2) наименьшие неотрицательные вычеты;
3) наибольшие отрицательные вычеты;
4) наименьшие положительные вычеты;
5) вычеты, входящие в интервал $(15;23)$.

Определим классы, в которые входят данные в условии вычеты (целые числа). Для этого разделим их с остатком на 7:

$23 = 7 \cdot 3 + 2$, $23 \in [2]_7$; $-46 = 7 \cdot (-7) + 3$, $-46 \in [3]_7$; $63 = 7 \cdot 9$, $63 \in [0]_7$;

$4 = 7 \cdot 0 + 4$, $4 \in [4]_7$; $732 = 7 \cdot 104 + 4$, $732 \in [4]_7$; $-127 = 7 \cdot (-19) + 6$,

$-127 \in [6]_7$.

1. 2 – наименьший по абсолютной величине вычет класса $[2]_7$,

3 – наименьший по абсолютной величине вычет класса $[3]_7$,

0 – наименьший по абсолютной величине вычет класса $[0]_7$,

–3 – наименьший по абсолютной величине вычет класса $[4]_7$,

–1– наименьший по абсолютной величине вычет класса $[6]_7$.

Следовательно, производим замену вычетов $23 \mapsto 2$, $-46 \mapsto 3$, $63 \mapsto 0$, $4 \mapsto -3$, $732 \mapsto -3$, $-127 \mapsto -1$.

2. 2 – наименьший неотрицательный вычет класса $[2]_7$, 3 – наименьший неотрицательный вычет класса $[3]_7$, 0 – наименьший неотрицательный вычет класса $[0]_7$, 4 – наименьший неотрицательный вычет класса $[4]_7$, 6 – наименьший неотрицательный вычет класса $[6]_7$. Производим замену вычетов $23 \mapsto 2$, $-46 \mapsto 3$, $63 \mapsto 0, 4 \mapsto 4$, $732 \mapsto 4$, $-127 \mapsto 6$.
3. –5 – наибольший отрицательный вычет класса $[2]_7$, –4 – наибольший отрицательный вычет класса $[3]_7$, –7 – наибольший отрицательный вычет класса $[0]_7$, –3 – наибольший отрицательный вычет класса $[4]_7$, –1 – наибольший отрицательный вычет класса $[6]_7$. Производим замену вычетов $23 \mapsto -5$, $-46 \mapsto -4$, $63 \mapsto -7, 4 \mapsto -3$, $732 \mapsto -3$, $-127 \mapsto -1$.
4. 2 – наименьший положительный вычет класса $[2]_7$, 3 – наименьший положительный вычет класса $[3]_7$, 7 – наименьший положительный вычет класса $[0]_7$, 4 – наименьший положительный вычет класса $[4]_7$, 6 – наименьший положительный вычет класса $[6]_7$. Производим замену вычетов $23 \mapsto 2$, $-46 \mapsto 3$, $63 \mapsto 7, 4 \mapsto 4$, $732 \mapsto 4$, $-127 \mapsto 6$.
5. из промежутка $(15;23)$ число $16 \in [2]_7$, $17 \in [3]_7$, $21 \in [0]_7$, $18 \in [4]_7$, $20 \in [6]_7$. Производим замену $23 \mapsto 16$, $-46 \mapsto 17$, $63 \mapsto 21$, $4 \mapsto 18$, $732 \mapsto 18$, $-1272 \mapsto 20$.

ОПРЕДЕЛЕНИЕ. Если из каждого класса вычетов $[0]_n, [1]_n, ..., [n-1]_n$ взять по одному представителю, то получим множество элементов $\{a_0; a_1; ...; a_{n-1}\}_n$, которое называют *полной системой вычетов* по модулю *n*.

Для элементов любой полной системы вычетов по модулю n справедливы свойства:

СВОЙСТВО 12. Любые n попарно не сравнимых по модулю n целых чисел образуют полную систему вычетов по модулю n.

Доказательство. Пусть даны числа $b_1, b_2, ..., b_n$, для любых двух из которых сравнение $b_i \equiv b_j \pmod{n}$ является ложным, следовательно, любые два числа этого множества одному классу вычетов не принадлежат. По модулю n существует n различных, попарно не пересекающихся классов вычетов, поэтому каждое из n данных чисел принадлежит какому-либо классу вычетов (между множеством данных чисел и множеством классов вычетов устанавливается взаимно-однозначное соответствие). В итоге имеем множество представителей всех классов вычетов по модулю n, взятых по одному из каждого класса, т. е. полную систему вычетов по модулю n.

Следствие. Всякое целое число сравнимо с каким-либо единственным вычетом полной системы вычетов по модулю n.

СВОЙСТВО 13. Любые два элемента полной системы вычетов $\{a_0; a_1; ...; a_{n-1}\}_n$ не сравнимы по модулю n.

Доказательство. Возьмем два любых неравных элемента a_i, a_j данной полной системы вычетов. Если $a_i \equiv a_j \pmod{n}$, то элементы a_i, a_j принадлежат одному классу вычетов, чего не может быть по определению полной системы вычетов.

СВОЙСТВО 14. Если $\{a_0; a_1; ...; a_{n-1}\}_n$ – полная система вычетов по модулю n, k – такое целое число, что $(k; n) = 1$, то множество $\{ka_0; ka_1; ...; ka_{n-1}\}_n$ – полная система вычетов по модулю n.

Доказательство (методом от противного). *Предположение*: пусть множество $\{ka_0; ka_1; ...; ka_{n-1}\}_n$ не является полной системой вычетов по модулю n.

Т. к. множество состоит из n элементов, то полной системой вычетов оно не будет только в случае, если какие-то два элемента ka_i, ka_2 принадлежат одному классу вычетов. Это означает по определению класса вычетов, что

$ka_i \equiv ka_j (\mathrm{mod}\, n)$, откуда по свойству 8 получаем $a_i \equiv a_j (\mathrm{mod}\, n)$. Следовательно, a_i, a_j принадлежат одному классу вычетов, чего по условию быть не может. Предположение оказалось неверным.

СВОЙСТВО 15. Если $\{a_0; a_1; ...; a_{n-1}\}_n$ – полная система вычетов по модулю *n*, *b* – любое целое число, то $\{a_0 + b; a_1 + b; ...; a_{n-1} + b\}_n$ – полная система вычетов по модулю *n*.

Доказательство (методом от противного). *Предположение*: пусть множество чисел $\{a_0 + b; a_1 + b; ...; a_{n-1} + b\}$ не является полной системой вычетов по модулю *n*, следовательно, среди чисел $a_0 + b, a_1 + b, ..., a_{n-1} + b$ найдутся хотя бы два числа, принадлежащие одному классу вычетов. Пусть для $i \neq j$ $a_i + b \equiv a_j + b (\mathrm{mod}\, n)$, тогда из свойства 1 и свойства 4 получаем $a_i \equiv a_j (\mathrm{mod}\, n)$, чего по условию не может быть.

ОБОБЩЕНИЕ СВОЙСТВ 14 и 15. Если x пробегает полную систему вычетов по модулю m, а y пробегает полную систему вычетов по модулю n и числа m и n взаимно простые, то числа $z = n \cdot x + m \cdot y$ пробегают полную систему вычетов по модулю $m \cdot n$.

Доказательство. Число x принимает m различных значений, число y принимает n значений, тогда можно составить $m \cdot n$ различных упорядоченных пар $(x; y)$, следовательно, будем иметь $m \cdot n$ чисел вида $z = n \cdot x + m \cdot y$. Покажем, что никакие два таких числа не сравнимы по модулю $m \cdot n$. Доказательство проведем методом от противного. *Предположение*: пусть среди чисел $z = n \cdot x + m \cdot y$ найдутся хотя бы два таких $z_1 = n \cdot x_1 + m \cdot y_1$ и $z_2 = n \cdot x_2 + m \cdot y_2$, для которых выполняется условие

$$n \cdot x_1 + m \cdot y_1 \equiv n \cdot x_2 + m \cdot y_2 (\mathrm{mod}\ m \cdot n),$$

тогда по свойству 6 справедлива система сравнений

$$\begin{cases} n \cdot x_1 + m \cdot y_1 \equiv n \cdot x_2 + m \cdot y_2 (\mathrm{mod}\ m) \\ n \cdot x_1 + m \cdot y_1 \equiv n \cdot x_2 + m \cdot y_2 (\mathrm{mod}\ n) \end{cases},$$

из которой получаем систему сравнений

$$\begin{cases} n \cdot x_1 \equiv n \cdot x_2 (\text{mod } m) \\ m \cdot y_1 \equiv m \cdot y_2 (\text{mod } n) \end{cases}.$$

Разделив обе части каждого сравнения системы на соответствующие общие делители, взаимно простые с модулями, получим систему сравнений

$$\begin{cases} x_1 \equiv x_2 (\text{mod } m) \\ y_1 \equiv y_2 (\text{mod } n) \end{cases}.$$

Каждое сравнение этой системы является ложным, т. к. числа x_1 и x_2 являются различными вычетами полной системы вычетов по модулю m, аналогично и числа y_1 и y_2 – различные вычеты по модулю n. Получили противоречие, следовательно, наше предположение оказалось неверным.

Рассмотрим одну из числовых функций функцию Эйлера, которая используется в теории сравнений.

ОПРЕДЕЛЕНИЕ. Количество натуральных чисел, не превосходящих натурального *n* и с *n* взаимно простых, называют функцией Эйлера от *n*, обозначают $\varphi(n)$.

Примеры.

Найти $\varphi(n)$, где $n \in \{1;2;4;6;8;11\}$.

1) При *n*=1 имеем, что только одно натуральное число 1 не превосходит его, причем $(1;1)=1$, следовательно, $\varphi(1)=1$.
2) При *n*=2 два натуральных числа 1 и 2 не превосходят 2, т. к. $(1;2)=1$ и $(2;2)=2\neq 1$, то $\varphi(2)=1$.
3) При *n*=4 два натуральных числа 1 и 3 не превосходят 4 и $(1;4)=1$, $(3;4)=1$. $\varphi(4)=2$.
4) Рассмотрим случай *n*=6. Запишем ряд натуральных чисел, не превосходящих 6, вычеркнем числа не взаимно простые с 6: 1, ~~2~~, ~~3~~, ~~4~~, 5, ~~6~~. Незачеркнутыми остались только два числа 1 и 5, следовательно, $\varphi(6)=2$.
5) *n*=8. 1, ~~2~~, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~. Значение функции Эйлера $\varphi(8)=4$.
6) *n*=11. 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, ~~11~~. $\varphi(11)=10$.

Данные примеры показывают, что очевидной зависимости значения функции Эйлера от числа *n* нет. Выведем формулы для вычисления $\varphi(n)$ при любом значении натурального числа *n*.

1. Дано простое число *p*. Все натуральные числа от 1 до $p-1$ (меньшие *p*) с *p* взаимно просты, следовательно, $\varphi(p)=p-1$.
2. Пусть $n=p^k$, где *p* – простое число, а $k\in N$. Расположим числа от 1 до p^k в ряд:

   1, 2, …, (*p*-1), *p*, (*p*+1), (*p*+2), …, 2*p*, (2*p*+1), (2*p*+2), …, 3*p*, …, $p\left(p^{k-1}-1\right)$, ($p\left(p^{k-1}-1\right)$+1), ($p\left(p^{k-1}-1\right)$+2) …, p^k.

   Числа данного ряда можно разбить на p^{k-1} множеств по *p* чисел:

   (*tp*+1), (*tp*+2), …, (*t*+1)*p*, где $0\le t\le p^{k-1}-1$.

   Каждое из этих множеств содержит только по одному числу, кратному *p*, остальные *p*–1 числа на *p* не делятся, следовательно, с *p* взаимно просты. Всего количество чисел от 1 до p^k взаимно простых с *p* равно $(p-1)\cdot p^{k-1}$, следовательно, $\varphi\left(p^k\right)=(p-1)\cdot p^{k-1}$.
3. Пусть дано составное число *m*, т. е. существуют такие два целых числа $a\ne 1$ и $b\ne 1$, что $m=a\cdot b$. Если натуральные числа *a* и *b* взаимно простые, то верно равенство $\varphi(a\cdot b)=\varphi(a)\cdot\varphi(b)$. Говорят, что функция Эйлера *мультипликативна*.

   Если $n=p_1^{k_1}\cdot p_2^{k_2}\cdot\ldots\cdot p_t^{k_t}$ – каноническое представление числа *n*, то

   $\varphi\left(p_1^{k_1}\cdot p_2^{k_2}\cdot\ldots\cdot p_t^{k_t}\right)=(p_1-1)\cdot p_1^{k_1-1}\cdot(p_2-1)\cdot p_2^{k_2-1}\cdot\ldots\cdot p_t^{k_t-1}$.

Примеры.

1) $\varphi(41)=41-1=40$, т. к. 41 – простое число.
2) $\varphi(91)=\varphi(7\cdot 13)=\varphi(7)\cdot\varphi(13)=(7-1)\cdot(13-1)=6\cdot 12=72$.
3) $\varphi(125)=\varphi\left(5^3\right)=(5-1)\cdot 5^{3-1}=4\cdot 25=100$.
4) $\varphi(1176)=\varphi\left(2^3\cdot 3\cdot 7^2\right)=(2-1)\cdot 2^{3-1}\cdot(3-1)\cdot(7-1)\cdot 7^{2-1}=336$.

ОПРЕДЕЛЕНИЕ. Класс вычетов $[k]_n$ называется взаимно простым с модулем *n*, если $(k;n)=1$.

Т. к. для модуля n представителями различных классов могут быть числа 1, 2, …, n, то количество классов по модулю n взаимно простых с n равно количеству чисел, не превосходящих n и с n взаимно простых, т. е. их число равно $\varphi(n)$.

ОПРЕДЕЛЕНИЕ. Если из каждого класса вычетов по модулю n взаимно простого с n взять по одному представителю, то получим множество чисел $\{a_1, a_2, ..., a_{\varphi(n)}\}_n$, которое называют *приведенной системой вычетов по модулю n*.

Пример.

Записать приведенную систему вычетов для модуля n=7; n=8.

1) Для модуля n=7 имеем классы вычетов $[1]_7$, $[2]_7$, $[3]_7$, $[4]_7$, $[5]_7$, $[6]_7$, $[7]_7$. Из этих классов с модулем n=7 взаимно простыми являются классы $[1]_7$, $[2]_7$, $[3]_7$, $[4]_7$, $[5]_7$, $[6]_7$. Из каждого из них выберем по одному представителю: $-6 \in [1]_7$, $37 \in [2]_7$, $17 \in [3]_7$, $-59 \in [4]_7$, $110 \in [5]_7$, $-345 \in [6]_7$. Запишем приведенную систему вычетов по модулю 7: $\{-6; 37; 17; -59; 110; -345\}_7$.
2) $\varphi(8) = 4$, следовательно, приведенная система вычетов по модулю 8 состоит из 4 чисел. Одной из приведенных систем вычетов по модулю 8 является множество $\{41; -53; 45; 95\}_8$.

Для приведенных систем вычетов по модулю n справедливы следующие свойства.

СВОЙСТВО 16. Любые $\varphi(n)$ целых чисел, попарно не сравнимых по модулю n и взаимно простых с n, образуют приведенную систему вычетов по модулю n.

Доказательство. Пусть даны целые числа $b_1, b_2, .., b_{\varphi(n)}$, для которых выполняются условия: $b_i \not\equiv b_j \pmod n$ и $(b_i; n) = 1$ для любых неравных $i, j \in \{1; 2; ...; \varphi(n)\}$. Т. к. $b_i \not\equiv b_j \pmod n$, то числа b_i и b_j принадлежат разным классам вычетов по модулю n. В силу условия $(b_i; n) = 1$ получаем, что класс вычетов, содержащий число b_i, является взаимно простым с модулем n. Для натурального числа n число классов с ним взаимно простых равно $\varphi(n)$.

Следовательно, множество $\{b_1, b_2, .., b_{\varphi(n)}\}$ является приведенной системой вычетов по модулю n.

СВОЙСТВО 17. Если $\{a_1, a_2, ..., a_{\varphi(n)}\}_n$ – приведенная система вычетов по модулю n и натуральное число k взаимно простое с n, то множество $\{ka_1, ka_2, ..., ka_{\varphi(n)}\}$ – является приведенной системой вычетов по модулю n.

Доказательство. Если множество $\{ka_1, ka_2, ..., ka_{\varphi(n)}\}$ содержит числа, не удовлетворяющие одному из условий определения, то это возможно только, если:

1) какие-либо два числа ka_i и ka_j принадлежат одному классу вычетов по модулю n. Тогда $ka_i \equiv ka_j (\mathrm{mod}\, n)$, а т. к. по условию $(k;n)=1$, то по свойству 8 истинно сравнение $a_i \equiv a_j (\mathrm{mod}\, n)$, что противоречит условию;
2) какое-либо число ka_i не является взаимно простым с модулем n, тогда по свойствам делимости в кольце целых чисел[1] найдется такое простое число p, что $ka_i \vdots p$ и $n \vdots p$. Но $ka_i \vdots p \Leftrightarrow k \vdots p$ или $a_i \vdots p$. Оба эти утверждения противоречат условию.

Вывод: множество чисел $\{ka_1, ka_2, ..., ka_{\varphi(n)}\}$ образует приведенную систему вычетов.

Для натурального числа n найдем сумму значений функции Эйлера для всех делителей этого числа. Обозначим $f(n) = \sum_{n:d} \varphi(d)$.

Теорема 1 (тождество Гаусса). *Для любого натурального числа n справедливо равенство* $f(n) = n$.

Доказательство. Пусть для чисел a и b выполняются условия: $(a;b)=1$ и $a \vdots \delta$, $b \vdots \sigma$. Тогда, исходя из правила умножения суммы на сумму, получаем равенство $f(a) \cdot f(b) = \left(\sum_{a:\delta} \varphi(\delta) \right) \cdot \left(\sum_{b:\sigma} \varphi(\sigma) \right) = \sum_{a:\delta} \sum_{b:\sigma} (\varphi(\delta) \cdot \varphi(\sigma))$.

[1] Ляпин, Е. С. Алгебра и теория чисел. – Ч. I : Числа / Е. С. Ляпин, А. Е. Евсеев. – М. : Просвещение, 1974. – Гл. II. – § 4.

В силу мультипликативности функции Эйлера получаем $\varphi(\delta)\cdot\varphi(\sigma)=\varphi(\delta\cdot\sigma)$. Числа вида $\delta\cdot\sigma$ являются делителями числа $a\cdot b$, т. к. $a\vdots\delta$ и $b\vdots\sigma$. В силу условия взаимной простоты чисел a и b любой делитель числа $a\cdot b$ представим в виде произведения $a_1\cdot b_1$, где a_1 – делитель числа a, b_1 – делитель числа b и $(a_1;b_1)=1$. Получаем, что $\sum\limits_{a:\delta}\sum\limits_{b:\sigma}(\varphi(\delta)\cdot\varphi(\sigma))=\sum\limits_{ab:c}\varphi(c)$.

Следовательно, $f(a)\cdot f(b)=f(a\cdot b)$, т. е. $f(n)$ – мультипликативна.

Пусть $n=p^k$, тогда $f(n)=\varphi(1)+\varphi(p)+\varphi(p^2)+...+\varphi(p^k)=$

$1+(p-1)+p(p-1)+...+p^{k-1}(p-1)=\ 1+p-1+p^2-p+...+p^k-p^{k-1}=p^k$.

Если натуральное число n имеет каноническое представление $n=p_1^{k_1}\cdot p_2^{k_2}\cdot....\cdot p_t^{k_t}$, то $f(n)=f(p_1^{k_1})\cdot f(p_2^{k_2})\cdot....\cdot f(p_t^{k_t})=p_1^{k_1}\cdot p_2^{k_2}\cdot....\cdot p_t^{k_t}=n$.■

Пример.

Найти значение $f(12)$.

Способ 1 (по определению).

Делителями числа 12 являются числа: 1, 2, 3, 4, 6, 12.

Тогда $f(12)=\varphi(1)+\varphi(2)+\varphi(3)+\varphi(4)+\varphi(6)+\varphi(12)$=1+1+2+2+2+4=12.

Способ 2 (по тождеству Гаусса). $f(12)=12$.

СВОЙСТВО 18. Пусть $f(x)=a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0$ – многочлен с целыми коэффициентами, $a_i\equiv b_i(\mathrm{mod}\,m),\ i=0,1,...,n$ и для целого x выполнено условие $x\equiv y(\mathrm{mod}\,m)$, тогда:

1) $(a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0)\equiv(b_nx^n+b_{n-1}x^{n-1}+...+b_1x+b_0)(\mathrm{mod}\,m)$;

2) $f(x)\equiv f(y)(\mathrm{mod}\,m)$.

Доказательство. 1) Докажем, что разность чисел $a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0$ и $b_nx^n+b_{n-1}x^{n-1}+...+b_1x+b_0$ делится на m.

Рассмотрим разность

$$A=(a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0)-(b_nx^n+b_{n-1}x^{n-1}+...+b_1x+b_0)=$$

$$=(a_nx^n-b_nx^n)+(a_{n-1}x^{n-1}-b_{n-1}x^{n-1})+...+(a_1x-b_1x)+(a_0-b_0)=$$

$$=(a_n-b_n)x^n+(a_{n-1}-b_{n-1})x^{n-1}+...+(a_1-b_1)x+(a_0-b_0).$$

Т. к. по условию для всех $i=0,...,n$ верны сравнения $a_i \equiv b_i (\mathrm{mod}\, m)$, то числа $(a_i - b_i)x^i$ делятся на m при любых целых значениях x. Следовательно, $A \vdots m$, т. е. свойство доказано.

Из условия $x \equiv y (\mathrm{mod}\, m)$ и по свойству 5 получаем систему сравнений

$$\begin{cases} a_1 x \equiv a_1 y (\mathrm{mod}\, m) \\ a_2 x^2 \equiv a_2 y^2 (\mathrm{mod}\, m) \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ a_n x^n \equiv a_n y^n (\mathrm{mod}\, m) \end{cases}.$$

Из свойства 1 и свойства 4 окончательно имеем сравнение

$$\left(a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0\right) \equiv \left(a_n y^n + a_{n-1} y^{n-1} + ... + a_1 y + a_0\right) (\mathrm{mod}\, m).$$

Пусть числа a и m взаимно просты. Рассмотрим последовательность (a^n) натуральных степеней числа a: $a, a^2, a^3, ..., a^t, ...$ Данная последовательность имеет бесконечное число членов.

Известно, что различных классов вычетов по модулю m существует всего m. Каждое целое число входит в какой-то из этих классов, следовательно, в некоторый класс попадет бесчисленное множество степеней числа a. Выберем из данного класса две степени a^s и a^l, пусть $l > s \geq 1$. Тогда имеем истинное сравнение $a^l \equiv a^s (\mathrm{mod}\, m)$. Т. к. $(a, m) = 1$, то и $(a^s, m) = 1$. По свойству 8 обе части сравнения можно разделить на a^s, в итоге получим сравнение $a^{l-s} \equiv 1 (\mathrm{mod}\, m)$. Т. е. существует такое натуральное число $k = l - s$, что $a^k \equiv 1 (\mathrm{mod}\, m)$. Для любого натурального n, в силу следствия 2 свойства 5, $a^{kn} \equiv 1 (\mathrm{mod}\, m)$. Это сравнение показывает, что класс вычетов $[1]_m$ содержит бесчисленное множество степеней числа a. Т. к. числа s и l были выбраны произвольно, то значение k не определено однозначно.

Пьер Ферма[2] для простого модуля, Леонард Эйлер[3] для любого модуля нашли значения $k \neq 0$, при которых имеет место сравнение $a^k \equiv 1 (\mathrm{mod}\, m)$.

[2] Ферма Пьер (Fermat Pierre) (1601–1665) – французский математик.

[3] Эйлер Леонард (Euler Leonhard) (1707–1783) – математик, механик и физик. С 1727 г. по 1741 г. и с 1766 г. и до конца жизни жил в Петербурге, являлся членом Петербургской академии.

Теорема 2 (теорема Эйлера). *Для любого целого числа* $a \geq 1$ *и любого* $m \geq 2$, *таких, что* $(a;m)=1$, *справедливо сравнение* $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$.

Доказательство. Пусть множество $\{x_1; x_2; ...; x_{\varphi(m)}\}_m$ – приведенная система вычетов по модулю m. По свойству 17 множество $\{ax_1; ax_2; ...; ax_{\varphi(m)}\}_m$ – также приведенная система вычетов по модулю m. Следовательно, для элементов первого и второго множеств можно установить взаимно однозначное соответствие элементов, такое, что верны сравнения

$$\begin{cases} ax_1 \equiv x_1' (\mathrm{mod}\, m) \\ ax_2 \equiv x_2' (\mathrm{mod}\, m) \\ \ldots\ldots\ldots\ldots \\ ax_{\varphi(m)} \equiv x'_{\varphi(m)} (\mathrm{mod}\, m) \end{cases}.$$

Здесь числа x_i' есть числа x_j, т. е. множества $\{x_1; x_2; ...; x_{\varphi(m)}\}_m$ и $\{x_1'; x_2'; ...; x'_{\varphi(m)}\}_m$ равны. В соответствии со свойством 5 верно сравнение

$$(ax_1 \cdot ax_2 \cdot ... \cdot ax_{\varphi(m)}) \equiv (x_1' \cdot x_2' \cdot ... \cdot x'_{\varphi(m)}) (\mathrm{mod}\, m), \quad \text{или}$$

$$a^{\varphi(m)} \cdot (x_1 \cdot x_2 \cdot ... \cdot x_{\varphi(m)}) \equiv (x_1' \cdot x_2' \cdot ... \cdot x'_{\varphi(m)}) (\mathrm{mod}\, m).$$

По определению приведенной системы вычетов имеем $(x_i; m)=1$ для всех чисел $x_1, x_2, ..., x_{\varphi(m)}$, следовательно, и число $x_1 \cdot x_2 \cdot ... \cdot x_{\varphi(m)}$ с m также взаимно просто. Тогда, после сокращения обеих частей сравнения на $x_1 \cdot x_2 \cdot ... \cdot x_{\varphi(m)}$, по свойству 8 будет истинным сравнение $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$.■

Теорема 3 (теорема 1 Ферма). *Для любого целого числа a, не делящегося на простое число p, справедливо сравнение* $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.

Доказательство. Т. к. число *a* не делится на простое число *p*, то в силу того, что *p* имеет только два натуральных делителя 1 и *p*, имеем $(a; p)=1$. По теореме Эйлера получаем, $a^{\varphi(p)} \equiv 1 (\mathrm{mod}\, p)$. Но $\varphi(p) = p-1$ для любого простого числа *p*. Окончательно получаем $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.■

Замечание. Теорему 1 Ферма можно рассматривать как частный случай теоремы Эйлера при $n = p$, где p – простое число.

Теорема 4 (теорема 2 Ферма). *Для любого целого числа a и любого простого числа p справедливо сравнение* $a^p \equiv a(\mathrm{mod}\, p)$.

Доказательство. Т. к. простое число p делится только на 1 и на p, то наибольший общий делитель чисел a и p может быть одним из этих чисел.

1) Пусть $(a;p)=1$. По теореме 1 Ферма имеем $a^{p-1} \equiv 1(\mathrm{mod}\, p)$. По свойству 5 (следствие 1) обе части сравнения можно домножить на целое число a, тогда получим $a^p \equiv a(\mathrm{mod}\, p)$.

2) Пусть $(a;p)=p$, т. е. $a \vdots p$. Рассмотрим разность $a^p - a$, в которой и уменьшаемое, и вычитаемое делятся на p. Получаем, что $(a^p - a) \vdots p$, по определению сравнения это означает истинность сравнения $a^p \equiv a(\mathrm{mod}\, p)$.■

Примеры.

1. $(12;5)=1$, $\varphi(12)=4 \Rightarrow 5^4 \equiv 1(\mathrm{mod}12)$. Данное сравнение означает, что при делении числа 5^4 на 12 в остатке получается 1. Действительно, $5^4 = 625 = 12 \cdot 52 + 1$.

   Аналогично $12^4 \equiv 1(\mathrm{mod}5)$.
2. 23 – простое число, $\varphi(23)=22$, тогда для любого целого числа a, не делящегося на 23, справедливо сравнение $a^{22} \equiv 1(\mathrm{mod}23)$. По свойству 5 (следствие 2) обе части сравнения можно возвести в одну и ту же натуральную степень k, получим истинное сравнение $a^{22k} \equiv 1(\mathrm{mod}23)$. Данное сравнение означает, что при делении любой степени числа, взаимно простого с 23, показатель степени которого кратен 22, получается остаток, равный 1.
3. Доказать, что при делении квадрата любого целого числа на 4 остаток не может быть равен 2 или 3.

Способ 1. При делении на 4 любого целого числа получается один из остатков: 0, 1, 2 или 3. Множество всех целых чисел можно разделить на два класса – четных и нечетных чисел: $2Z$ и $2Z+1$. Любое четное число b с числом 4 не является взаимно простым, т. е. $(b;4)=2$ или $(b;4)=4$. Если $(b;4)=2$, то $b = 2 \cdot b'$, где b' – нечетное число, тогда $b^2 = 4 \cdot (b')^2$. Квадрат любого

четного числа делится на 4 (остаток при делении на 4 равен 0). Если число b нечетное, то его можно записать как $b=2t+1, t\in Z$. Т. к. в этом случае $b^2=4\left(t^2+t\right)+1$, то остаток при делении на 4 квадрата нечетного числа равен 1.

Вывод: остаток при делении на 4 квадрата любого целого числа может быть равен 0 или 1 (не равен 2 или 3).

Способ 2. Любое целое число b можно разделить на 4 с остатком: $b=4t+r$, где $0\le r<4$, т. е. $r\in\{0;1;2;3\}$. Получаем $b-r=4t$, следовательно, $(b-r)\vdots 4$ и $b\equiv r(\mathrm{mod}\,4)$. Аналогично имеем $b^2\equiv r^2(\mathrm{mod}\,4)$. Если $r=0$, то $b^2\equiv 0(\mathrm{mod}\,4)$ или $b^2\vdots 4$. Если $r=1$, то $b^2\equiv 1(\mathrm{mod}\,4)$, или при делении b^2 на 4 получается в остатке 1. Если $r=2$, то $b^2\equiv 4\equiv 0(\mathrm{mod}\,4)$, или $b^2\vdots 4$. Если $r=3$, то $b^2\equiv 9\equiv 1(\mathrm{mod}\,4)$, или при делении b^2 на 4 получается в остатке 1. Вывод: остаток при делении на 4 квадрата любого целого числа может быть равен 0 или 1 (не равен 2 или 3).

Теоремы Эйлера и Ферма позволяют находить остатки от деления на модуль больших степеней заданного числа.

Необходимо найти остаток от деления степени a^n на m, где $(a,m)=1$ и $n\ge\varphi(m)$, тогда, по теореме о делении с остатком[4], число n можно представить в виде $n=\varphi(m)\cdot q+r$ и $0\le r<\varphi(m)$. Получаем $a^n=a^{\varphi(m)q+r}=\left(a^{\varphi(m)}\right)^q\cdot a^r$. Т. к. $a^{\varphi(m)}\equiv 1(\mathrm{mod}\,m)$, то $\left(a^{\varphi(m)}\right)^q\cdot a^r\equiv a^r(\mathrm{mod}\,m)$, причем a^r может оказаться значительно меньше, чем a^n.

Рассмотрим случай, когда $(a,m)\ne 1$. Тогда $\left(a^n,m\right)=d>1$ и $a^n=m\cdot t+R,\ 0\le R<m$, причем по свойствам делимости $(R,m)=\left(a^n,m\right)=d$, следовательно, $R\vdots d$ и $R=d\cdot R_1$. Имеем $a^n-R=m\cdot t$, тогда $R\equiv a^n(\mathrm{mod}\,m)$. Найдем наименьшее натуральное число k, такое, что $a^k\vdots d$. Степень a^n можно представить в виде произведения степеней $a^n=a^k\cdot a^{n-k}$, т. к. $a^k=a_1\cdot d$, то $a^n=a^{n-k}\cdot a_1\cdot d$. В силу сравнения $R\equiv a^n(\mathrm{mod}\,m)$ и того, что $m=m_1\cdot d$, получаем истинное сравнение $R_1\equiv a_1\cdot a^{n-k}(\mathrm{mod}\,m_1)$, где $0\le R_1<m_1$. Число R_1 может быть

[4] Ляпин, Е. С. Алгебра и теория чисел. – Ч. I : Числа / Е. С. Ляпин, А. Е. Евсеев. – М. : Просвещение, 1974. – Гл. II. – § 4.

найдено путем вычисления произведения остатков от деления чисел a^{n-k} и a_1 на m_1.

Примеры.

1. Найти остаток от деления 243^{1256} на 38.

Решение. $243^{1256} = 38q + r$, здесь $(243,38) = 1$,

$$243^{1256} - r = 38q,$$

$$243^{1256} \equiv r \pmod{38},$$

$$\varphi(38) = \varphi(2 \cdot 19) = \varphi(2) \cdot \varphi(19) = 1 \cdot 18 = 18,$$

$$1256 = 18 \cdot 69 + 14,$$

$$r \equiv 243^{1256} \equiv \left(243^{18}\right)^{69} \cdot 243^{14} \equiv 243^{14} \pmod{38}.$$

Найдем остаток от деления 243^{14} на 38.

$$243 \equiv 15 \pmod{38},$$

$$243^2 \equiv 225 \equiv 35 \equiv -3 \pmod{38},$$

$$243^4 \equiv 9 \pmod{38},$$

$$243^8 \equiv 81 \equiv 5 \pmod{38},$$

$$243^{12} \equiv 243^4 \cdot 243^8 \equiv 9 \cdot 5 \equiv 45 \equiv 7 \pmod{38},$$

$$243^{14} \equiv 243^{12} \cdot 243^2 \equiv 7 \cdot (-3) \equiv -21 \equiv 17 \pmod{38}.$$

Получили $r = 17$, т. е. $243^{1256} = 38q + 17$.

2. Найти остаток от деления числа 178^{1734} на 176.

Решение. Т. к. $(178,176) = 2 \neq 1$, а $178^{1734} = (2 \cdot 89)^{1734} = 2^{1734} \cdot 89^{1734}$ и $176 = 2^4 \cdot 11$ – каноническое представление чисел, то $(178^{1734},176) = 2^4 = 16$.

Из равенства $178^{1734} = 176 \cdot t + r$ и условия делимости 178^{1734} и 176 на 16 имеем $r \vdots 16$ и $r = 16 \cdot r_1$.

Наименьшее натуральное число k находим из условия $(178^k,176) = 2^4$. Число 178^k имеет каноническое представление: $178^k = 2^k \cdot 89^k$, следовательно, $k = 4$.

$$178^{1734} = 178^4 \cdot 178^{1730} = 176 \cdot t + r,$$

$$178^4 \cdot 178^{1730} \equiv r \pmod{176},$$

$2^4 \cdot 89^4 \cdot 178^{1730} \equiv 16 \cdot r_1 \pmod{(16 \cdot 11)}$, все части сравнения разделим на 16,

$89^4 \cdot 178^{1730} \equiv r_1 (\mathrm{mod} 11)$,

$89^4 = 11 \cdot l + r_2$, $178^{1730} = 11 \cdot s + r_3$, $89^4 \cdot 178^{1730} = 11(11 \cdot l \cdot s + l \cdot r_3 + s \cdot r_2) + r_2 \cdot r_3$,

$89^4 \cdot 178^{1730} \equiv r_1 \equiv r_2 \cdot r_3 (\mathrm{mod} 11)$.

Найдем остатки r_2 и r_3.

$89 \equiv 1(\mathrm{mod} 11) \Rightarrow 89^4 \equiv 1(\mathrm{mod} 11)$, следовательно, $r_2 = 1$,

$(178,11) = 11$, тогда по теореме Эйлера справедливо сравнение

$178^{\varphi(11)} \equiv 1(\mathrm{mod} 11)$, $178^{10} \equiv 1(\mathrm{mod} 11)$.

$1730 = 10 \cdot 173$, $178^{1730} \equiv (178^{10})^{173} \equiv 1(\mathrm{mod} 11)$, следовательно, $r_3 = 1$.

В итоге получаем $r_1 \equiv r_2 \cdot r_3 \equiv 1 \cdot 1 \equiv 1(\mathrm{mod} 11)$ и $r = r_1 \cdot 16 = 16$.

Упражнения для самостоятельного решения

1. Определить, каким классам вычетов по модулю 12 принадлежат целые числа: 134, 42, –53, 27, 674, –341, 55, 67?
2. При помощи каких преобразований, на основании каких свойств сравнений можно из одного сравнения получить другое:

1) $39 \equiv -65(\mathrm{mod} 52) \rightarrow 3 \equiv -5(\mathrm{mod} 4)$;
2) $21 \equiv 45(\mathrm{mod} 8) \rightarrow 49 \equiv 125(\mathrm{mod} 8)$;
3) $-34 \equiv 42(\mathrm{mod} 19) \rightarrow -15 \equiv 4(\mathrm{mod} 19)$?

3. Дополнить множество $\{-23; 45; ...\}$ до полной системы вычетов по модулю 13; до приведенной системы вычетов по модулю 13.
4. Определить, какой остаток может получиться при делении третьей степени целого числа на 3.
5. Доказать, что для любого целого числа a истинно высказывание $(a^{28} - a^4) \vdots 7$.
6. Доказать, что квадрат любого нечетного числа сравним с единицей по модулю 8.
7. Доказать, что нечетное число вида $4k + 3$ нельзя представить как сумму квадратов двух целых чисел.
8. Найти остаток от деления числа $(9674^6 + 28)^{15}$ на 39.

9. Найти остаток от деления числа $\left(3^{100}+5^{100}\right)^{1000}$ на 15.
10. Определить две последние цифры числа 2^{2012}.
11. При делении натурального числа N на 3 и на 37 получаются, соответственно, остатки 1 и 33. Найти остаток от деления числа N на 111.
12. Доказать, что число $5^{2n-1}\cdot 2^{n+1}+3^{n+1}\cdot 2^{2n-1}$ делится на 19 при любом натуральном значении n.

2. КОРНИ СРАВНЕНИЙ

Пусть даны многочлены с целыми коэффициентами $f(x)=a_n x^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$ и $g(x)=b_k x^k+b_{k-1}x^{k-1}+\ldots+b_1x+b_0$.

ОПРЕДЕЛЕНИЕ. Решить сравнение $f(x)\equiv g(x)(\mathrm{mod}\,m)$ – значит найти все целые значения x, при подстановке которых в многочлены $f(x)$ и $g(x)$ получаются целые числа, разность которых делится на m.

Если $f(c)\equiv g(c)(\mathrm{mod}\,m)$, то число c является корнем сравнения $f(x)\equiv g(x)(\mathrm{mod}\,m)$.

Теорема 5. *Если число c является корнем сравнения $f(x)\equiv g(x)(\mathrm{mod}\,m)$, то и любое число c_1, такое, что $c\equiv c_1(\mathrm{mod}\,m)$, удовлетворяет тому же сравнению.*

Доказательство. Обозначим разность многочленов $f(x)-g(x)=h(x)$, тогда $h(c)\equiv 0(\mathrm{mod}\,m)$ и число c – корень сравнения $h(x)\equiv 0(\mathrm{mod}\,m)$. Т. к. по условию $c\equiv c_1(\mathrm{mod}\,m)$, то по свойству 18 верно сравнение $h(c_1)\equiv 0(\mathrm{mod}\,m)$. Следовательно, c_1 – корень сравнения $f(x)\equiv g(x)(\mathrm{mod}\,m)$.■

Из теоремы получаем, что если целое число c является корнем сравнения $f(x)\equiv g(x)(\mathrm{mod}\,m)$, то и любое число класса вычетов $[c]_m$ – также корень этого сравнения.

ОПРЕДЕЛЕНИЕ. Решить сравнение $f(x)\equiv g(x)(\mathrm{mod}\,m)$ – значит найти все классы вычетов по модулю m, любое число из которых удовлетворяет этому сравнению.

Из определения следует один из способов решения сравнения – метод проб. Т. к. по модулю m существует ровно m различных классов вычетов, то достаточно провести m проб для отыскания решений сравнений. Для этого необходимо каждое из чисел x_i $(i=1,...,m)$ полной системы вычетов по модулю m подставить вместо неизвестной в сравнение $f(x)\equiv g(x)(\mathrm{mod}\, m)$.

Примеры.

1. Дан многочлен $f(x)=x^3-3$. Найти решения сравнения $x^3-3\equiv 0(\mathrm{mod}\, 6)$. Подставим каждый из вычетов полной системы вычетов по модулю 6 в данное сравнение и проверим, при каких из них получается истинное сравнение (т. е. число $f(x_i)$ делится на 6).

   $\{0,1,2,3,4,5\}_6$ – полная система вычетов по модулю 6 .

   $f(0)=-3$ не делится на 6, класс вычетов $[0]_6$ не является решением сравнения;

   $f(1)=-2$ не делится на 6, класс вычетов $[1]_6$ не является решением сравнения;

   $f(2)=5$ не делится на 6, класс вычетов $[2]_6$ не является решением сравнения;

   $f(3)=24$ делится на 6, класс вычетов $[3]_6$ *является решением сравнения*;

   $f(4)=61$ не делится на 6, класс вычетов $[4]_6$ не является решением сравнения;

   $f(5)=122$ не делится на 6, класс вычетов $[5]_6$ не является решением сравнения.

   Ответ: $x\equiv 3(\mathrm{mod}\, 6)$ или $x\in[3]_6$.

2. Найти решения сравнения $f(x)\equiv 0(\mathrm{mod}\, 7)$, где $f(x)=x^4+2x-1$.

   $\{0,1,2,3,-3,-2,-1\}_7$ – полная система вычетов по модулю 7.

   $f(0)=-1$ не делится на 7, класс вычетов $[0]_7$ не является решением сравнения;

$f(1)=2$ не делится на 7, класс вычетов $[1]_7$ не является решением сравнения;

$f(2)=19$ не делится на 7, класс вычетов $[2]_7$ не является решением сравнения;

$f(3)=86$ не делится на 7, класс вычетов $[3]_7$ не является решением сравнения;

$f(-3)=74$ не делится на 7, класс вычетов $[-3]_7$ не является решением сравнения;

$f(-2)=11$ не делится на 7, класс вычетов $[-2]_7$ не является решением сравнения;

$f(-1)=-2$ не делится на 7, класс вычетов $[-1]_7$ не является решением сравнения.

Ответ: решений нет.

Способ проб применим для решения сравнений с небольшими модулями, иначе он является громоздким.

Упражнения для самостоятельного решения

1. Проверить, какие из вычетов 1, 4, –15, 27, 156 являются решениями сравнения $3x^5-5x^3+6\equiv 0(\mathrm{mod}\,7)$.
2. Найти решения сравнения $15x^3+2x^2-4x+2\equiv 0(\mathrm{mod}\,5)$.
3. Найти общие решения сравнений $3x^2-5x+3\equiv 0(\mathrm{mod}\,7)$ и $4x^2+2x-4\equiv 0(\mathrm{mod}\,7)$.
4. Составить сравнение третьей степени, имеющее решениями классы $[2]_5$ и $[4]_5$.
5. Определить простое значение модуля m, такое, что сравнение $3x^4-5\equiv 0(\mathrm{mod}\,m)$ имеет решения $[3]_m$ и $[5]_m$.

3. РАВНОСИЛЬНЫЕ СРАВНЕНИЯ С ОДНИМ НЕИЗВЕСТНЫМ

ОПРЕДЕЛЕНИЕ. Два сравнения $f_1(x) \equiv g_1(x) (\mathrm{mod}\, m)$ и $f_2(x) \equiv g_2(x) (\mathrm{mod}\, m)$ называются равносильными, если множество решений одного сравнения являются решениями второго.

На основании определения можно сделать вывод, что сравнение $f(x) \equiv g(x) (\mathrm{mod}\, m)$ равносильно сравнению $f(x) - g(x) \equiv 0 (\mathrm{mod}\, m)$. Поэтому в дальнейшем будем рассматривать сравнения $f(x) \equiv 0 (\mathrm{mod}\, m)$.

Теорема 6. *Если в сравнении* $(a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0) \equiv 0 (\mathrm{mod}\, m)$ *коэффициенты* $a_n, a_{n-1}, ..., a_1, a_0$ *заменить числами, сравнимыми с ними по модулю* m*, то полученное сравнение будет равносильно данному.*

Доказательство. Для каждого коэффициента a_i $(i = 0,1,...,n)$ выберем число b_i, такое, что $b_i \equiv a_i (\mathrm{mod}\, m)$.

Покажем, что любое решение сравнения

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

будет являться решением сравнения

$$(b_n x^n + b_{n-1} x^{n-1} + ... + b_1 x + b_0) \equiv 0 (\mathrm{mod}\, m).$$

Пусть некоторое целое число c является корнем сравнения

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

т. е. числовое сравнение

$$(a_n c^n + a_{n-1} c^{n-1} + ... + a_1 c + a_0) \equiv 0 (\mathrm{mod}\, m)$$

является истинным.

По свойству 5 имеем систему $n+1$ истинных сравнений

$$\begin{cases} a_0 \equiv b_0 (\mathrm{mod}\, m) \\ a_1 c \equiv b_1 c (\mathrm{mod}\, m) \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ a_n c^n \equiv b_n c^n (\mathrm{mod}\, m) \end{cases},$$

откуда по свойству 4 получаем сравнение

$$(a_n c^n + a_{n-1} c^{n-1} + ... + a_1 c + a_0) \equiv (b_n c^n + b_{n-1} c^{n-1} + ... + b_1 c + b_0) (\mathrm{mod}\, m).$$

Из полученного сравнения и истинного сравнения

$\left(a_n c^n + a_{n-1} c^{n-1} + ... + a_1 c + a_0\right) \equiv 0 (\mathrm{mod}\, m)$

по свойству 3 получаем, что сравнение

$\left(b_n c^n + b_{n-1} c^{n-1} + ... + b_1 c + b_0\right) \equiv 0 (\mathrm{mod}\, m)$

также истинно, т. е. число c является решением и сравнения

$\left(b_n x^n + b_{n-1} x^{n-1} + ... + b_1 x + b_0\right) \equiv 0 (\mathrm{mod}\, m)$.

Аналогично доказывается, что любое решение сравнения

$\left(b_n x^n + b_{n-1} x^{n-1} + ... + b_1 x + b_0\right) \equiv 0 (\mathrm{mod}\, m)$

является решением сравнения

$\left(a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0\right) \equiv 0 (\mathrm{mod}\, m)$.

Окончательно делаем вывод, что данные сравнения равносильны. ■

Следствие. Если в сравнении $\left(a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0\right) \equiv 0 (\mathrm{mod}\, m)$ все коэффициенты, делящиеся на m, заменить нулями и опустить соответствующие слагаемые, то получится равносильное сравнение.

Пример.

Дано сравнение $f(x) \equiv 0 (\mathrm{mod}\, 3)$, где $f(x)$ – многочлен $f(x) = x^5 + 4x^4 - 3x^2 + 6$. Заменим коэффициенты этого многочлена на сравнимые с ними по модулю 3 вычетами:

$\left.\begin{array}{l} 4 \equiv 1 (\mathrm{mod}\, 3) \\ 3 \equiv 0 (\mathrm{mod}\, 3) \\ 6 \equiv 0 (\mathrm{mod}\, 3) \end{array}\right|$ получаем многочлен $f_1(x) = x^5 + x^4$.

Покажем равносильность сравнений $f_1(x) \equiv 0 (\mathrm{mod}\, 3)$ и $f(x) \equiv 0 (\mathrm{mod}\, 3)$. Для этого найдем решения каждого сравнения.

Множество $\{0, 1, -1\}_3$ – полная система вычетов по модулю 3.

Рассмотрим сравнение $f(x) \equiv 0 (\mathrm{mod}\, 3)$.

$f(0) = 6$, 6 делится на 3, следовательно, 0 – корень сравнения;

$f(1) = 8$, 8 не делится на 3;

$f(-1) = 6$, 6 делится на 3, следовательно, (–1) – корень сравнения.

Решениями сравнения $f(x) \equiv 0 (\mathrm{mod}\, 3)$ являются классы вычетов $[0]_3$ и $[-1]_3$.

Для сравнения $f_1(x)\equiv 0(\mathrm{mod}3)$ имеем $f_1(0)=0$, $f_1(1)=2$, $f_1(-1)=0$. Т. е. решениями этого сравнения являются классы вычетов $[0]_3$ и $[-1]_3$.

Вывод: т. к. решения совпадают, то сравнения $f(x)\equiv 0(\mathrm{mod}3)$ и $f_1(x)\equiv 0(\mathrm{mod}3)$ равносильны.

Теорема 7. *Если к обеим частям сравнения* $f(x)\equiv g(x)(\mathrm{mod}\,m)$ *прибавить любой многочлен* $h(x)$ *с целыми коэффициентами, то получится сравнение, равносильное данному.*

Доказательство. Пусть c – одно из решений сравнения $f(x)\equiv g(x)(\mathrm{mod}\,m)$, тогда из истинных числовых сравнений $f(c)\equiv g(c)(\mathrm{mod}\,m)$ и $h(c)\equiv h(c)(\mathrm{mod}\,m)$ получаем истинное числовое сравнение $f(c)+h(c)\equiv g(c)+h(c)(\mathrm{mod}\,m)$, т. е. c – решение сравнения $f(x)+h(x)\equiv g(x)+h(x)(\mathrm{mod}\,m)$. И наоборот, решение d сравнения $f(x)+h(x)\equiv g(x)+h(x)(\mathrm{mod}\,m)$ является решением сравнения $f(x)\equiv g(x)(\mathrm{mod}\,m)$. Следовательно, сравнения $f(x)\equiv g(x)(\mathrm{mod}\,m)$ и $f(x)+h(x)\equiv g(x)+h(x)(\mathrm{mod}\,m)$ равносильны. ■

Теорема 8. *Если обе части сравнения* $f(x)\equiv g(x)(\mathrm{mod}\,m)$ *умножить на одно и то же целое число, взаимно простое с модулем, то получится сравнение, равносильное данному.*

Доказательство. Пусть $(k,m)=1$ и c – корень сравнения $f(x)\equiv g(x)(\mathrm{mod}\,m)$, т. е. $f(c)\equiv g(c)(\mathrm{mod}\,m)$ – истинное числовое сравнение. По свойству 5 числовое сравнение $k\cdot f(c)\equiv k\cdot g(c)(\mathrm{mod}\,m)$ является истинным. Из этого следует, что число c – корень сравнения $k\cdot f(x)\equiv k\cdot g(x)(\mathrm{mod}\,m)$.

Если же число d – корень сравнения $k\cdot f(x)\equiv k\cdot g(x)(\mathrm{mod}\,m)$, то числовое сравнение $k\cdot f(d)\equiv k\cdot g(d)(\mathrm{mod}\,m)$ истинно. По определению числового сравнения разность $[k\cdot f(d)-k\cdot g(d)]$ делится на m, следовательно, произведение $k\cdot[f(d)-g(d)]$ делится на m. Т. к. по условию $(k,m)=1$, то на m делится разность $[f(d)-g(d)]$. Из этого условия получаем истинное сравнение $f(d)\equiv g(d)(\mathrm{mod}\,m)$, откуда d – корень сравнения $f(x)\equiv g(x)(\mathrm{mod}\,m)$. Вывод: сравнения $f(x)\equiv g(x)(\mathrm{mod}\,m)$ и $k\cdot f(x)\equiv k\cdot g(x)(\mathrm{mod}\,m)$ равносильны. ■

Теорема 9. *Если обе части сравнения и модуль умножить на одно и то же натуральное число, то получится сравнение, равносильное данному.*

Доказательство. Пусть дано сравнение $f(x)\equiv g(x)(\mathrm{mod}\,m)$ и натуральное число n. Если число c – корень сравнения $f(x)\equiv g(x)(\mathrm{mod}\,m)$, то имеем истинное числовое сравнение $f(c)\equiv g(c)(\mathrm{mod}\,m)$, откуда $f(c)-g(c)=m\cdot t$. Умножим обе части этого равенства на натуральное число n, получим равенство $[f(c)-g(c)]\cdot n=(m\cdot t)\cdot n$ или $f(c)\cdot n-g(c)\cdot n=(m\cdot n)\cdot t$, т. е. разность чисел $f(c)\cdot n-g(c)\cdot n$ делится на натуральное число $m\cdot n$, поэтому справедливо сравнение $f(c)\cdot n\equiv g(c)\cdot n(\mathrm{mod}\,m\cdot n)$. Из истинности этого сравнения получаем, что число c – корень сравнения $f(x)\cdot n\equiv g(x)\cdot n(\mathrm{mod}\,m\cdot n)$.

Если число d – корень сравнения $f(x)\cdot n\equiv g(x)\cdot n(\mathrm{mod}\,m\cdot n)$, то истинно числовое сравнение $f(d)\cdot n\equiv g(d)\cdot n(\mathrm{mod}\,m\cdot n)$. По свойству 7 обе части сравнения и модуль можно разделить на их общий делитель натуральное число n, тогда получаем истинное числовое сравнение $f(d)\equiv g(d)(\mathrm{mod}\,m)$. Т. е. число d – корень сравнения $f(x)\equiv g(x)(\mathrm{mod}\,m)$.

Вывод: сравнения $f(x)\equiv g(x)(\mathrm{mod}\,m)$ и $f(x)\cdot n\equiv g(x)\cdot n(\mathrm{mod}\,m\cdot n)$ равносильны. ■

Упражнения для самостоятельного решения

1. Выделить равносильные среди сравнений $5x^4-3x+6\equiv 0(\mathrm{mod}\,5)$, $7x-1\equiv 3(\mathrm{mod}\,5)$, $-6x^3+2x^2+x\equiv -4(\mathrm{mod}\,5)$, $5x^4-3x+6\equiv 0(\mathrm{mod}\,25)$.
2. Для сравнения $145x^6+4x^4-37x\equiv -27(\mathrm{mod}\,7)$ указать равносильное с наименьшими неотрицательными коэффициентами; с наименьшими по абсолютной величине коэффициентами; с четными коэффициентами; с нечетными коэффициентами.
3. Указать, при помощи каких преобразований из сравнения $45x^6-2x^3+36x\equiv -54(\mathrm{mod}\,9)$ получено сравнение $7(x^3-9)\equiv 0(\mathrm{mod}\,9)$.

4. СРАВНЕНИЯ ПЕРВОЙ СТЕПЕНИ

ОПРЕДЕЛЕНИЕ. Степенью сравнения $a_n x^n + ... + a_1 x + a_0 \equiv 0 (\mathrm{mod}\, m)$ называется наивысший показатель степени, коэффициент при котором не делится на m.

Если в сравнении все коэффициенты делятся на m, то говорят, что сравнение не имеет степени. Решением таких сравнений является все множество Z целых чисел.

Из определения степени сравнения следует, что сравнение первой степени (линейное сравнение) имеет вид $ax \equiv b (\mathrm{mod}\, m)$, где $a \neq m \cdot t \ \ \forall t \in Z$. Выясним, сколько решений может иметь линейное сравнение и как эти решения можно найти.

Теорема 10. *Если в сравнении* $ax \equiv b (\mathrm{mod}\, m)$ *коэффициент* a *и модуль* m *не взаимно просты, а число* b *не делится на НОД*(a,m)*, то сравнение решений не имеет.*

Доказательство (от противного). *Предположим*, что сравнение $ax \equiv b (\mathrm{mod}\, m)$ имеет решение, т. е. найдется такое целое число c, что истинным будет числовое сравнение $a \cdot c \equiv b (\mathrm{mod}\, m)$. Имеем равенство $a \cdot c - b = m \cdot t$, где $t \in Z$. Т. к. a и m не взаимно просты, то $(a,m) = d \neq 1$ и $a = d \cdot a_1$, $m = d \cdot m_1$. Из этих условий $b = d(a_1 \cdot c - m_1 \cdot t)$, т. е. $b \vdots d$, что противоречит условию. Следовательно, наше предположение оказалось неверным. Теорема доказана. ■

Из данной теоремы следует, что необходимо искать решения только тех линейных сравнений $ax \equiv b (\mathrm{mod}\, m)$, в которых число b делится на наибольший общий делитель коэффициента a и модуля m. Если $(a,m) = d$ и $b \vdots d$, то по свойству 7 имеем сравнение $a_1 \cdot x \equiv b_1 (\mathrm{mod}\, m_1)$, которое равносильно исходному, причем $(a_1, m_1) = 1$. Это означает, что при решении линейного сравнения получаем сравнение, в котором коэффициент при неизвестном и модуль являются взаимно простыми числами. Поэтому рассмотрим решение линейного сравнения $ax \equiv b (\mathrm{mod}\, m)$, где $(a,m) = 1$.

Теорема 11. *Если* $(a,m)=1$, *то сравнение* $ax\equiv b(\mathrm{mod}\,m)$ *имеет единственное решение.*

Доказательство. Рассмотрим полную систему вычетов $\{x_1,x_2,...,x_m\}_m$. По свойству 14 при $(a,m)=1$ полной системой вычетов будет и множество $\{ax_1,ax_2,...,ax_m\}_m$. Т. к. любое целое число входит только в один класс вычетов по модулю m, то существует единственное ax_i, $i\in\{1,2,...,m\}$ такое, что $ax_i\equiv b(\mathrm{mod}\,m)$.

Найдем решение сравнения $ax\equiv b(\mathrm{mod}\,m)$, где $(a,m)=1$, используя теорему Эйлера.

Т. к. $(a,m)=1$, то $a^{\varphi(m)}\equiv 1(\mathrm{mod}\,m)$. Умножив обе части данного сравнения на b, получим $b\cdot a^{\varphi(m)}\equiv b(\mathrm{mod}\,m)$ или $a\cdot\left(b\cdot a^{\varphi(m)-1}\right)\equiv b(\mathrm{mod}\,m)$. Следовательно, $x\in\left[b\cdot a^{\varphi(m)-1}\right]_m$, причем это решение единственное. ■

Пример.

Решить сравнение $11x\equiv 3(\mathrm{mod}15)$.

Решение: т. к. $(11,15)=1$, то сравнение имеет единственное решение $\left[3\cdot 11^{\varphi(15)-1}\right]_{15}$. Найдем наименьший неотрицательный вычет этого класса.

$\varphi(15)=\varphi(3)\cdot\varphi(5)=2\cdot 4=8$;

$3\cdot 11^7\equiv r(\mathrm{mod}15)$;

$11\equiv -4(\mathrm{mod}15)$;

$11^2\equiv 16\equiv 1(\mathrm{mod}15)$;

$11^6\equiv 1(\mathrm{mod}15)$;

$11^7\equiv 11(\mathrm{mod}15)$;

$3\cdot 11^7\equiv 33\equiv 3(\mathrm{mod}15)$.

Ответ: $x\in[3]_{15}$.

Рассмотрим случай, когда в сравнении $ax\equiv b(\mathrm{mod}\,m)$ коэффициент a и модуль m имеют наибольший общий делитель d, отличный от единицы и $b\vdots d$.

Теорема 12. *Если* $(a,m)=d>1$ *и* $b \vdots d$, *то сравнение* $ax \equiv b(\mathrm{mod}\, m)$ *имеет* d *различных решений. Все решения образуют один класс по модулю* $\frac{m}{d}$.

Доказательство. Из условия имеем, что $a=d\cdot a_1$, $m=d\cdot m_1$, $b=d\cdot b_1$, где $(a_1,m_1)=1$. Тогда исходное сравнение равносильно сравнению $a_1\cdot x \equiv b_1(\mathrm{mod}\, m_1)$, которое имеет единственное решение $[c]_{m_1}$. Это означает, что числовое сравнение $a_1\cdot c \equiv b_1(\mathrm{mod}\, m_1)$ – истинно. По теореме 9 равносильное сравнение $ax \equiv b(\mathrm{mod}\, m)$ имеет то же решение $[c]_m$. Рассмотрим числовую последовательность $[x_0]_{m_1}$, где $x_0 \equiv c(\mathrm{mod}\, m_1)$ и x_0 – наименьший неотрицательный вычет класса $[c]_{m_1}$:

$$
\begin{array}{ccccccc}
\ldots & \downarrow & x_0-dm_1, & \downarrow & x_0, & \downarrow & x_0+dm_1, \quad \ldots \\
 & \downarrow & x_0-(d-1)m_1, & \downarrow & x_0+m_1, & \downarrow & x_0+(d+1)m_1, \\
 & \downarrow & x_0-(d-2)m_1, & \downarrow & x_0+2m_1, & \downarrow & x_0+(d+2)m_1, \\
 & \downarrow & \ldots, & \downarrow & \ldots, & \downarrow & \ldots, \\
 & \downarrow & x_0-2m_1, & \downarrow & x_0+(d-2)m_1, & \downarrow & x_0+(2d-2)m_1, \\
 & \downarrow & x_0-m_1, & \downarrow & x_0+(d-1)m_1, & \downarrow & x_0+(2d-1)m_1, \\
 & \downarrow & & \downarrow & & \downarrow &
\end{array}
$$

Замечаем, что числа последовательности образуют таблицу, состоящую из бесконечного числа столбцов и d строк.

Множество чисел первой строки $\{\ldots, x_0-dm_1, x_0, x_0+dm_1, \ldots\}=\{\ldots, x_0-m, x_0, x_0+m, \ldots\}$ есть класс вычетов $[x_0]_m$ по модулю $d\cdot m_1=m$. Аналогично в каждой из строк находятся целые числа, образующие класс вычетов по модулю $d\cdot m_1=m$. Следовательно, класс вычетов $[x_0]_{m_1}$ можно представить в виде объединения классов $[x_0]_m$, $[x_0+m_1]_m$, …, $[x_0+(d-1)m_1]_m$.

Вывод: классы вычетов $[x_0]_m$, $[x_0+m_1]_m$, …, $[x_0+(d-1)m_1]_m$ – решения сравнения $ax \equiv b(\mathrm{mod}\, m)$. Эти решения образуют один класс $[x_0]_{m_1}$, где $m_1=\frac{m}{d}$.■

Пример.

Решить сравнение $12x \equiv 6 (\mathrm{mod} 9)$.

Способ 1 (метод проб). $\{-4,-3,-2,-1,0,1,2,3,4\}_9$ – полная система вычетов по модулю 9.

$12 \cdot (-4) = -48$, $-48-6 = -54 = 9 \cdot (-6)$, т. е. $[-4]_9$ – решение сравнения;

$12 \cdot (-3) = -36$, $-36-6 = -42 = 9 \cdot (-5)+3$, -42 на 9 не делится;

$12 \cdot (-2) = -24$, $-24-6 = -30 = 9 \cdot (-4)+6$, -30 на 9 не делится;

$12 \cdot (-1) = -12$, $-12-6 = -18 = 9 \cdot (-3)$, т. е. $[-1]_9$ – решение сравнения;

$12 \cdot 0 = 0$, $0-6 = -6 = 9 \cdot (-1)+3$, -6 на 9 не делится;

$12 \cdot 1 = 12$, $12-6 = 6 = 9 \cdot 0+6$, 6 на 9 не делится;

$12 \cdot 2 = 24$, $24-6 = 18 = 9 \cdot 2$, т. е. $[2]_9$ – решение сравнения;

$12 \cdot 3 = 36$, $36-6 = 30 = 9 \cdot 3+3$, 30 на 9 не делится;

$12 \cdot 4 = 48$, $48-6 = 42 = 9 \cdot 4+6$, 42 на 9 не делится.

Ответ: $[-4]_9$, $[-1]_9$, $[2]_9$.

Способ 2. $(12;9) = 3$ и $6 \vdots 3$, сравнение имеет 3 решения.

Сравнение $4x \equiv 2 (\mathrm{mod} 3)$ равносильно исходному сравнению. Заменим коэффициент 4 на 1 (т. к. $4 \equiv 1 (\mathrm{mod} 3)$), получается сравнение $x \equiv 2 (\mathrm{mod} 3)$. Следовательно, класс вычетов $[2]_3$ – решение последнего сравнения. Тогда решениями исходного сравнения являются классы $[2]_9$, $[2+1 \cdot 3]_9 = [5]_9 = [-4]_9$, $[2+2 \cdot 3]_9 = [8]_9 = [-1]_9$.

Ответ: $[-4]_9$, $[-1]_9$, $[2]_9$.

Рассмотрим еще некоторые способы решения линейного сравнения с одним неизвестным.

Пусть дано сравнение $ax \equiv b (\mathrm{mod}\, m)$, где $(a;m) = 1$. Тогда несократимая дробь $\frac{m}{a}$ может быть представлена в виде следующей конечной цепной дроби

$$\frac{m}{a}=[q_1;q_2,...,q_n]=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\cfrac{1}{\ddots\cfrac{}{}\cfrac{}{q_{n-1}+\cfrac{1}{q_n}}}}}.$$

Из свойств подходящих дробей цепной дроби следует равенство $m\cdot Q_{n-1}-a\cdot P_{n-1}=(-1)^n$, где $\frac{P_{n-1}}{Q_{n-1}}$ – подходящая дробь[5] порядка $n-1$ данной цепной дроби. Из равенства $-a\cdot P_{n-1}-(-1)^n=m\cdot Q_{n-1}$ получаем сравнение $-a\cdot P_{n-1}\equiv(-1)^n(\mathrm{mod}\,m)$ или $a\cdot P_{n-1}\equiv(-1)^{n-1}(\mathrm{mod}\,m)$. Отсюда имеем $a\cdot\left((-1)^{n-1}P_{n-1}\cdot b\right)\equiv\left((-1)^{n-1}\right)^2\cdot b\equiv b(\mathrm{mod}\,m)$. Следовательно, единственным решением исходного сравнения является класс, содержащий вычет $x=(-1)^{n-1}\cdot P_{n-1}\cdot b$.

Пример.

Решить сравнение $111x\equiv 75(\mathrm{mod}\,322)$.

Несократимая дробь $\frac{322}{111}$ представима в виде конечной цепной дроби $2+\cfrac{1}{1+\cfrac{1}{9+\cfrac{1}{11}}}=[2;1,9,11]$. Вычислим числители подходящих дробей, для этого составим таблицу:

n		1	2	3	4
q_n	0	2	1	9	11
P_n	1	2	3	29	322

Получаем $n=4$ и $P_3=29$, следовательно, $x=(-1)^3\cdot 29\cdot 75\equiv -2175\equiv 79(\mathrm{mod}\,322)$.

Ответ: $[79]_{322}$.

Рассмотрим сравнение $ax\equiv b(\mathrm{mod}\,p)$, где p – простое число и $0<a<p$. Тогда сравнение имеет решение $x\equiv b\cdot(-1)^{a-1}\cdot\frac{1}{p}\cdot C_p^a(\mathrm{mod}\,p)$, где $C_p^a=\frac{p!}{(p-a)!\cdot a!}$.

[5] Правила вычисления подходящих дробей см.: Лекции по теории чисел : учеб. пособие для студентов вузов. – М. : ФИЗМАТЛИТ, 2007. – 192 с. – § 2. – П. 9.

Пример.

Решить сравнение $8x \equiv 5(\mathrm{mod}11)$.

Вычисляем $C_{11}^{8} = \frac{11!}{3!\cdot 8!} = \frac{9\cdot 10\cdot 11}{1\cdot 2\cdot 3} = 3\cdot 5\cdot 11 = 165$;

$x \equiv 5\cdot(-1)^{7}\cdot\frac{1}{11}\cdot 165 \equiv -75 \equiv 2(\mathrm{mod}11)$.

Ответ: $[2]_{11}$.

Упражнения для самостоятельного решения

Решить сравнения:

1) $147x - 56 \equiv 24(\mathrm{mod}11)$;

2) $12x \equiv 67(\mathrm{mod}17)$;

3) $15x - 43 \equiv 43x(\mathrm{mod}11)$;

4) $35x \equiv 46(\mathrm{mod}\,21)$;

5) $36x \equiv 81(\mathrm{mod}\,45)$;

6) $63x \equiv 15(\mathrm{mod}\,36)$.

5. РЕШЕНИЕ ЛИНЕЙНЫХ УРАВНЕНИЙ С ДВУМЯ НЕИЗВЕСТНЫМИ

Уравнение вида $ax + by = c$, где a, b и c целые числа, называется линейным неопределенным (или диофантовым[6]) уравнением. Решить такое уравнение – значит найти все упорядоченные пары целых чисел $(x_0; y_0)$, удовлетворяющие условию $ax_0 + by_0 = c$.

Рассмотрим один из способов решения неопределенных линейных уравнений с двумя неизвестными – применение теории сравнений.

Из уравнения $ax + by = c$ получаем равенство $ax - c = -by$. Т. к. все числа, входящие в это равенство, целые, то имеем, что разность $ax - c$ делится на b. Следовательно, от решения уравнения переходим к решению сравнения

[6] Названо по имени Диофанта (вероятно, 3 в.) – древнегреческого математика из Александрии.

$ax \equiv c(\mathrm{mod}\, b)$. Данное сравнение, а следовательно, и уравнение будет иметь решение только тогда, когда $c \vdots (a;b)$.

Если $(a;b)=1$, то сравнение $ax \equiv c(\mathrm{mod}\, b)$ имеет единственное решение $x \equiv x_0(\mathrm{mod}\, b)$, или $x = x_0 + b \cdot t$, где $t \in Z$. Подставим найденное выражение для x в уравнение $a(x_0 + b \cdot t) + by = c$, откуда $y = \dfrac{c - a(x_0 + b \cdot t)}{b} = \dfrac{c - a \cdot x_0}{b} - a \cdot t$. Обозначим $y_0 = \dfrac{c - a \cdot x_0}{b}$. Окончательно получаем решение уравнения

$\begin{cases} x = x_0 + b \cdot t \\ y = y_0 - a \cdot t \end{cases}$, $t \in Z$.

Если $(a;b) = d$, $d > 1$ и $c \vdots d$, то имеем уравнение $d \cdot a_1 \cdot x + d \cdot b_1 \cdot y = d \cdot c_1$, все слагаемые которого делятся на d, причем $(a_1;b_1)=1$. Значит, решение уравнения $ax + by = c$ сведется к решению уравнения $a_1 x + b_1 y = c_1$.

Примеры.

1. Решить в целых числах уравнение $14x - 23y = 6$.

Т. к. $(14;23)=1$, то уравнение имеет решение в целых числах. Из уравнения выразим слагаемое с неизвестным, при котором коэффициент имеет меньшее значение.

$23y + 6 = 14x$,

$23y - (-6) = 14x$, следовательно,

$23y \equiv -6 = (\mathrm{mod}14)$,

$-5y \equiv -20(\mathrm{mod}14)$, т. к. $23 \equiv -5(\mathrm{mod}14)$ и $-6 \equiv -20(\mathrm{mod}14)$,

обе части сравнения можно разделить на 5 (по свойству 8), получаем сравнение

$y \equiv 4(\mathrm{mod}14)$, откуда $y = 4 + 14t,\ t \in Z$.

Подставим найденное значение y в уравнение: $23(4 + 14t) + 6 = 14x$.

$x = \dfrac{23 \cdot 4 + 6}{14} + 23t$, $x = 7 + 23t$, $t \in Z$.

Решение уравнения запишем в виде системы

$\begin{cases} x = 7 + 23t \\ y = 4 + 14t \end{cases}$, $t \in Z$.

Ответ: $(7 + 23t; 4 + 14t)$, $t \in Z$.

2. Сколько контейнеров вместимостью 160 и 180 кг понадобится для перевозки груза общим весом 3 тонны?

Пусть понадобится x контейнеров по 160 кг и y контейнеров по 180 кг. Тогда для x и y выполняются условия

$\begin{cases} 0 < x \le \left[\dfrac{3000}{160}\right] \\ 0 < y \le \left[\dfrac{3000}{180}\right] \end{cases}$, здесь $[k]$ – целая часть числа k.

$$\begin{cases} 0 < x \le 18 \\ 0 < y \le 16 \end{cases}.$$

Составляем уравнение $160x + 180y = 3000$, здесь $(160;180) = 20$ и $3000 \vdots 20$.

$8x + 9y = 15$,

$9y - 15 = -8x$,

$9y \equiv 15 (\mathrm{mod} 8)$, обе части заменим на меньшие вычеты,

$y \equiv 7 (\mathrm{mod} 8)$, откуда $y = 7 + 8t$, $t \in Z$,

$x = \dfrac{9(7 + 8t) - 15}{-8} = 6 - 9t$.

$\begin{cases} x = 6 - 9t \\ y = 7 + 8t \end{cases}$, $t \in Z$.

$\begin{cases} 0 < 6 - 9t \le 18 \\ 0 < 7 + 8t \le 16 \end{cases}$,

$\left\{ \begin{array}{l} -\dfrac{4}{3} \le t < \dfrac{2}{3} \\ -\dfrac{7}{8} < t \le \dfrac{9}{8} \end{array} \right. \Rightarrow t = 0$.

Подставляем найденное значение $t = 0$ и находим $\begin{cases} x = 6 \\ y = 7 \end{cases}$.

Ответ: 6 контейнеров по 160 кг и 7 контейнеров по 180 кг.

Упражнения для самостоятельного решения

1. Решить в целых числах уравнения:

   1) $15x-23y=13$;

   2) $25x+60y=15$;

   3) $32x+56y=28$.

2. Найти корни уравнения $12x-13y=14$, сумма которых имеет наименьшее положительное значение.
3. (Старинная китайская задача). На 100 монет надо купить 100 птиц: кур, петухов и цыплят. Одна курица стоит 5 монет, один петух – 4 монеты, 4 цыпленка – 1 монету. Сколько кур, петухов и цыплят купили?
4. Указать значения параметра a, при которых уравнение $18x+ay=27$

   1) не имеет решений в целых числах;

   2) имеет решения в целых числах.

6. СИСТЕМЫ СРАВНЕНИЙ ПЕРВОЙ СТЕПЕНИ

Рассмотрим систему линейных сравнений

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

Решить систему сравнений – значит найти все такие значения неизвестной x, которые удовлетворяют как первому, так и второму сравнению.

Пусть модули m_1 и m_2 имеют наибольший общий делитель $(m_1, m_2) = d$ и наименьшее общее кратное $[m_1, m_2] = M$.

Теорема 13. *Если $c_2 - c_1$ не делится на d, то система сравнений* $\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \end{cases}$ *не имеет решений.*

Доказательство. Из первого сравнения системы $x \equiv c_1 (m_1)$ получаем $x = c_1 + m_1 \cdot t,\ t \in Z$. Для нахождения решений системы необходимо найти такие

целые значения t, при которых получившиеся значения x удовлетворяли бы и второму сравнению системы, т. е. выполнялось бы условие $c_1 + m_1 \cdot t \equiv c_2 (\mathrm{mod}\, m_2)$ или $m_1 \cdot t \equiv c_2 - c_1 (\mathrm{mod}\, m_2)$. Получили линейное сравнение с неизвестной t, в котором $(m_1, m_2) = d$. Данное сравнение будет иметь решения только тогда, когда $(c_2 - c_1) \vdots d$.■

Теорема 14. *Если система сравнений*

$$\begin{cases} x \equiv c_1 (\mathrm{mod}\, m_1) \\ x \equiv c_2 (\mathrm{mod}\, m_2) \end{cases}$$

имеет решения, то они составляют единственный класс вычетов по модулю $[m_1, m_2] = M$.

Доказательство. Данная система имеет решения только тогда, когда $c_2 - c_1$ делится на d. Тогда по теореме 12 сравнение $m_1 \cdot t \equiv c_2 - c_1 (\mathrm{mod}\, m_2)$ имеет решение, которое является классом вычетов по модулю $\frac{m_2}{d}$, т. е. $t = t_0 + \frac{m_2}{d} \cdot q,\ q \in Z$. Подставим это выражение t в x, получим $x = c_1 + m_1 \cdot t = c_1 + m_1 \cdot \left(t_0 + \frac{m_2}{d} \cdot q \right) = (c_1 + m_1 \cdot t_0) + \frac{m_1 \cdot m_2}{d} \cdot q$. Но число $\frac{m_1 \cdot m_2}{d}$ – это наименьшее общее кратное модулей m_1 и m_2, следовательно, $x = (c_1 + m_1 \cdot t_0) + M \cdot q,\ q \in Z$. Обозначим $c_1 + m_1 \cdot t_0 = x_0$, окончательно имеем $x = x_0 + M \cdot q$ или $x \in [x_0]_M$.■

Примеры.

1. Решить систему сравнений $\begin{cases} 3x \equiv 1 (\mathrm{mod}\, 5) \\ 5x \equiv 4 (\mathrm{mod}\, 7) \end{cases}$.

Первое сравнение $3x \equiv 1 (\mathrm{mod}\, 5)$ системы решим методом замены вычетов.

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

$x \equiv 2 (\mathrm{mod}\, 5)$ т. к. $(3;6) = 3$ и $(5;3) = 1$,

$x = 2 + 5t,\ t \in Z$, подставим выражение x во второе сравнение системы:

$5(2 + 5t) \equiv 4 (\mathrm{mod}\, 7)$,

$25t \equiv -6 (\mathrm{mod}\, 7)$, сравнение имеет решение, т. к. $(25;7)=1$,

$4t \equiv 8 (\mathrm{mod}\, 7)$,

$t \equiv 2 (\mathrm{mod}\, 7)$, следовательно, $t = 2 + 7q,\ q \in Z$,

$x = 2 + 5t = 2 + 5(2 + 7q) = 12 + 35q,\ q \in Z$.

Ответ: $x \in [12]_{35}$.

2. Решить систему сравнений $\begin{cases} 3x \equiv 1 (\mathrm{mod}\, 20) \\ 2x \equiv 3 (\mathrm{mod} 15) \end{cases}$.

$3x \equiv 1 (\mathrm{mod}\, 20)$ имеет решения, т. к. $(3;20)=1$,

$3x \equiv 21 (\mathrm{mod}\, 20)$,

$x \equiv 7 (\mathrm{mod}\, 20)$,

$x = 7 + 20t,\ t \in Z$,

$2(7 + 20t) \equiv 3 (\mathrm{mod} 15)$,

$40t \equiv -11 (\mathrm{mod} 15)$ решений не имеет, т. к. $(40;15)=5$ и (-11) не делится на 5.

Ответ: Система решений не имеет.

Система сравнений примера 2 может быть решена иначе.

$$\begin{cases} 3x \equiv 1 (\mathrm{mod}\, 20) \\ 2x \equiv 3 (\mathrm{mod} 15) \end{cases} \Leftrightarrow \begin{cases} x \equiv 7 (\mathrm{mod}\, 20) \\ x \equiv 9 (\mathrm{mod} 15) \end{cases},$$

т. к. $(20;15)=5$ и $9 - 7 \neq 5l,\ l \in Z$, то система решений не имеет.

3. Решить систему сравнений $\begin{cases} 2x \equiv -1 (\mathrm{mod}\, 5) \\ -5x \equiv 3 (\mathrm{mod}\, 6) \\ 11x \equiv 5 (\mathrm{mod}\, 8) \end{cases}$.

$2x \equiv -1 \equiv 4 (\mathrm{mod}\, 5) \xrightarrow{(2;5)=1} x \equiv 2 (\mathrm{mod}\, 5),\ x = 2 + 5t,\ t \in Z$;

$-5(2 + 5t) \equiv 3 (\mathrm{mod}\, 6) \rightarrow -25t \equiv 13 (\mathrm{mod}\, 6) \xrightarrow{(-25;6)=1} -t \equiv 1 (\mathrm{mod}\, 6) \rightarrow$

$t \equiv -1 (\mathrm{mod}\, 6),\ t = -1 + 6q,\ q \in Z$;

$x = 2 + 5(-1 + 6q) = -3 + 30q,\ q \in Z$;

$11(-3 + 30q) \equiv 5 (\mathrm{mod}\, 8) \rightarrow 330q \equiv 38 (\mathrm{mod}\, 8) \xrightarrow{(330;38)=2,8:2} 165q \equiv 19 (\mathrm{mod}\, 4) \rightarrow$

$q \equiv 3 (\mathrm{mod}\, 4),\ q = 3 + 4l,\ l \in Z$;

$x = -3 + 30q = -3 + 30(3 + 4l) = 87 + 120l,\ l \in Z$.

Ответ: $x \in [87]_{120}$.

Упражнения для самостоятельного решения

1. Решить системы сравнений:

1) $\begin{cases} 3x \equiv 7 (\mathrm{mod} 11) \\ 2x \equiv -3 (\mathrm{mod} 7) \end{cases}$; 2) $\begin{cases} 23x + 1 \equiv -3x (\mathrm{mod} 5) \\ 12x \equiv 16 (\mathrm{mod} 28) \end{cases}$;

3) $\begin{cases} x \equiv -15 (\mathrm{mod} 12) \\ 3x \equiv 8 (\mathrm{mod} 14) \\ x \equiv 21 (\mathrm{mod} 28) \end{cases}$; 4) $\begin{cases} 5x \equiv -136 (\mathrm{mod} 9) \\ 21x \equiv 23 (\mathrm{mod} 11) \\ 15x \equiv 14 (\mathrm{mod} 13) \end{cases}$.

2. При каких значениях параметра k имеют решения системы сравнений:

1) $\begin{cases} 23x \equiv -14k (\mathrm{mod} 13) \\ 32x \equiv 25 (\mathrm{mod} 7) \end{cases}$; 2) $\begin{cases} 4x \equiv 51 (\mathrm{mod} 11) \\ 3x \equiv 10 (\mathrm{mod} k) \end{cases}$?

7. СРАВНЕНИЯ ВЫСШИХ СТЕПЕНЕЙ

Рассмотрим многочлен $f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$ с целыми коэффициентами. Пусть p – простое число и a_n не делится на p, тогда сравнение $f(x) \equiv 0 (\mathrm{mod}\, p)$ – сравнение степени n.

Теорема 15. *Сравнение* $f(x) \equiv 0 (\mathrm{mod}\, p)$ *равносильно сравнению степени не выше* $p-1$.

Доказательство. Если $n < p$, то теорема очевидна. Если же $n \geq p$, то многочлен $f(x)$ разделим на многочлен $x^p - x$, получим $f(x) = (x^p - x) \cdot g(x) + r(x)$, где степень остатка $r(x)$ меньше p, т. е. не больше $p-1$. По теореме 2 Ферма для любого целого x истинно сравнение $x^p \equiv x (\mathrm{mod}\, p)$, откуда по определению сравнения $(x^p - x) \vdots p$. Т. к. в сравнении $(x^p - x) \cdot g(x) + r(x) \equiv 0 (\mathrm{mod}\, p)$ первое слагаемое правой части делится на p, то это сравнение равносильно сравнению $r(x) \equiv 0 (\mathrm{mod}\, p)$, которое имеет степень не выше $p-1$.

Из доказательства теоремы ясно, что для поиска равносильного сравнения по модулю p, имеющего меньшую степень, можно найти остаток от деления $f(x)$ на $x^p - x$. Но этот способ не всегда приемлем, особенно,

когда многочлен $f(x)$ имеет большую степень. Для понижения степени сравнения при $n \geq p$ воспользуемся следующими рассуждениями. Сравнение $a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 \equiv 0 (\mathrm{mod}\, p)$ можно представить как сумму сравнений $a_n x^n \equiv 0 (\mathrm{mod}\, p)$, $a_{n-1} x^{n-1} \equiv 0 (\mathrm{mod}\, p)$, …, $a_1 x \equiv 0 (\mathrm{mod}\, p)$ и $a_0 \equiv 0 (\mathrm{mod}\, p)$. Пусть $f(x) = (x^p - x) \cdot g(x) + r(x)$ и r, степень остатка $r(x)$, удовлетворяет условию $1 \leq r \leq p-1$. Тогда, разделив показатель степени n на $p-1$ с остатком, получим $n = (p-1) \cdot k + r$. Действительно, из сравнения $x \equiv x^p (\mathrm{mod}\, p)$ получаем сравнение $x^r \equiv x^{(p-1)+r} (\mathrm{mod}\, p)$, затем сравнение $x^{(p-1)+r} \equiv x^{2(p-1)+r} (\mathrm{mod}\, p)$. В силу свойства 3 имеем истинное сравнение $x^r \equiv x^{(p-1)+r} \equiv x^{2(p-1)+r} (\mathrm{mod}\, p)$. Продолжив цепочку сравнений, в итоге придем к сравнению $x^r \equiv x^{k(p-1)+r} (\mathrm{mod}\, p)$, где $(p-1) \cdot k + r = n$. ■

Правило понижения степени сравнения по модулю p:

1) показатель степени i слагаемого $a_i x^i$ разделить на $p-1$ так, что остаток r_i удовлетворяет условию $1 \leq r_1 \leq p-1$;
2) слагаемое $a_i x^i$ заменить на слагаемое $a_i x^{r_i}$.

Пример.

Решить сравнение $28x^9 + 32x^8 - 26x^7 + 19x^4 - 18x + 2 \equiv 0 (\mathrm{mod}\, 3)$.

Заменим коэффициенты на сравнимые с ними по модулю 3 вычеты:

$28 \equiv 1 (\mathrm{mod}\, 3)$, $32 \equiv 2 (\mathrm{mod}\, 3)$, $-26 \equiv 1 (\mathrm{mod}\, 3)$, $19 \equiv 1 (\mathrm{mod}\, 3)$, $-18 \equiv 0 (\mathrm{mod}\, 3)$.

Модуль $p = 3$, $p - 1 = 2$, разделим показатели степеней слагаемых на 2, чтобы остатки были отличны от нуля:

$9 = 2 \cdot 4 + 1$, $8 = 2 \cdot 3 + 2$, $7 = 2 \cdot 3 + 1$, $4 = 2 \cdot 1 + 2$, заменим степени x^i на x^{r_i}.

Получаем сравнение $x^1 + 2x^2 + x^1 + 1x^2 + 2 \equiv 0 (\mathrm{mod}\, 3)$ после приведения подобных слагаемых $3x^2 + 2x + 2 \equiv 0 (\mathrm{mod}\, 3)$ или $2x + 2 \equiv 0 (\mathrm{mod}\, 3)$. Из последнего сравнения следует $2x \equiv -2 (\mathrm{mod}\, 3)$, окончательно $x \equiv -1 (\mathrm{mod}\, 3)$.

Ответ: $[-1]_3$.

Теорема 16. *Сравнение степени* n $f(x) \equiv 0 (\mathrm{mod}\, p)$, *где* $f(x) = a_n x^n + ... + a_1 x + a_0$, *имеет не более* n *решений*.

Доказательство (индукцией по n).

1) База индукции – проверим истинность утверждения теоремы при начальном значении $n=0$. По определению степени сравнения имеем, что в сравнении $a_0 \equiv 0(\bmod p)$ a_0 не делится на p, следовательно, сравнение решений не имеет.

   Если $n=1$, то получим сравнение $a_1 x + a_0 \equiv 0(\bmod p)$, в котором a_1 не делится на p, т. е. числа a_1 и p взаимно простые, поэтому сравнение $a_1 x \equiv -a_0 (\bmod p)$ имеет единственное решение.

2) Предположим, что при $n=k-1$ утверждение теоремы верно, т. е. сравнение $a_{k-1}x^{k-1} + ... + a_1 x + a_0 \equiv 0(\bmod p)$ имеет не более $k-1$ решений.

3) Шаг индукции – докажем истинность утверждения теоремы при следующем значении n, при $n=k$.

   Если сравнение $a_k x^k + ... + a_1 x + a_0 \equiv 0(\bmod p)$ имеет некоторое решение $[c]_p$, то числовое сравнение $a_k c^k + ... + a_1 c + a_0 \equiv 0(\bmod p)$ истинно. Тогда по теореме 7 сравнение $(a_k x^k + ... + a_1 x + a_0) - (a_k c^k + ... + a_1 c + a_0) \equiv 0(\bmod p)$ равносильно исходному. После группировки слагаемых получим сравнение $a_k (x^k - c^k) + ... + a_1 (x - c) \equiv 0(\bmod p)$, или $a_k (x-c)(x^{k-1} + x^{k-2} \cdot c + ... + c^{k-1}) + ... + a_2 (x-c)(x+c) + a_1 (x-c) \equiv 0(\bmod p)$.

   Вынесем общий множитель $(x-c)$ за скобки и приведем подобные слагаемые, в итоге придем к сравнению $(x-c)(b_{k-1}x^{k-1} + ... + b_1 x + b_0) \equiv 0(\bmod p)$, причем $b_{k-1} = a_k$.

   Если целое число d является решением исходного сравнения и $d \notin [c]_p$, то в произведении $(d-c)(b_{k-1}d^{k-1} + ... + b_1 d + b_0)$ на p делится множитель $(b_{k-1}d^{k-1} + ... + b_1 d + b_0)$. Следовательно, число d является решением сравнения $b_{k-1}x^{k-1} + ... + b_1 x + b_0 \equiv 0(\bmod p)$, которое имеет по предположению не более $k-1$ решений.

   Вывод: сравнение $a_k x^k + ... + a_1 x + a_0 \equiv 0(\bmod p)$ имеет не более k решений. ■

Следствие. Если сравнение степени n $(n < p)$ имеет более n решений, то все коэффициенты сравнения делятся на p.

Теорема 17 *(Вильсона). Для любого простого числа* p *справедливо сравнение* $(p-1)!+1 \equiv 0 (\mathrm{mod}\, p)$.

Доказательство. 1) Если $p = 2$, то сравнение $(2-1)!+1 \equiv 1+1 \equiv 2 \equiv 0 (\mathrm{mod}\, 2)$ истинно.

2) Если простое число $p \neq 2$, то оно нечетное. Рассмотрим многочлен $f(x) = (x-1)(x-2)\cdot\ldots\cdot(x-(p-2))(x-(p-1))$ степени $p-1$.

Сравнение $f(x) - (x^{p-1} - 1) \equiv 0 (\mathrm{mod}\, p)$ имеет степень не более $p-2$. Т. к. по теореме 1 Ферма для $(x; p) = 1$ верно сравнение $x^{p-1} \equiv 1 (\mathrm{mod}\, p)$ и $(1; p) = (2; p) = \ldots = (p-1; p) = 1$, то классы $[1]_p$, $[2]_p$, …, $[p-1]_p$ являются решениями сравнения $f(x) - (x^{p-1} - 1) \equiv 0 (\mathrm{mod}\, p)$. Получили, что число решений сравнения больше степени этого сравнения, следовательно, все коэффициенты, в том числе и свободный член, должны делиться на p. Найдем свободный член многочлена $f(x) - (x^{p-1} - 1)$:

$$(x-1)(x-2)\cdot\ldots\cdot(x-(p-2))(x-(p-1)) - (x^{p-1} - 1) =$$

$$= g(x) + (1 \cdot 2 \cdot\ldots\cdot(p-1)+1) = g(x) + ((p-1)!+1).$$

Получили, что $(p-1)!+1 \vdots p$ или $(p-1)!+1 \equiv 0 (\mathrm{mod}\, p)$. ■

Теорема 18. *Пусть* $m = m_1 \cdot m_2 \cdot\ldots\cdot m_k$, *где* $(m_i; m_j) = 1$, $i \neq j$.

Тогда: 1) сравнение $f(x) \equiv 0 (\mathrm{mod}\, m)$ *равносильно системе сравнений*

$$\begin{cases} f(x) \equiv 0 (\mathrm{mod}\, m_1) \\ \ldots\ldots\ldots\ldots \\ f(x) \equiv 0 (\mathrm{mod}\, m_k) \end{cases};$$

2) если сравнение $f(x) \equiv 0 (\mathrm{mod}\, m)$ *имеет* n *решений, а сравнения системы*

$$\begin{cases} f(x) \equiv 0 (\mathrm{mod}\, m_1) \\ \ldots\ldots\ldots\ldots \\ f(x) \equiv 0 (\mathrm{mod}\, m_k) \end{cases}, \text{ соответственно, по } n_1, n_2, \ldots, n_k,$$

то $n = n_1 \cdot n_2 \cdot\ldots\cdot n_k$.

Доказательство. 1) Покажем, что любое решение сравнения $f(x)\equiv 0(\mathrm{mod}\, m)$ является решением системы

$$\begin{cases} f(x)\equiv 0(\mathrm{mod}\, m_1) \\ \ldots\ldots\ldots\ldots \\ f(x)\equiv 0(\mathrm{mod}\, m_k) \end{cases}.$$

Пусть число c – одно из решений сравнения $f(x)\equiv 0(\mathrm{mod}\, m)$, тогда $f(c)\vdots m$. По условию $m = m_1 \cdot m_2 \cdot \ldots \cdot m_k$, следовательно, $f(c)\vdots m_i$ для всех $i \in (1,2,\ldots k)$, т. е. c – решение каждого сравнения $f(x)\equiv 0(\mathrm{mod}\, m_i)$ системы, а значит, и решение системы

$$\begin{cases} f(x)\equiv 0(\mathrm{mod}\, m_1) \\ \ldots\ldots\ldots\ldots \\ f(x)\equiv 0(\mathrm{mod}\, m_k) \end{cases}.$$

Обратно, докажем, что любое решение системы является решением сравнения $f(x)\equiv 0(\mathrm{mod}\, m)$.

Т. к. $(m_i; m_j)=1,\ i \neq j$, то наименьшее общее кратное чисел $m_1, m_2, \ldots, m_k$ равно произведению $m_1 \cdot m_2 \cdot \ldots \cdot m_k$, т. е. $[m_1, m_2, \ldots, m_k] = m$. Если многочлен $f(x)$ удовлетворяет условию

$$\begin{cases} f(x)\equiv 0(\mathrm{mod}\, m_1) \\ \ldots\ldots\ldots\ldots \\ f(x)\equiv 0(\mathrm{mod}\, m_k) \end{cases},$$

то по свойству 10 справедливо сравнение $f(x)\equiv 0(\mathrm{mod}\,[m_1, m_2, \ldots, m_k])$ или $f(x)\equiv 0(\mathrm{mod}\, m)$. Тогда решение системы будет и решением сравнения $f(x)\equiv 0(\mathrm{mod}\, m)$.

Вывод: сравнение $f(x)\equiv 0(\mathrm{mod}\, m)$ и система

$$\begin{cases} f(x)\equiv 0(\mathrm{mod}\, m_1) \\ \ldots\ldots\ldots\ldots \\ f(x)\equiv 0(\mathrm{mod}\, m_k) \end{cases}$$ равносильны.

2) Т. к. сравнение $f(x)\equiv 0(\mathrm{mod}\, m)$ и система

$$\begin{cases} f(x) \equiv 0 (\mathrm{mod}\, m_1) \\ \ldots\ldots\ldots\ldots \\ f(x) \equiv 0 (\mathrm{mod}\, m_k) \end{cases}$$

равносильны, то решением системы является класс вычетов по модулю $[m_1, m_2, ..., m_k] = m$, удовлетворяющий каждому сравнению системы. Поэтому, чтобы найти число n решений сравнения $f(x) \equiv 0 (\mathrm{mod}\, m)$, достаточно подсчитать число решений системы. ■

Следствие 1. Если хотя бы одно из сравнений не имеет решения, то и вся система, следовательно, и сравнение $f(x) \equiv 0 (\mathrm{mod}\, m)$ не имеют решения.

Следствие 2. Если в сравнении $f(x) \equiv 0 (\mathrm{mod}\, m)$ модуль m – составное число, то сравнение равносильно системе сравнений, модули которых являются степенями различных простых чисел.

Пусть каждое из сравнений $f(x) \equiv 0 (\mathrm{mod}\, m_i)$ системы имеет некоторое решение c_i, тогда исходная система сравнений равносильна системе

$$\begin{cases} x \equiv c_1 (\mathrm{mod}\, m_1) \\ \ldots\ldots\ldots\ldots \\ x \equiv c_k (\mathrm{mod}\, m_k) \end{cases},$$

которая имеет единственное решение $x \equiv x_0 (\mathrm{mod}\, m)$, следовательно, набору $(c_1; c_2; ...; c_k)$ сопоставляется x_0. Пусть сравнение $f(x) \equiv 0 (\mathrm{mod}\, m_1)$ имеет n_1 решений, сравнение $f(x) \equiv 0 (\mathrm{mod}\, m_2)$ – n_2 решений и т. д., сравнение $f(x) \equiv 0 (\mathrm{mod}\, m_k)$ – n_k решений. Тогда из этих решений можно составить $n_1 \cdot n_2 \cdot ... \cdot n_k$ различных наборов, каждый из которых соответствует некоторому решению системы, а следовательно, и сравнения $f(x) \equiv 0 (\mathrm{mod}\, m)$. Ясно, что все эти решения различны, т. к. различным наборам решений сравнений системы $(c_1; c_2; ...; c_k)$ и $(d_1; d_2; ...; d_k)$, где существует такое значение i, что $c_i \notin [d_i]_{m_i}$, соответствуют различные системы

$$\begin{cases} x \equiv c_1 (\mathrm{mod}\, m_1) \\ \ldots\ldots\ldots\ldots \\ x \equiv c_k (\mathrm{mod}\, m_k) \end{cases} \text{ и } \begin{cases} x \equiv d_1 (\mathrm{mod}\, m_1) \\ \ldots\ldots\ldots\ldots \\ x \equiv d_k (\mathrm{mod}\, m_k) \end{cases}.$$

В итоге сравнение $f(x)\equiv 0(\mathrm{mod}\, m)$ имеет $n_1\cdot n_2\cdot ...\cdot n_k$, а по условию n решений, поэтому $n=n_1\cdot n_2\cdot ...\cdot n_k$.

Пример.

Решить сравнение $19x\equiv 13(\mathrm{mod}\, 46)$.

Т. к. $(19;46)=1$, то сравнение имеет единственное решение.

Разложим модуль на взаимно простые множители $46=2\cdot 23$, тогда сравнение равносильно системе $\begin{cases}19x\equiv 13(\mathrm{mod}\, 23)\\ 19x\equiv 13(\mathrm{mod}\, 2)\end{cases}$.

Решим эту систему.

$19x\equiv 13(\mathrm{mod}\, 23)\xrightarrow{19\equiv -4(\mathrm{mod}\, 23),\,13\equiv 36(\mathrm{mod}\, 23)}\ -4x\equiv 36(\mathrm{mod}\, 23)\ \rightarrow\ x\equiv -9(\mathrm{mod}\, 23)$,

$x=-9+23l,\ l\in Z$;

$19(-9+23l)\equiv 13(\mathrm{mod}\, 2)\ \rightarrow\ 437l\equiv 184(2)\ \rightarrow\ l\equiv 0(2)\ \rightarrow\ l=2t,\ t\in Z$;

$x=-9+23\cdot 2t$, $x=-9+46t,\ t\in Z$.

Ответ: $[-9]_{46}$.

Рассмотрим сравнение $f(x)\equiv 0(\mathrm{mod}\, p^{\alpha})$, где p – простое число. Пусть целое число c – решение данного сравнения, т. е. $f(c)\vdots p^{\alpha}$, в этом случае имеем, что $f(c)$ делится на каждую из степеней $p^{\alpha-1}$, $p^{\alpha-2}$, …, p^2, p. Решения сравнения $f(x)\equiv 0(\mathrm{mod}\, p^{\alpha})$ надо искать среди решений сравнения $f(x)\equiv 0(\mathrm{mod}\, p)$.

Пусть x_0 – решение сравнения $f(x)\equiv 0(\mathrm{mod}\, p)$, тогда $x\equiv x_0(\mathrm{mod}\, p)$ и $x=x_0+p\cdot t_0$, $t_0\in Z$. Необходимо найти такие значения t_0, при которых получаются значения неизвестной x, удовлетворяющие сравнению $f(x)\equiv 0(\mathrm{mod}\, p^2)$. Разложим многочлен $f(x)=a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0$ по формуле Тейлора[7]:

$$f(x)=f(x_0)+\frac{f'(x_0)}{1!}\cdot(x-x_0)+\frac{f''(x_0)}{2!}\cdot(x-x_0)^2+...+\frac{f^{(n)}(x_0)}{n!}\cdot(x-x_0)^n+R_n.$$

[7] Фролов, С. В. Курс высшей математики. – Т. I : учебное пособие для втузов / С. В. Фролов, Р. Я. Шостак. – М. : Высшая школа, 1973. – § 14.4.

Т. к. многочлен $f(x)$ – многочлен степени n с целыми коэффициентами, то $f(x)$ в точке x_0 имеет n производных, а остаточный член R_n в формуле Тейлора при $x \to x_0$ стремится к нулю, т. е. можно считать, что $f(x) = f(x_0) + \frac{f'(x_0)}{1!} \cdot (x - x_0) + \frac{f''(x_0)}{2!} \cdot (x - x_0)^2 + \ldots + \frac{f^{(n)}(x_0)}{n!} \cdot (x - x_0)^n$. Т. к. все коэффициенты многочлена – целые числа, получаем, что $f^{(i)}(x_0) \vdots (i!)$. Подставим в разложение $f(x)$ значение $x = x_0 + p \cdot t_0$, тогда

$$f(x_0 + p \cdot t_0) = f(x_0) + \frac{f'(x_0)}{1!} \cdot p \cdot t_0 + \frac{f''(x_0)}{2!} \cdot (p \cdot t_0)^2 + \ldots + \frac{f^{(n)}(x_0)}{n!} \cdot (p \cdot t_0)^n.$$

Из равенства $f(x_0 + p \cdot t_0) = f(x_0) + \frac{f'(x_0)}{1!} \cdot p \cdot t_0 + p^2 \cdot t_0^2 \left[\frac{f''(x_0)}{2!} + \ldots + \frac{f^{(n)}(x_0)}{n!} \cdot (p \cdot t_0)^{n-2} \right]$ имеем, что сравнение $f(x_0 + p \cdot t_0) \equiv 0 \pmod{p^2}$ равносильно сравнению $f(x_0) + \frac{f'(x_0)}{1!} \cdot p \cdot t_0 \equiv 0 \pmod{p^2}$, а т. к. $f(x_0) \vdots p$, то после деления обеих частей и модуля сравнения получим равносильное сравнение $\frac{f(x_0)}{p} + f'(x_0) \cdot t_0 \equiv 0 \pmod{p}$ или $f'(x_0) \cdot t_0 \equiv -\frac{f(x_0)}{p} \pmod{p}$.

Если $f'(x_0)$ не делится на p, тогда сравнение $f'(x_0) \cdot t_0 \equiv -\frac{f(x_0)}{p} \pmod{p}$ имеет единственное решение $t_0 \equiv t_0' \pmod{p}$ или $t_0 = t_0' + p \cdot t_1, t_1 \in Z$. Тогда $x = x_0 + p \cdot t_0 = \underbrace{x_0 + p \cdot t_0'}_{x_1} + p^2 \cdot t_1 = x_1 + p^2 \cdot t_1$, $x \equiv x_1 \pmod{p^2}$, т. е. x_1 – решение сравнения $f(x) \equiv 0 \pmod{p^2}$.

Среди всех значений t_1 найдем такие, при которых получившиеся значения неизвестной x удовлетворяют сравнению $f(x) \equiv 0 \pmod{p^3}$, следовательно, и сравнению $f(x_1 + p^2 \cdot t_1) \equiv 0 \pmod{p^3}$.

В формулу Тейлора для многочлена $f(x)$ при $x \to x_1$ подставим значение $x = x_1 + p^2 \cdot t_1$, получим

$f\left(x_1+p^2\cdot t_1\right)=f\left(x_1\right)+\frac{f'\left(x_1\right)}{1!}\cdot p^2\cdot t_1+\frac{f''\left(x_1\right)}{2!}\cdot\left(p^2\cdot t_1\right)^2+\ldots+\frac{f^{(n)}\left(x_1\right)}{n!}\cdot\left(p^2\cdot t_1\right)^n$, откуда

$f\left(x_1+p^2\cdot t_1\right)=f\left(x_1\right)+\frac{f'\left(x_1\right)}{1!}\cdot p^2\cdot t_1+\left(p^2\cdot t_1\right)^2\cdot\left[\frac{f''\left(x_1\right)}{2!}+\ldots+\frac{f^{(n)}\left(x_1\right)}{n!}\cdot\left(p^2\cdot t_1\right)^{n-2}\right]$. Из последнего равенства следует сравнение $f\left(x_1\right)+f'\left(x_1\right)\cdot p^2\cdot t_1\equiv 0\left(\mathrm{mod}\,p^3\right)$, которое равносильно сравнению $f'\left(x_1\right)\cdot t_1\equiv-\frac{f\left(x_1\right)}{p^2}\left(\mathrm{mod}\,p\right)$. Т. к. $x_1=x_0+p\cdot t_0'$, то $x_0\equiv x_1\left(\mathrm{mod}\,p\right)$, откуда по свойству 18 получаем сравнения $f\left(x_0\right)\equiv f\left(x_1\right)\left(\mathrm{mod}\,p\right)$ и $f'\left(x_0\right)\equiv f'\left(x_1\right)\left(\mathrm{mod}\,p\right)$. По предположению $f'\left(x_0\right)$ не делится на p, следовательно, $f'\left(x_1\right)$ не делится на p, поэтому сравнение $f'\left(x_1\right)\cdot t_1\equiv-\frac{f\left(x_1\right)}{p^2}\left(\mathrm{mod}\,p\right)$ имеет единственное решение $t_1\equiv t_1'\left(\mathrm{mod}\,p\right)$. Получили значения $t_1=t_1'+p\cdot t_2,\ t_2\in Z$, откуда после подстановки имеем $x=x_1+p^2\cdot\left(t_1'+p\cdot t_2\right)=\underbrace{x_1+p^2\cdot t_1'}_{x_2}+p^3\cdot t_2=x_2+p^3\cdot t_2$, $t_2\in Z$, т. е. $x\equiv x_2\left(\mathrm{mod}\,p^3\right)$.

Повторяя эту цепочку решений, придем окончательно к решению $x\equiv x_{\alpha-1}\left(\mathrm{mod}\,p^\alpha\right)$.

Если $f'\left(x_0\right)$ делится на p, а $\frac{f\left(x_0\right)}{p}$ не делится на p, то сравнение $f'\left(x_0\right)\cdot t_0\equiv-\frac{f\left(x_0\right)}{p}\left(\mathrm{mod}\,p\right)$ решений не имеет, следовательно, не будут иметь решения и сравнения $f\left(x\right)\equiv 0\left(\mathrm{mod}\,p^2\right)$ и $f\left(x\right)\equiv 0\left(\mathrm{mod}\,p^\alpha\right)$.

Если $f'\left(x_0\right)$ и $\frac{f\left(x_0\right)}{p}$ делятся на p, то сравнению $f'\left(x_0\right)\cdot t_0\equiv-\frac{f\left(x_0\right)}{p}\left(\mathrm{mod}\,p\right)$ удовлетворяют любые целые значения t_0. Тогда среди чисел $x=x_0+p\cdot t_0$ надо выделить те, которые являются решениями сравнения $f\left(x\right)\equiv 0\left(\mathrm{mod}\,p^3\right)$ и т.д.

Пример.

Решить сравнение $f\left(x\right)\equiv 0\left(\mathrm{mod}125\right)$, где $f\left(x\right)=x^3-2x^2-30x+41$.

$125=5^3$,

$x^3-2x^2-30x+41\equiv 0\left(\mathrm{mod}\,5\right)\xrightarrow{30\vdots 5,\ 41\equiv 1\left(\mathrm{mod}\,5\right)}x^3-2x^2+1\equiv 0\left(\mathrm{mod}\,5\right)$;

$x^3-2x^2+1=\left(x^3-x^2\right)-\left(x^2-1\right)=\left(x-1\right)\left(x^2-x-1\right)$;

$(x-1)(x^2-x-1)\equiv 0(\mathrm{mod}5) \Leftrightarrow (x-1)(x^2-x-1)\vdots 5$, т. к. 5 – простое число, то $(x-1)\vdots 5$ или $(x^2-x-1)\vdots 5$.

Из делимости $(x-1)$ на 5 получаем сравнение $x-1\equiv 0(\mathrm{mod}5)$ или $x\equiv 1(\mathrm{mod}5)$, т. е. $x=1+5t,\ t\in Z$.

Из условия $(x^2-x-1)\vdots 5$ получаем сравнение $x^2-x-1\equiv 0(\mathrm{mod}5)$ или $x^2+4x+4\equiv 0(\mathrm{mod}5)$, откуда $(x+2)^2\equiv 0(\mathrm{mod}5)$ и $x\equiv -2(\mathrm{mod}5)$, $x=-2+5l,\ l\in Z$.

Найдем решения сравнения $f(x)\equiv 0(\mathrm{mod}125)$ при $x=1+5t,\ t\in Z$ $(x_0=1)$, для этого составим сравнение $f'(1)\cdot t\equiv -\frac{f(1)}{5}(\mathrm{mod}\ 5)$.

$f(1)=1-2-30+41=10$, $f'(x)=3x^2-4x-30$ и $f'(1)=3-4-30=-31$.

$-31t\equiv -2(\mathrm{mod}\ 5) \rightarrow t\equiv 2(\mathrm{mod}\ 5) \rightarrow t=2+5k,\ k\in Z \rightarrow$

$x=1+5(2+5k)=11+25k,\ k\in Z$, здесь $x_1=11$.

Составим сравнение $f'(11)\cdot k\equiv -\frac{f(11)}{25}(\mathrm{mod}\ 5)$.

$f(11)=11^3-2\cdot 11^2-30\cdot 11+41=800$, $f'(x)=3\cdot 11^2-4\cdot 11-30=289$,

$289k\equiv -32(\mathrm{mod}\ 5) \rightarrow k\equiv 2(\mathrm{mod}\ 5) \rightarrow k=2+5h,\ h\in Z \rightarrow$

$x=11+25(2+5h)=61+125h,\ h\in Z \rightarrow \underline{x\equiv 61(\mathrm{mod}\ 125)}$.

Найдем решения сравнения $f(x)\equiv 0(\mathrm{mod}125)$ при $x=-2+5l$.

Составим сравнение $f'(-2)\cdot l\equiv -\frac{f(-2)}{5}(\mathrm{mod}\ 5)$:

$f(-2)=(-2)^3-2\cdot(-2)^2-30\cdot(-2)+41=85$, $f'(-2)=3\cdot(-2)^2-4\cdot(-2)-30=-10$,

тогда $-10\cdot l\equiv -17(\mathrm{mod}\ 5)$. Это сравнение решений не имеет, т. к. (-17) не делится на 5, в то время как $(-10)\vdots 5$.

Ответ: $x\in[61]_{125}$.

Упражнения для самостоятельного решения

1. Записать сравнения наименьшей степени, равносильные сравнениям:

1) $34x^{12}+4x^9-23x^6-13x^4+x-16\equiv 0(\mathrm{mod}7)$;

2) $15x^{34}+2x^{19}-2x^6+24\equiv 3x^5-x(\mathrm{mod}5)$;

3) $-10x^4+236x^{34}-243x^{14}\equiv 53(\mathrm{mod}11)$.

2. Решить сравнения:

1) $21x^{10}-6x^8-15x^7+2x-9\equiv 0(\mathrm{mod}\,7)$;

2) $25x^{12}-143x^{10}+11x^9-23x^3-14x-10\equiv 0(\mathrm{mod}\,11)$.

3. Решить сравнения:

1) $42x\equiv 23(\mathrm{mod}\,143)$;

2) $-57x\equiv 63(\mathrm{mod}\,126)$.

4. Решить сравнения:

1) $5x^4-4x^3+23x-16\equiv 0(\mathrm{mod}\,32)$;

2) $17x^5+23x^4+17x^2-x+11\equiv 0(\mathrm{mod}\,81)$.

8. КВАДРАТИЧНЫЕ СРАВНЕНИЯ

ОПРЕДЕЛЕНИЕ. Сравнение вида $ax^2+bx+c\equiv 0(\mathrm{mod}\,m)$, где $a\neq m\cdot t$, называется квадратичным (или квадратным).

Это сравнение эквивалентно сравнению $4a^2x^2+4abx+4ac\equiv 0(\mathrm{mod}\,4am)$, которое после преобразования имеет вид $(2ax+b)^2\equiv b^2-4ac(\mathrm{mod}\,4am)$. Введем обозначения $2ax+b=y$ и $b^2-4ac=D$, получим двучленное сравнение $y^2\equiv D(\mathrm{mod}\,4am)$. Если двучленное сравнение $y^2\equiv D(\mathrm{mod}\,4am)$ имеет решение y_0, то $x_0=\dfrac{y_0-b}{2a}$ является решением сравнения $ax^2+bx+c\equiv 0(\mathrm{mod}\,m)$ в том случае, если $(y_0-b)\vdots 2a$.

Рассмотрим сравнение $x^2\equiv a(\mathrm{mod}\,p)$, где p – простое нечетное число. При $a\in[0]_p$ получаем сравнение $x^2\equiv 0(\mathrm{mod}\,p)$, которое имеет единственное решение $[0]_p$. Если a не делится на p, то $(a;p)=1$ и по теореме 1 Ферма $a^{p-1}\equiv 1(\mathrm{mod}\,p)$, отсюда $a^{p-1}-1=\left(a^{\frac{p-1}{2}}-1\right)\left(a^{\frac{p-1}{2}}+1\right)\equiv 0(\mathrm{mod}\,p)$. По определению сравнения имеем, что $\left(a^{\frac{p-1}{2}}-1\right)\left(a^{\frac{p-1}{2}}+1\right)\vdots p$. Числа $a^{\frac{p-1}{2}}-1$ и $a^{\frac{p-1}{2}}+1$ не могут делиться на p одновременно, в противном случае их разность делилась бы на нечетное простое число p, но при вычитании этих чисел имеем $\left(a^{\frac{p-1}{2}}-1\right)-\left(a^{\frac{p-1}{2}}+1\right)=-2$.

Пусть сравнение $x^2 \equiv a(\mathrm{mod}\, p)$ имеет решение $[x_0]_p$, тогда класс вычетов $[-x_0]_p$ (или $[p-x_0]_p$) также является решением этого сравнения. Действительно, $(-x_0)^2 = x_0^2 \equiv a(\mathrm{mod}\, p)$.

Аналогично $(p-x_0)^2 = p(p-2x_0)+x_0^2 \equiv x_0^2 \equiv a(\mathrm{mod}\, p))$. Причем, если a не делится на p, то $[x_0]_p \neq [0]_p$. Т. к. $x_0-(-x_0)=2x_0$ не делится на нечетное простое число p, то $x_0 \not\equiv -x_0(\mathrm{mod}\, p)$, т. е. $[x_0]_p \neq [-x_0]_p$.

Т. к. класс вычетов $[0]_p$ не может быть решением сравнения $x^2 \equiv a(\mathrm{mod}\, p)$, то $(x_0; p)=1$ и по теореме 1 Ферма справедливо сравнение $x_0^{p-1} \equiv 1(\mathrm{mod}\, p)$. Обе части сравнения $x_0^2 \equiv a(\mathrm{mod}\, p)$ возведем в степень $\frac{p-1}{2}$, получим сравнение $x_0^{p-1} \equiv a^{\frac{p-1}{2}}(\mathrm{mod}\, p)$, следовательно, если сравнение $x^2 \equiv a(\mathrm{mod}\, p)$ имеет решение, то $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p)$.

Рассмотрим квадраты чисел приведенной системы вычетов $\{1;2;3;...;p-1\}_p$, заметим, что $\alpha^2 \equiv (p-\alpha)^2(\mathrm{mod}\, p)$, следовательно, среди квадратов этих вычетов имеется ровно $\frac{p-1}{2}$ чисел, попарно несравнимых по модулю p, обозначим эти числа $a_1, a_2, ..., a_{\frac{p-1}{2}}$. Для каждого из чисел $a_i \in \left\{a_1, a_2, ..., a_{\frac{p-1}{2}}\right\}$ сравнение $x^2 \equiv a_i(\mathrm{mod}\, p)$ имеет решение. Следовательно, чисел a, удовлетворяющих условию $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p)$, ровно $\frac{p-1}{2}$.

ОПРЕДЕЛЕНИЕ. Число a называется квадратичным вычетом числа p, если имеет решение сравнение $x^2 \equiv a(\mathrm{mod}\, p)$.

Из определения следует, что для нечетного простого числа p существует $\frac{p-1}{2}$ квадратичных вычетов.

Если число a удовлетворяет условию $a^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\, p)$, то оно не является квадратичным вычетом числа p, назовем его *невычетом* числа p.

Теорема 19. *Произведение двух квадратичных вычетов числа p или двух невычетов числа p есть квадратичный вычет числа p. Произведение квадратичного вычета и невычета числа p есть невычет числа p.*

Доказательство. Если $(a; p) = 1$ и $(b; p) = 1$, то $a^{\frac{p-1}{2}} \equiv \pm 1 (\mathrm{mod}\, p)$ и $b^{\frac{p-1}{2}} \equiv \pm 1 (\mathrm{mod}\, p)$. Тогда $(ab)^{\frac{p-1}{2}} \equiv \pm 1 (\mathrm{mod}\, p)$. Здесь $+1 = (+1)\cdot(+1) = (-1)\cdot(-1)$ и $-1 = (-1)\cdot(+1) = (+1)\cdot(-1)$.■

Для решения квадратичного двучленного сравнения $x^2 \equiv a (\mathrm{mod}\, p)$ не существует практического способа, если не считать способ применения особых таблиц. Можно выделить частные случаи решения сравнений с определенными модулями $p = 4k + 3$ и $p = 8k + 5$.

Пусть $p = 4k + 3$, тогда $\frac{p-1}{2} = 2k + 1$. Если сравнение $x^2 \equiv a (\mathrm{mod}\, p)$ имеет решение, то $a^{2k+1} \equiv 1 (\mathrm{mod}\, p)$. После умножения обеих частей сравнения на a получим $a^{2k+2} \equiv a (\mathrm{mod}\, p)$ или $\left(a^{k+1}\right)^2 \equiv a (\mathrm{mod}\, p)$, следовательно, $x \equiv \pm a^{k+1} (\mathrm{mod}\, p)$ – искомое решение сравнения.

Пусть $p = 8k + 5$, тогда $\frac{p-1}{2} = 4k + 2$ и $a^{4k+2} \equiv 1 (\mathrm{mod}\, p)$, или $\left(a^{2k+1} - 1\right)\left(a^{2k+1} + 1\right) \equiv 0 (\mathrm{mod}\, p)$. Из последнего сравнения получаем, что только один из множителей делится на p:

1) $a^{2k+1} \equiv 1 (\mathrm{mod}\, p)$, тогда $a^{2k+2} \equiv a (\mathrm{mod}\, p)$ и $x \equiv \pm a^{k+1} (\mathrm{mod}\, p)$ – решение сравнения;

2) $a^{2k+1} \equiv -1 (\mathrm{mod}\, p)$, тогда $a^{2k+2} \equiv -a (\mathrm{mod}\, p)$. Число 2 является квадратичным невычетом[8] модуля $p = 8k + 5$, поэтому $2^{\frac{p-1}{2}} \equiv 2^{4k+2} \equiv -1 (\mathrm{mod}\, p)$. Перемножим почленно два последних сравнения, получим $\left(2^{2k+1} \cdot a^{k+1}\right)^2 \equiv a (\mathrm{mod}\, p)$. Следовательно, решением исходного сравнения являются классы вычетов $\left[2^{2k+1} \cdot a^{k+1}\right]_{8k+5}$ и $\left[-2^{2k+1} \cdot a^{k+1}\right]_{8k+5}$.

[8] Доказательство см. : Сушкевич, А. К. Теория чисел. Элементарный курс / А. К. Сушкевич. – М. : Вузовская книга, 2007. – 240 с. (п. 48, V).

Примеры.

1. Решить сравнение $x^2 \equiv 5(\mathrm{mod}\,7)$. Модуль сравнения $p=7$ можно записать как $p=4\cdot 1+3$ $(k=1)$, т. е. решениями сравнения, если они существуют, должны быть классы вычетов $\left[-5^{1+1}\right]_7=[-4]_7$ и $\left[5^{1+1}\right]_7=[4]_7$.

Проверка. Т. к. числовые сравнения $(-4)^2 \equiv 5(\mathrm{mod}\,7)$ и $4^2 \equiv 5(\mathrm{mod}\,7)$ ложны, то исходное сравнение решений не имеет.

2. Решить сравнение $x^2 \equiv -5(\mathrm{mod}\,7)$. Здесь решениями сравнения, если они существуют, должны быть классы вычетов $\left[-(-5)^{1+1}\right]_7=[-4]_7$ и $\left[(-5)^{1+1}\right]_7=[4]_7$.

Проверка. Т. к. числовые сравнения $(-4)^2 \equiv -5(\mathrm{mod}\,7)$ и $4^2 \equiv -5(\mathrm{mod}\,7)$ истинны, следовательно, классы $[-4]_7$ и $[4]_7$ являются решениями.

3. Решить сравнения $x^2 \equiv \pm 5(\mathrm{mod}13)$. Модуль сравнения $p=13$ можно записать как $p=8\cdot 1+5$, где $k=1$, т. е. решениями сравнений, если они существуют, должны быть соответствующие классы вычетов $\left[2^3\cdot(\pm 5)^2\right]_{13}$ и $\left[-2^3\cdot(\pm 5)^2\right]_{13}$.

Проверка. Если $x=\pm 2^3\cdot(\pm 5)^2=\pm 200$, то сравнения $(\pm 200)^2 \equiv \pm 5(\mathrm{mod}13)$ являются ложными. Вывод: исходное сравнение решений не имеет.

9. ПОРЯДОК КЛАССА ПО МОДУЛЮ

ОПРЕДЕЛЕНИЕ. Порядком вычета a по модулю m, где $(a;m)=1$, называют наименьшую натуральную степень $P(a)_m$, что $a^{P(a)_m} \equiv 1(\mathrm{mod}\,m)$.

Из определения следует, что если $0<\delta<P(a)_m$, то $a^{\delta} \not\equiv 1(\mathrm{mod}\,m)$.

Примеры.

1) $a=4, m=5$, $4^1 \equiv 4(\mathrm{mod}5), 4^2 \equiv 1(\mathrm{mod}5)$, следовательно, $P(4)_5=2$;

2) $a=3, m=5$, $2^1 \equiv 2(\mathrm{mod}5), 2^2 \equiv 4(\mathrm{mod}5), 2^3 \equiv 3(\mathrm{mod}5), 2^4 \equiv 1(\mathrm{mod}5)$, т. е. $P(2)_5=4$.

Теорема 20. *Если* $b \equiv a(\mathrm{mod}\,m)$, *то* $P(b)_m = P(a)_m$.

Доказательство. Пусть вычет a по модулю m имеет порядок $P(a)_m$. Обе части сравнения $b \equiv a(\mathrm{mod}\,m)$ возведем в натуральную степень $P(a)_m$, получим

сравнение $b^{P(a)_m} \equiv a^{P(a)_m} (\mathrm{mod}\, m)$, тогда $b^{P(a)_m} \equiv 1 (\mathrm{mod}\, m)$. Если же существует такое натуральное $k < P(a)_m$, что $b^k \equiv 1 (\mathrm{mod}\, m)$, то $a^k \equiv 1 (\mathrm{mod}\, m)$, чего быть не может в силу определения порядка вычета. ■

Замечание. Все числа одного класса вычетов по модулю m имеют один и тот же порядок.

Теорема 21. *Если* $a^n \equiv 1 (\mathrm{mod}\, m)$, *то* $n \vdots P(a)_m$.

Доказательство. Из определения порядка вычета показатель n не может быть меньше $P(a)_m$, следовательно, $n \geq P(a)_m$. Разделим n на $P(a)_m$ с остатком: $n = P(a)_m \cdot q + r$, где $0 \leq r < P(a)_m$. Получаем сравнение $a^n \equiv \left(a^{P(a)_m}\right)^q \cdot a^r \equiv a^r \equiv 1 (\mathrm{mod}\, m)$. Тогда, в силу определения порядка, имеем $r = 0$, т. е. $n = P(a)_m \cdot q$ и $n \vdots P(a)_m$.■

Следствие. $\varphi(m) \vdots P(a)_m$, отсюда имеем: чтобы определить порядок вычета a по модулю m, достаточно рассмотреть натуральные делители $\varphi(m)$.

Теорема 22. *Сравнение* $a^s \equiv a^t (\mathrm{mod}\, m)$ *при* $(a;m) = 1$ *имеет место тогда и только тогда, когда* $s \equiv t (\mathrm{mod}\, P(a)_m)$.

Доказательство.

$\underline{\Rightarrow|}$ Пусть в сравнении $a^s \equiv a^t (\mathrm{mod}\, m)$ выполняется соотношение для показателей $t < s$. Т. к. $(a;m) = 1$, то $(a^t;m) = 1$, поэтому верно сравнение $a^{s-t} \equiv 1 (\mathrm{mod}\, m)$, откуда имеем $(s-t) \vdots P(a)_m$ или $s \equiv t (\mathrm{mod}\, P(a)_m)$.

$\underline{\Leftarrow|}$ Пусть $s \equiv t (\mathrm{mod}\, P(a)_m)$ и $s \geq t$, тогда $s - t = P(a)_m \cdot q, q \in N$, $s = P(a)_m \cdot q + t$, следовательно, $a^s \equiv \left(a^{P(a)_m}\right)^q \cdot a^t \equiv a^t (\mathrm{mod}\, m)$. ■

Теорема 23. *В числовой последовательности* $a, a^2, a^3, \ldots$ *все числа принадлежат* $P(a)_m$ *классам, представителями которых являются числа* $a, a^2, \ldots, a^{P(a)_m}$.

Доказательство. Числа $a, a^2, \ldots, a^{P(a)_m}$ попарно не сравнимы между собой по модулю m, т. к. если бы для каких-либо двух степеней a^i и a^j (где $i \neq j$ и $0 < j < i \leq P(a)_m$) было верно сравнение $a^i \equiv a^j (\mathrm{mod}\, m)$, то получили бы сравнение $i \equiv j (\mathrm{mod}\, P(a)_m)$, откуда $(i-j) \vdots P(a)_m$, т. е. $i - j = 0$ и $i = j$.

С другой стороны, если бы попарно несравнимых чисел $a, a^2, ..., a^k$ было больше, чем $P(a)_m$, то существовало бы такое число $h > P(a)_m$, что для некоторого $0 < l < P(a)_m$ выполнялось бы условие $h - l = P(a)_m$. Тогда из того, что $h \equiv l (\mathrm{mod}\, P(a)_m)$, следует сравнение $a^h \equiv a^l (\mathrm{mod}\, m)$. ■

Теорема 24. *Числа a^k и a имеют один порядок по модулю m тогда и только тогда, когда $(k; P(a)_m) = 1$.*

Доказательство.

$\Rightarrow$ Пусть $P(a^k)_m = P(a)_m$, т. е. $(a^k)^{P(a)_m} \equiv a^{P(a)_m} \equiv 1 (\mathrm{mod}\, m)$. Если $(k; P(a)_m) = d > 1$, то $\frac{k}{d}$ и $\frac{P(a)_m}{d}$ являются натуральными числами, причем $\frac{P(a)_m}{d} < P(a)_m$. Из равенства $(a^k)^{\frac{P(a)_m}{d}} = (a^{P(a)_m})^{\frac{k}{d}}$ получаем сравнение $(a^{P(a)_m})^{\frac{k}{d}} \equiv 1^{\frac{k}{d}} \equiv 1 (\mathrm{mod}\, m)$, т. е. $(a^k)^{\frac{P(a)_m}{d}} \equiv 1 (\mathrm{mod}\, m)$, что означает $P(a^k)_m = \frac{P(a)_m}{d} < P(a)_m$, что противоречит условию.

$\Leftarrow$ По условию $(k; P(a)_m) = 1$ и пусть t – наименьшее натуральное число такое, что $(a^k)^t \equiv 1 (\mathrm{mod}\, m)$, т. е. $P(a^k)_m = t$. Имеем сравнение $a^{k \cdot t} \equiv 1 (\mathrm{mod}\, m)$, тогда $(k \cdot t) \vdots P(a)_m$. Но т. к. $(k; P(a)_m) = 1$, то $t \vdots P(a)_m$, а в силу выбора числа t имеем, что $t = P(a)_m$, т. е. $P(a^k)_m = P(a)_m$. ■

Замечание. Среди степеней $a, a^2, a^3, ...$ все степени a^k, у которых показатели взаимно просты с порядком $P(a)_m$, имеют тот же порядок по модулю m, что и само число a.

ОПРЕДЕЛЕНИЕ. Порядком класса вычетов по модулю m называется порядок любого представителя этого класса. $P([a]_m)_m = P(a)_m$.

Пусть по модулю m несколько классов вычетов имеют порядок k, количество таких классов обозначим $\psi(k)$. Т. к. порядок по модулю m определить можно только для вычета, взаимно простого с модулем, то представители классов, имеющих порядок, образуют приведенную систему вычетов, следовательно, классов, имеющих по модулю m порядок,

существует ровно $\varphi(m)$. Пусть эти классы имеют порядки $k_1, k_2, ..., k_t$, причем $\varphi(m) \vdots k_i$. Из изложенного следует, что $\psi(k_1)+\psi(k_2)+...+\psi(k_t)=\varphi(m)$.

Примеры.

1. Рассмотрим модуль $m=11$. Порядки k вычетов по модулю $m=11$ являются делителями $\varphi(11)=10$, т. е. $k=P(a)_{11} \in \{1;2;5;10\}$. Определим порядки вычетов приведенной системы вычетов $\{1;2;3;4;5;6;7;8;9;10\}_{11}$ и запишем в таблицу:

a	1	2	3	4	5	6	7	8	9	10
$P(a)_{11}$	1	10	5	5	5	10	10	10	5	2

Из таблицы видно, что $\psi(1)=1$, $\psi(2)=1$, $\psi(5)=4$, $\psi(10)=4$ и $\psi(1)+\psi(2)+\psi(5)+\psi(10)=10=\varphi(11)$.

2. Пусть $m=20$, $\varphi(20)=\varphi(2^2\cdot 5)=\varphi(2^2)\cdot\varphi(5)=2\cdot 4=8$ и $k=P(a)_{20} \in \{1;2;4;8\}$. Запишем приведенную систему вычетов $\{1;3;7;9;11;13;17;19\}_{20}$.

a	1	3	7	9	11	13	17	19
$P(a)_{20}$	1	4	4	2	2	4	4	2

$\psi(1)=1$, $\psi(2)=3$, $\psi(4)=4$, $\psi(8)=0$ и $\psi(1)+\psi(2)+\psi(4)+\psi(8)=8=\varphi(20)$.

Упражнения для самостоятельного решения

1. Определить порядки вычетов по модулю $m=17$.
2. Заполнить таблицу:

a	5	7	11	13
$P(a)_{24}$				

3. Указать наименьший неотрицательный вычет по модулю $m=47$, имеющий порядок $P(a)_{47}=46$.

10. ПЕРВООБРАЗНЫЕ ВЫЧЕТЫ

Рассмотрим натуральные степени вычета a = 3 по простому модулю 7.

$3^1 \equiv 3(\mathrm{mod}\,7)$, $3^2 \equiv 2(\mathrm{mod}\,7)$, $3^3 \equiv 6(\mathrm{mod}\,7)$, $3^4 \equiv 4(\mathrm{mod}\,7)$,
$3^5 \equiv 5(\mathrm{mod}\,7)$, $3^6 \equiv 1(\mathrm{mod}\,7)$, $3^7 \equiv 0(\mathrm{mod}\,7)$.

Замечаем, что степени a^k, где $k \in \{1;2;3;4;5;6;7\}$, вычета a = 3 по модулю 7 образуют полную систему вычетов по модулю 7. Кроме этого, $3^6 \equiv 1(\mathrm{mod}\,7)$, где $6 = P(3)_7 = \varphi(7)$.

ОПРЕДЕЛЕНИЕ. Вычет a по модулю m называется первообразным вычетом, если $P(a)_m = \varphi(m)$.

Из определения можно сделать вывод: для того чтобы определить, является ли вычет a первообразным по модулю m, достаточно проверить выполнение условия $a^k \not\equiv 1(\mathrm{mod}\,m)$, где $0 < k < \varphi(m)$ и $\varphi(m) \vdots k$.

В рассмотренном выше примере вычет a=3 является первообразным по модулю 7.

Теорема 25. *Если a – первообразный вычет по модулю m, то числа $a, a^2, ..., a^{\varphi(m)}$ образуют приведенную систему вычетов по модулю m.*

Доказательство. Т. к. a – первообразный вычет по модулю m, то порядок вычета a равен $P(a)_m = \varphi(m)$, тогда по теореме 23 все числа $a, a^2, ..., a^{\varphi(m)}$ попарно несравнимы по модулю m. Т. к. $(a;m)=1$, то $(a^k;m)=1$ для любого натурального k, всего этих чисел $\varphi(m)$, и следовательно, они образуют приведенную систему вычетов по модулю m. ■

Следствие. Если $m = p$ – простое число, то из того, что a – первообразный вычет по модулю p, следует, что числа $a, a^2, ..., a^{p-1}$ образуют приведенную систему вычетов по модулю p.

Пример.

Для $p = 11$ вычет $a = 2$ – первообразный, т. к. $P(2)_{11} = 10 = \varphi(11)$. Тогда имеем приведенную систему вычетов по модулю 11:

$\{2^1;2^2;2^3;2^4;2^5;2^6;2^7;2^8;2^9;2^{10}\}_{11}$. Найдем наименьшие неотрицательные вычеты, сравнимые с вычетами данной приведенной системы по модулю 11.

$2^1 \equiv 2(\text{mod}11)$, $2^2 \equiv 4(\text{mod}11)$, $2^3 \equiv 8(\text{mod}11)$, $2^4 \equiv 5(\text{mod}11)$, $2^5 \equiv 10(\text{mod}11)$, $2^6 \equiv 9(\text{mod}11)$, $2^7 \equiv 7(\text{mod}11)$, $2^8 \equiv 3(\text{mod}11)$, $2^9 \equiv 6(\text{mod}11)$, $2^{10} \equiv 1(\text{mod}11)$.

После замены вычетов получим приведенную систему вычетов: $\{1;2;3;4;5;6;7;8;9;10\}_{11}$.

Теорема 26. *Если целое число a является первообразным вычетом по модулю m, то* a^t *также первообразный вычет тогда и только тогда, когда* $НОД(t,\varphi(m))=1$.

Доказательство.

$\underline{\Rightarrow|}$ Пусть a – первообразный вычет по модулю m и $НОД(t,\varphi(m))=1$. Докажем, что в этом случае a^t – также первообразный вычет по модулю m.

По определению первообразного вычета $P(a)_m = \varphi(m)$ и $a^{\varphi(m)} \equiv 1(\text{mod}\, m)$. Пусть вычет a^t имеет порядок k по модулю m, т. е. справедливо сравнение $(a^t)^k \equiv 1(\text{mod}\, m)$, причем k – наименьшее натуральное число с таким условием. Тогда из сравнения $a^{t\cdot k} \equiv 1(\text{mod}\, m)$ и определения порядка вычета число $t\cdot k$ делится на $\varphi(m)$ порядок вычета a, следовательно, имеем равенство $t\cdot k = \varphi(m)\cdot l,\ l \in Z$, а в силу взаимной простоты чисел t и $\varphi(m)$ получаем, что на $\varphi(m)$ делится множитель k. Ясно, что наименьшим натуральным числом, делящимся на $\varphi(m)$, является само число $\varphi(m)$. Этим показали, что $P(a^t)_m = \varphi(m)$, следовательно, вычет a^t является первообразным по модулю m.

$\underline{\Leftarrow|}$ Имеем условие: $P(a^t)_m = \varphi(m) = P(a)_m$, необходимо показать, что в этом случае числа t и $\varphi(m)$ – взаимно простые. Пусть $(t;\varphi(m)) = d > 1$, тогда $t = d\cdot t_1$ и $\varphi(m) = d\cdot l$, причем $(t_1;l)=1$ и $t_1 < t,\ l < \varphi(m)$. Обе части сравнения $a^{\varphi(m)} \equiv 1(\text{mod}\, m)$ возведем в степень t_1, получим $(a^{\varphi(m)})^{t_1} \equiv 1(\text{mod}\, m)$ или $(a^{d\cdot l})^{t_1} \equiv (a^{d\cdot t_1})^l \equiv (a^t)^l \equiv 1(\text{mod}\, m)$, откуда получаем, что порядок вычета a^t равен

$P(a^t)_m = l$, чего быть не может по условию. Получили, что наше предположение $(t;\varphi(m)) \neq 1$ оказалось неверным. ■

Рассмотрим простое число p, тогда $\varphi(p) = p-1$ и $\varphi(p) = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_s^{\alpha_s}$ – каноническое представление числа $p-1$. Целое число a, не делящееся на p, будет являться первообразным вычетом по модулю p в том случае, если для любой натуральной степени k, меньшей $\varphi(p)$, верно условие $a^k \not\equiv 1(\mathrm{mod}\, p)$. А т. к. k необходимо искать среди делителей числа $\varphi(p) = p-1$, то можно сделать вывод: число a будет являться первообразным вычетом по модулю p тогда и только тогда, когда

$a^{\frac{p-1}{p_1}} \not\equiv 1(\mathrm{mod}\, p)$, …, $a^{\frac{p-1}{p_s}} \not\equiv 1(\mathrm{mod}\, p)$.

Пример.

Пусть модуль $p = 7$, тогда $p-1 = 6 = 2 \cdot 3$. Т. к. для вычета $a = 3$ выполняются условия $3^{\frac{6}{2}} = 3^3 = 27 \not\equiv 1(\mathrm{mod}\, 7)$ и $3^{\frac{6}{3}} = 3^2 = 9 \not\equiv 1(\mathrm{mod}\, 7)$, имеем, что $a = 3$ – первообразный вычет по модулю $p = 7$.

11. ИНДЕКСЫ

Рассмотрим степени $a, a^2, ..., a^{p-1}$ первообразного вычета a по простому модулю p. Эти степени попарно несравнимы по модулю p, следовательно, образуют приведенную систему вычетов. Любое целое число x, взаимно простое с p, входит в один из классов вычетов $[a^i]_p$, т. е. для числа x найдется такой показатель i, что будет справедливо сравнение $a^i \equiv x(\mathrm{mod}\ p)$.

ОПРЕДЕЛЕНИЕ. Число γ называется индексом класса вычетов $[x]_p$ при основании a, если $a^\gamma \equiv x(\mathrm{mod}\ p)$ или $[a^\gamma]_p = [x]_p$.

Индексы обозначают следующим образом:

$\gamma = ind_a x$ – индекс числа (класса) x при фиксированном модуле p;

$\gamma = ind\, x$ – индекс числа (класса) x при фиксированных модуле p и основании a.

Тогда, если γ – индекс числа x по модулю p, то справедливо сравнение $a^{ind_a x} \equiv x(\mathrm{mod}\, p)$.

Примеры.

1. Пусть модуль $p=13$, $a=2$ – первообразный вычет; т. к. $2^6 \equiv 12(\mathrm{mod}13)$, то $ind_2 12 = 6$. Если некоторое целое число b является вычетом класса $[12]_{13}$, то $ind_2 b = 6$. $2^{13} \equiv 2(\mathrm{mod}13) \Rightarrow ind_2 2 = 13$, но $2^{13} \equiv 2^1 \equiv 2(\mathrm{mod}13) \Rightarrow ind_2 2 = 1$. Данный пример показывает, что индекс числа находится неоднозначно.

2. Пусть модуль $m=21$, $a=5$, т. к. $5^6 \equiv 1(\mathrm{mod}\,21)$ и $6 \neq \varphi(21)$, то $a=5$ первообразным вычетом не является, и не для всех целых чисел, взаимно простых с модулем, можно определить индекс по основанию 5 и модулю 21. Например, нельзя найти индекс $ind_5 2$.

Теорема 27. *Если a – первообразный вычет по модулю m и $(b;m)=1$, то сравнение $c \equiv b(\mathrm{mod}\, m)$ имеет место тогда и только тогда, когда имеет место сравнение $ind_a c \equiv ind_a b(\mathrm{mod}\,\varphi(m))$.*

Доказательство.

$\underline{\Rightarrow|}$ Из определения индекса имеем $a^{ind_a b} \equiv b(\mathrm{mod}\, m)$, т. к. $(b;m)=1$ и $c \equiv b(\mathrm{mod}\, m)$, то существует $ind_a c$ и справедливо сравнение $a^{ind_a c} \equiv c(\mathrm{mod}\, m)$. Следовательно, имеем сравнение $a^{ind_a c} \equiv a^{ind_a b}(\mathrm{mod}\, m)$. Т. к. a – первообразный вычет по модулю m, то $P(a)_m = \varphi(m)$ и по теореме 22 $ind_a c \equiv ind_a b(\mathrm{mod}\,\varphi(m))$.

$\underline{\Leftarrow|}$ Пусть для целых чисел b и c, взаимно простых с модулем m, выполняется сравнение $ind_a c \equiv ind_a b(\mathrm{mod}\,\varphi(m))$, т. е. $ind_a c - ind_a b = \varphi(m)\cdot k$, $k \in Z$, откуда $ind_a c = ind_a b + \varphi(m)\cdot k$. Из определения индекса имеем $c \equiv a^{ind_a c} \equiv a^{in_a b+\varphi(m)} \equiv a^{ind_a} \cdot a^{\varphi(m)} \equiv a^{ind_a b} \equiv b(\mathrm{mod}\, m)$.■

ОПРЕДЕЛЕНИЕ. Переход от сравнения $c \equiv b(\mathrm{mod}\, m)$ к сравнению $ind_a c \equiv ind_a b(\mathrm{mod}\,\varphi(m))$ называют индексированием, обратный переход – потенцированием.

СВОЙСТВО 19. Если a – первообразный вычет по модулю m, $(b;m)=1$ и $(c;m)=1$, то $ind_a(b\cdot c)\equiv ind_a b+ind_a c(\mathrm{mod}\,\varphi(m))$.

Доказательство. $a^{ind_a(b\cdot c)}\equiv b\cdot c\equiv a^{ind_a b}\cdot a^{ind_a c}\equiv a^{ind_a b+ind_a c}(\mathrm{mod}\,m)$, следовательно, $ind_a(b\cdot c)\equiv ind_a b+ind_a c(\mathrm{mod}\,\varphi(m))$.

СЛЕДСТВИЕ. Если a – первообразный вычет по модулю m, $(b;m)=1$ и $n\in N$, то $ind_a b^n\equiv n\cdot ind_a b(\mathrm{mod}\,\varphi(m))$.

СВОЙСТВО 20. Если a – первообразный вычет по модулю m, $(b;m)=1$, $(c;m)=1$ и $b\vdots c$, то $ind_a\left(\frac{b}{c}\right)\equiv ind_a b-ind_a c(\mathrm{mod}\,\varphi(m))$.

Доказательство. Т. к. $b\vdots c$, то существует такое целое число k, что верно равенство $b=c\cdot k$. Тогда $ind_a b\equiv ind_a k+ind_a c(\mathrm{mod}\,\varphi(m))$, откуда имеем сравнение $ind_a k\equiv ind_a b-ind_a c(\mathrm{mod}\,\varphi(m))$ или $ind_a\left(\frac{b}{c}\right)\equiv ind_a b-ind_a c(\mathrm{mod}\,\varphi(m))$.

Т. к. по простому модулю p всегда существуют первообразные вычеты, то, взяв за основание один из них, получим систему (таблицу) индексов, в которой каждое число x, взаимно простое с модулем p, будет иметь свой индекс. Причем любое положительное число из класса вычетов $[ind_a x]_{\varphi(m)}$ будет являться индексом числа x. Обычно из всех возможных значений индекса выбирают наименьшее. Тогда получаем условие: если p – простой модуль, то $ind_a x\le p-1$.

Построим таблицу индексов по модулю $p=23$.

В качестве основания выберем наименьший первообразный вычет по модулю 23. Таким вычетом является $a=5$.

$5^1\equiv 5(\mathrm{mod}\,23)$; $5^2\equiv 25\equiv 2(\mathrm{mod}\,23)$; $5^3\equiv 125\equiv 10(\mathrm{mod}\,23)$; $5^4\equiv 4(\mathrm{mod}\,23)$; $5^5\equiv 20(\mathrm{mod}\,23)$; $5^6\equiv 8(\mathrm{mod}\,23)$; $5^7\equiv 17(\mathrm{mod}\,23)$; $5^8\equiv 16(\mathrm{mod}\,23)$; $5^9\equiv 11(\mathrm{mod}\,23)$; $5^{10}\equiv 9(\mathrm{mod}\,23)$; $5^{11}\equiv 22(\mathrm{mod}\,23)$; $5^{12}\equiv 18(\mathrm{mod}\,23)$; $5^{13}\equiv 21(\mathrm{mod}\,23)$; $5^{14}\equiv 13(\mathrm{mod}\,23)$; $5^{15}\equiv 19(\mathrm{mod}\,23)$; $5^{16}\equiv 3(\mathrm{mod}\,23)$; $5^{17}\equiv 15(\mathrm{mod}\,23)$; $5^{18}\equiv 6(\mathrm{mod}\,23)$; $5^{19}\equiv 7(\mathrm{mod}\,23)$; $5^{20}\equiv 12(\mathrm{mod}\,23)$; $5^{21}\equiv 14(\mathrm{mod}\,23)$; $5^{22}\equiv 1(\mathrm{mod}\,23)$.

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
$ind_5 x$	22	2	16	4	1	18	19	6	10	3	9	20	14	21	17	8	7	12	15	5	13	11

Примеры.

1. Используя данную таблицу индексов, найдем индексы чисел: 124; –34 по модулю 23.

Т. к. $124 \equiv 9 (\mathrm{mod}\, 23)$, то $ind_5 124 = ind_5 9 = 10$; аналогично $(-34) \equiv 12 (\mathrm{mod}\, 23) \Rightarrow ind_5 (-34) = ind_5 12 = 20$.

2. Найти все целые числа, индексы которых по модулю 23 равны 7. Известно, что $ind_5 x = 7$. По таблице находим, что $x \equiv 17 (\mathrm{mod}\, 23)$, следовательно, $x \in [17]_{23}$.

3. Решить сравнение $8x \equiv -11 (\mathrm{mod}\, 23)$.

После замены вычета (-11) на наименьший неотрицательный вычет по модулю $p = 23$ получим сравнение $8x \equiv 12 (\mathrm{mod}\, 23)$. Проиндексируем полученное сравнение: $ind 8 + ind x \equiv ind 12 (\mathrm{mod}\, \varphi(23))$, по таблице находим соответствующие значения индексов, имеем сравнение $6 + ind x \equiv 20 (\mathrm{mod}\, 22)$, откуда $ind x \equiv 14 (\mathrm{mod}\, 22)$. По таблице индексов получаем $x \equiv 13 (\mathrm{mod}\, 23)$.

Ответ: $x \in [13]_{23}$.

4. Решить сравнение $15x^4 \equiv 17 (\mathrm{mod}\, 23)$.

Индексируем сравнение: $ind 15 + 4 ind x \equiv ind 17 (\mathrm{mod}\, \varphi(23)) \rightarrow 17 + 4 ind x \equiv 7 (\mathrm{mod}\, 22) \rightarrow 4 ind x \equiv 7 - 17 \equiv -10 (\mathrm{mod}\, 22)$. Т. к. $(4;22) = 2$ и $(-10) \vdots 2$, то последнее сравнение, следовательно, и исходное имеют 2 решения. После деления всех составляющих сравнения на 2 получим $2 ind x \equiv -5 \equiv 6 (\mathrm{mod} 11)$, откуда $ind x \equiv 3 (\mathrm{mod} 11)$. Имеем решения: $ind x \equiv 3 (\mathrm{mod}\, 22)$ и $ind x \equiv 14 (\mathrm{mod}\, 22)$. По таблице индексов получаем $x \equiv 10 (\mathrm{mod}\, 23)$ и $x \equiv 13 (\mathrm{mod}\, 23)$.

Ответ: $[10]_{23}; [13]_{23}$.

5. Решить сравнение $15 \cdot 7^{2x} \equiv 8 \cdot 3^{3x} (\mathrm{mod}\, 23)$.

Индексируем сравнение: $ind15+2x\cdot ind7\equiv ind8+3x\cdot ind3(\mathrm{mod}\,\varphi(23))$ → $17+2x\cdot 19\equiv 6+3x\cdot 16(\mathrm{mod}\,22)$ → $38x-48x\equiv 6-17(\mathrm{mod}\,22)$ → $-10x\equiv -11(\mathrm{mod}\,22)$ → $10x\equiv 11(\mathrm{mod}\,22)$. Т. к. $(10;22)=2$ и 11 не делится на 2, то сравнение решений не имеет.

6. Решить сравнение $5^{6x}\equiv 13(\mathrm{mod}\,23)$.

Индексируем сравнение: $6x\cdot ind5\equiv ind13(\mathrm{mod}\,\varphi(23))$ → $6x\cdot 1\equiv 14(\mathrm{mod}\,\varphi(23))$ → $6x\equiv 14(\mathrm{mod}\,22)$. Т. к. $(6;22)=2$ и $14\vdots 2$, то сравнение имеет 2 решения.

$3x\equiv 7(\mathrm{mod}11)$ → $3x\equiv 7\equiv 18(\mathrm{mod}11)$ → $x\equiv 6(\mathrm{mod}11)$. Запишем решения исходного сравнения: $x\equiv 6(\mathrm{mod}\,22)$ и $x\equiv 17(\mathrm{mod}\,22)$.

Ответ: $[6]_{22};[17]_{22}$.

Таблицы индексов по различным простым модулям приведены в приложении.

Упражнения для самостоятельного решения

1. Вычислить, используя таблицу индексов:
   1) $ind_{29}174$; 2) $ind_{41}(-13)$; 3) $ind_{67}25$;
   4) $ind_{53}(-1)$; 5) $ind_{47}74$; 6) $ind_{7}11142$.
2. Решить уравнения: 1) $ind_{29}x=5$; 2) $ind_{31}x=7$; 3) $ind_{19}x=11$.
3. Решить сравнения: 1) $24x^{12}\equiv -17(\mathrm{mod}\,71)$; 2) $3x^{9}\equiv 25(\mathrm{mod}\,43)$;
   3) $-17x^{3}\equiv 43(\mathrm{mod}19)$; 4) $5x^{61}\equiv 14(\mathrm{mod}\,59)$.
4. Решить сравнения: 1) $4^{2x}\equiv 15(\mathrm{mod}19)$; 2) $11^{3x}\equiv 62(\mathrm{mod}\,41)$;
   3) $25^{x}\equiv -23(\mathrm{mod}17)$; 4) $31^{x}\equiv 43(\mathrm{mod}\,67)$.

12. КОНЕЧНЫЕ СИСТЕМАТИЧЕСКИЕ ДРОБИ

Известно, что любое натуральное число n можно представить, и притом единственным образом, в виде систематической записи[9] по основанию $q>1$ $n=a_kq^k+a_{k-1}q^{k-1}+...+a_1q+a_0$, где $a_k\neq 0$ и $0\le a_i\le q-1$ для $i\in\{0;1;...;k\}$. Получим формулу для нахождения цифр $a_k,...,a_0$ в q-ичной записи числа n.

[9] Куликов, Л. Я. Алгебра и теория чисел : учеб. пособие для педагогических институтов / Л. Я. Куликов. – М. : Высшая школа, 1979. – 559 с. – Гл. 11. – § 4.

Разделим число n на q^s, при $0 \le s \le k$: $\frac{n}{q^s} = a_k q^{k-s} + ... + a_s + \frac{a_{s-1}}{q} + ... + \frac{a_0}{q^s}$.

Т. к. $a_{s-1}q^{s-1} + ... + a_0 < q^s$, то $\frac{a_{s-1}q^{s-1} + ... + a_0}{q^s} = \frac{a_{s-1}}{q} + ... + \frac{a_0}{q^{s-1}} < 1$. Получаем целую часть дроби $\left[\frac{n}{q^s}\right] = a_k q^{k-s} + ... + a_s$. Аналогично $\left[\frac{n}{q^{s+1}}\right] = a_k q^{k-s-1} + ... + a_{s+1}$. Тогда $a_s = \left[\frac{n}{q^s}\right] - q \cdot \left[\frac{n}{q^{s+1}}\right]$.

Рассмотрим представление любого рационального числа в систематической записи. Т. к. всегда можно выделить целую часть рационального числа, то будем рассматривать такие рациональные числа R, что $0 \le R < 1$, если $R = \frac{a}{b}$, то $0 \le a < b$.

Пусть $b = q^n$, где q – основание системы счисления. $R = \frac{a}{b} = \frac{a}{q^n}$, тогда $0 \le a < q^n$. Представим число a в виде систематической записи $a = c_k q^k + c_{k-1} q^{k-1} + ... + c_1 q + c_0$, $0 \le k < n$ и $0 \le c_i < q$.

$\frac{a}{q^n} = \frac{c_k}{q^{n-k}} + \frac{c_{k-1}}{q^{n-k+1}} + ... + \frac{c_0}{q^n}$, если $n - k > 1$, то можно добавить нулевые слагаемые $\frac{c_{n-1}}{q}, \frac{c_{n-2}}{q^2}, ..., \frac{c_{k+1}}{q^{n-k-1}}$, получим $\frac{a}{q^n} = \frac{c_{n-1}}{q} + ... + \frac{c_{k+1}}{q^{n-k-1}} + \frac{c_k}{q^{n-k}} + \frac{c_{k-1}}{q^{n-k+1}} + ... + \frac{c_0}{q^n}$. Если числители этих дробей обозначить $c_{n-i} = a_i \ (i = 1,...,n)$, то получим конечную систематическую дробь $\frac{a}{q^n} = \frac{a_1}{q} + \frac{a_2}{q^2} + ... + \frac{a_{n-k}}{q^k} + ... + \frac{a_n}{q^n}$, которую записывают короче $\frac{a}{q^n} = 0, a_1 a_2 ... a_{n_q}$, при $q = 10$ получают десятичную запись числа.

Пусть основание системы счисления q имеет каноническое разложение на простые множители $q = p_1^{\alpha_1} \cdot .... \cdot p_s^{\alpha_s}$. Рациональное число $\frac{a}{b}$, где $0 \le a < b$ и $(a;b) = 1$, можно представить в виде конечной систематической дроби $\frac{a}{b} = \frac{a_1}{q} + \frac{a_2}{q^2} + ... + \frac{a_n}{q^n}$, тогда $\frac{a}{b} = \frac{a_1 q^{n-1} + ... + a_n}{q^n} = \frac{c}{q^n}$. Из данного равенства имеем равенство $a \cdot q^n = b \cdot c$, которое в силу условия $(a;b) = 1$ показывает, что $q^n \vdots b$, а

это возможно лишь тогда, когда $b = p_1^{\beta_1} \cdot ... \cdot p_s^{\beta_s}$, причем возможно равенство нулю некоторых показателей β_i. Т. к. $q^n = p_1^{n \cdot \alpha_1} \cdot ... \cdot p_s^{n \cdot \alpha_s}$, то $\beta_i \le n \cdot \alpha_i \ (i = 1;...;s)$. Из вышеизложенного можно сделать вывод: несократимую рациональную дробь $\frac{a}{b}$ можно представить в виде конечной систематической q-ичной дроби только в том случае, если знаменатель b дроби раскладывается на те же множители, что и основание системы счисления. В частности, несократимая рациональная дробь $\frac{a}{b}$ может быть представлена в виде конечной десятичной дроби, если знаменатель этой дроби есть число вида $b = 2^{\alpha} \cdot 5^{\beta}$.

Примеры.

1. Рациональную дробь $\frac{7}{96}$ можно представить в виде конечной систематической дроби в 12-ичной системе счисления, т. к. $96 = 3 \cdot 2^5$ и $12 = 3 \cdot 2^2$.

$$\frac{7}{96} = \frac{7}{3 \cdot 2^5} = \frac{7}{3 \cdot 2^2 \cdot 2^3} = \frac{7 \cdot (3^2 \cdot 2)}{(3 \cdot 2^2) \cdot (3^2 \cdot 2) \cdot 2^3} = \frac{126}{12^3} = |126 = 12 \cdot 10 + 6 = (10)6_{12}| =$$

$$= \frac{12 \cdot 10 + 6}{12^3} = \frac{0}{12} + \frac{10}{12^2} + \frac{6}{12^3} = 0,0(10)6_{12}.$$

2. Рациональную дробь $\frac{9}{160}$ можно записать в виде конечной десятичной дроби, т. к. $160 = 2^5 \cdot 5$. Действительно, $\frac{9}{160} = 0,05625$.

3. Рациональную дробь $\frac{7}{96}$ нельзя представить в виде конечной десятичной дроби.

13. БЕСКОНЕЧНЫЕ СИСТЕМАТИЧЕСКИЕ ДРОБИ

Если в каноническом разложении числа b несократимой рациональной дроби $\frac{a}{b}$ имеются простые множители, которых нет в разложении q основа-

ния системы счисления, то число $\frac{a}{b}$ не может быть представлено в виде конечной q-ичной дроби.

ОПРЕДЕЛЕНИЕ. Правильной бесконечной q-ичной дробью называется ряд $\frac{a_1}{q}+...+\frac{a_n}{q^n}+...$, где $0 \le a_i < q \ \ (i=1,...,n)$. Т. к. $0 \le a_n < q$, то $\frac{a_n}{q^n} < \frac{1}{q^{n-1}}$. Ряд $\sum_{n=1}^{\infty}\frac{1}{q^{n-1}}$ является геометрической прогрессией со знаменателем $\frac{1}{q}<1$, поэтому сходится, следовательно, сходится и ряд $\sum_{n=1}^{\infty}\frac{a_n}{q^n}$, т. е. существует такое число a, что $a=\frac{a_1}{q}+...+\frac{a_n}{q^n}+...$. Тогда число a в q-ичной системе счисления имеет вид $a=0,a_1...a_n...$. Любое число x можно записать в виде $x=\pm\left(N+\frac{a}{b}\right)=\pm(N+0,a_1...a_n...)=\pm N,a_1...a_n...$, т. е. любое число x можно представить в виде суммы целого числа N и правильной несократимой дроби или в виде конечной или бесконечной систематической дроби.

Запишем следующий алгоритм деления на знаменатель b:

$qa=b\cdot a_1+r_1,\ 0\le r_1<b,$

$qr_1=b\cdot a_2+r_2,\ 0\le r_2<b,$

. . . . . .

$qr_{n-1}=b\cdot a_n+r_n,\ 0\le r_n<b,$

$qr_n=b\cdot a_{n+1}$, т. е. r_n – последний ненулевой остаток.

Из данного алгоритма получаем равенства:

$\frac{a}{b}=\frac{a_1}{q}+\frac{r_1}{b\cdot q},$

$\frac{r_1}{b}=\frac{a_2}{q}+\frac{r_2}{b\cdot q},$

. . . . . .

$\frac{r_{n-1}}{b}=\frac{a_{n+1}}{q}+\frac{r_n}{b\cdot q}.$

Имеем $\frac{a}{b}=\frac{a_1}{q}+\frac{r_1}{b\cdot q}=\frac{a_1}{q}+\frac{a_2}{q^2}+\frac{r_2}{b\cdot q^2}=...=\frac{a_1}{q}+\frac{a_2}{q^2}+...+\frac{a_n}{q^n}+\frac{r_n}{b\cdot q^n}$. Т. к. $0\le r_n<b$, то $0\le\frac{r_n}{b\cdot q^n}<\frac{1}{q^n}$, значит, $\lim\limits_{n\to\infty}\frac{r_n}{b\cdot q^n}=0$, поэтому $\lim\limits_{n\to\infty}\left(\frac{a}{b}-\left(\frac{a_1}{q}+...+\frac{a_n}{q^n}\right)\right)=\lim\limits_{n\to\infty}\frac{r_n}{b\cdot q^n}=0$.

Это означает, что $\frac{a}{b}=\sum\limits_{n=1}^{\infty}\frac{a_n}{q^n}$, т. е. $\frac{a}{b}=\frac{a_1}{q}+\frac{a_2}{q^2}+...+\frac{a_n}{q^n}+...=0,a_1a_2...a_n....$

Кроме этого, если бы было возможным неравенство $a_n\ge q$, то при $a_n=q$ получим $q\cdot r_{n-1}=b\cdot q+r_n$, т. е. $q\cdot r_{n-1}\ge b\cdot q$ и $r_{n-1}\ge b$, что противоречит условию $0\le r_{n-1}<b$. Получаем, что $a_n<q$, тогда $a_1,a_2,...,a_n...$ – цифры q-ичной системы счисления.

Если $\frac{a}{b}=\frac{a_1}{q}+\frac{a_2}{q^2}+...+\frac{a_n}{q^n}+...,$ то $\left[\frac{a\cdot q^n}{b}\right]=a_1q^{n-1}+a_2q^{n-2}+...+a_n$ и $\left[\frac{a\cdot q^{n-1}}{b}\right]=a_1q^{n-2}+a_2q^{n-3}+...+a_{n-1}$, тогда $a_n=\left[\frac{a\cdot q^n}{b}\right]-q\cdot\left[\frac{a\cdot q^{n-1}}{b}\right]$.

14. ПЕРИОДИЧЕСКИЕ СИСТЕМАТИЧЕСКИЕ ДРОБИ

ОПРЕДЕЛЕНИЕ. Систематическая дробь $0,a_1a_2...a_n...$ по основанию q называется чисто периодической с периодом длины s, если для всех $k\ge1$ выполняется равенство $a_k=a_{k+s}$, причем s – наименьшее натуральное число с таким свойством.

Чисто периодическая дробь с периодом длины s записывается в виде $0,(a_1a_2...a_s)$.

ОПРЕДЕЛЕНИЕ. Систематическая дробь $0,a_1a_2...a_n...$ называется смешанной периодической дробью с периодом длины s, если найдется такое число $m>0$, что для всех $k>m$ имеем $a_k=a_{k+s}$, причем s – наименьшее натуральное число с таким свойством.

Смешанная периодическая дробь с периодом длины s записывается в виде $0,a_1...a_m(a_{m+1}...a_{m+s})$, здесь $a_1...a_m$ – предпериод, $a_{m+1}...a_{m+s}$ – период дроби.

Теорема 28. *Если натуральные числа b и q взаимно простые, дробь $\frac{a}{b}$ – правильная несократимая дробь, то эта дробь представима в виде чисто периодической q-ичной дроби, период s которой равен порядку (показателю) числа q по модулю b (т. е. $P_b(q)=s$).*

Доказательство. Из того, что s – порядок числа q по модулю b, следует, что $q^s \equiv 1(\mathrm{mod}\, b)$, следовательно, число $c=\frac{q^s-1}{b}$ – целое.

$$\frac{a}{b}\cdot q^{k+s}=\frac{a\cdot q^{k+s}+a\cdot q^k-a\cdot q^k}{b}=\frac{a\cdot q^k}{b}+\frac{a\cdot q^k\left(q^s-1\right)}{b}=\frac{a\cdot q^k}{b}+a\cdot q^k\cdot c.$$

Из алгоритма представления дроби $\frac{a}{b}$ в виде q-ичной дроби получаем

$$a_{k+s}=\left[\frac{a_k\cdot q^{k+s}}{b}\right]-q\cdot\left[\frac{a\cdot q^{k+s-1}}{b}\right].$$

Тогда имеем:

$$a_{k+s}=\left[\frac{a\cdot q^{k+s}}{b}\right]-q\cdot\left[\frac{a\cdot q^{k+s-1}}{b}\right]=\left[\frac{a\cdot q^k}{b}\right]+a\cdot q^k\cdot c-q\cdot\left[\frac{a\cdot q^{k+s-1}}{b}\right]=$$

$$=\left[\frac{a\cdot q^k}{b}\right]+a\cdot q^k\cdot c-q\cdot\left[\frac{a\cdot q^{k-1}\left(1-1+q^s\right)}{b}\right]=\left[\frac{a\cdot q^k}{b}\right]+a\cdot q^k\cdot c-\left[\frac{a\cdot q^{k-1}}{b}+\frac{a\cdot q^{k-1}\left(q^s-1\right)}{b}\right]=$$

$$=\left[\frac{a\cdot q^k}{b}\right]+a\cdot q^k\cdot c-q\cdot\left[\frac{a\cdot q^{k-1}}{b}\right]+q\cdot\left[a\cdot q^{k-1}\cdot c\right]=\left[\frac{a\cdot q^k}{b}\right]-q\cdot\left[\frac{a\cdot q^{k-1}}{b}\right]=a_k,$$

т. е. $a_{k+s}=a_k$ для любых натуральных k.

Покажем, что s – наименьшее натуральное число с таким условием.

Предположим, что существует такое натуральное число t, меньшее, чем s, что $a_{k+t}=a_k$ для любых натуральных k. Тогда $a_{t+1}=a_1$, $a_{t+2}=a_2$, …, $a_{2t}=a_t$, $a_{2t+1}=a_{t+1}=a_1$ и т. д. Поэтому $\frac{a}{b}=\frac{a_1}{q}+\ldots+\frac{a_t}{q^t}+\frac{a_1}{q^{t+1}}+\ldots+\frac{a_t}{q^{2t}}+\ldots$, откуда

$$\frac{a\cdot q^t}{b}=\underbrace{a_1\cdot q^{t-1}+\ldots+a_t}_{n}+\underbrace{\frac{a_1}{q^{t+1}}+\ldots+\frac{a_t}{q^{2t}}+\ldots}_{\frac{a}{b}},$$ т. е. $\frac{a\cdot q^t}{b}=n+\frac{a}{b}$.

$a \cdot q^t = n \cdot b + a$, $a(q^t - 1) = n \cdot b$, т. е. $a(q^t - 1) \equiv 0 (\mathrm{mod}\, b)$, но по условию $(a,b) = 1$, тогда $q^t - 1 \equiv 0 (\mathrm{mod}\, b)$ или $q^t \equiv 1 (\mathrm{mod}\, b)$, чего быть не может, т. к. $0 < t < s$ и s – порядок q по модулю b.■

Примеры.

1. Определить число цифр в периоде (длину периода) при обращении обыкновенной дроби $\frac{a}{41}$, где $(a;41) = 1$, в десятичную.

1-й способ:

$q = 10,\ b = 41,\ \varphi(b) = 40$ и $40 \vdots s$. Найдем наименьшее значение $s \in \{1;2;4;5;8;10;20;40\}$ такое, что $10^s \equiv 1 (\mathrm{mod}\, 41)$.

$10 \equiv 10 (\mathrm{mod}\, 41)$;

$10^2 \equiv 100 \equiv 18 (\mathrm{mod}\, 41)$;

$10^4 \equiv 324 \equiv -4 (\mathrm{mod}\, 41)$;

$10^5 \equiv -40 \equiv 1 (\mathrm{mod}\, 41)$.

Получаем, что $s = 5$.

Ответ: длина периода равна 5.

2-й способ:

$10^s \equiv 1 (\mathrm{mod}\, 41)$, найдем наименьшее натуральное решение этого сравнения.

$s \cdot ind\, 10 \equiv ind\, 1 (\mathrm{mod}\, 40)$;

$32s \equiv 0 (\mathrm{mod}\, 40)$, $(32;40) = 8$ и $0 \vdots 8$;

$4s \equiv 0 (\mathrm{mod}\, 5)$;

$s \equiv 0 (\mathrm{mod}\, 5) \Rightarrow s = 5t, t \in Z$. Наименьшее натуральное $t = 1$, $s = 5$.

Ответ: длина периода равна 5.

Проверка: $\frac{14}{41} = 0,3414634146... = 0,(34146)$.

2. Определить число цифр в периоде при обращении обыкновенной дроби $\frac{a}{9}$, где $(a;9) = 1$, в десятичную.

Т. к. $10^1 \equiv 10 \equiv 1 (\mathrm{mod}\, 9)$, то $s = 1$.

Ответ: длина периода равна 1.

Если знаменатель b дроби $\frac{a}{b}$ в разложении на простые множители содержит числа, не входящие в каноническое разложение числа q, $b = p_1^{\alpha_1} \cdot ... \cdot p_k^{\alpha_k} \cdot g_1^{\beta_1} \cdot ... \cdot g_t^{\beta_t}$ и $q = p_1^{\gamma_1} \cdot ... \cdot p_k^{\gamma_k}$, где q не делится на простые числа $g_1, ..., g_t$, тогда правильная несократимая дробь $\frac{a}{b}$ представима в виде смешанной периодической дроби $\frac{a}{b} = 0, a_1 ... a_m (a_{m+1} ... a_{m+s})$, где $m = \max(\alpha_1, ..., \alpha_k)$, s – порядок числа q по модулю $c = g_1^{\beta_1} \cdot ... \cdot g_t^{\beta_t}$.

Пример.

Определить число знаков в предпериоде и периоде десятичной дроби, получающейся при обращении в десятичную обыкновенной дроби $\frac{599}{280}$.

$\frac{599}{280} = 2 + \frac{39}{280}$, $q = 10 = 2 \cdot 5$, $b = 280 = 2^3 \cdot 5 \cdot 7$; q не делится на 7, $\beta = 1$; $\alpha_1 = 3, \alpha_2 = 1$.

$m = \max(3;1) = 3 \Rightarrow$ предпериод содержит 3 цифры.

Определим длину периода, как порядок числа 10 по модулю 7:

$\varphi(7) = 6$, $6 \vdots 1; 2; 3; 6$;

$10 \equiv 3 (\mathrm{mod}\, 7)$;

$10^2 \equiv 9 \equiv 2 (\mathrm{mod}\, 7)$;

$10^3 \equiv 6 (\mathrm{mod}\, 7)$;

$10^6 \equiv 8 \equiv 1 (\mathrm{mod}\, 7)$, следовательно, $s = 6$.

Ответ: в предпериоде 3 цифры, в периоде 6 цифр.

Проверка: $\frac{599}{280} = 2{,}139(285714)$.

15. ПРОВЕРКА АРИФМЕТИЧЕСКИХ ДЕЙСТВИЙ

Пусть для целых чисел a и b остатки от деления на натуральное число m равны соответственно r_a и r_b. Тогда справедливы сравнения $a \equiv r_a (\mathrm{mod}\, m)$ и $b \equiv r_b (\mathrm{mod}\, m)$. Чтобы найти остаток от деления суммы чисел a и b на m, мож-

но найти наименьший неотрицательный вычет, сравнимый с $r_a + r_b$ по модулю m, т. е. $a+b \equiv r_a + r_b \equiv r_+ (\mathrm{mod}\, m)$. Аналогично $a-b \equiv r_a - r_b \equiv r_- (\mathrm{mod}\, m)$ и $a \cdot b \equiv r_a \cdot r_b \equiv r_\times (\mathrm{mod}\, m)$.

Если $a : b = c$, то $a = b \cdot c$, следовательно, $a \equiv r_a \equiv b \cdot c \equiv r_b \cdot r_c (\mathrm{mod}\, m)$, где r_c – остаток от деления числа c на m.

Рассмотрим систематическую запись числа a в десятичной системе счисления

$$a = \overline{a_k a_{k-1} \ldots a_1 a_0} = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0 = (a_k + \ldots + a_1 + a_0) + 9 \cdot \left(a_k \cdot \underbrace{1 \ldots 1}_{k-1} + \ldots + a_1 \right).$$

Получаем, что $a \equiv a_k + \ldots + a_1 + a_0 (\mathrm{mod} 9)$, что означает: число сравнимо по модулю 9 с суммой своих цифр.

Иначе $a = \overline{a_k a_{k-1} \ldots a_1 a_0} = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0 =$

$$= a_k (11-1)^k + a_{k-1} (11-1)^{k-1} + \ldots + a_2 (11-1)^2 + a_1 (11-1) + a_0 .$$

Применим бином Ньютона:

$$(11-1)^n = 11^n + (-1) n \cdot 11^{n-1} \cdot 1 + (-1)^2 \cdot n \cdot (n-1) \cdot 11^{n-2} \cdot 1^2 + \ldots + (-1)^{n-2} \cdot n \cdot (n-1) \cdot 11^2 \cdot 1^{n-2} +$$
$$+ (-1)^{n-1} \cdot n \cdot 11 \cdot 1^{n-1} + (-1)^n \cdot 1^n = 11 \cdot T_n + (-1)^n .$$

Тогда получим $a = (-1)^k \cdot a_k + \ldots + a_2 - a_1 + a_0 + 11 \cdot (a_k \cdot T_k + \ldots + a_2 \cdot T_2 + a_1 \cdot T_1)$, следовательно, $a \equiv (-1)^k \cdot a_k + \ldots + a_2 - a_1 + a_0 (\mathrm{mod} 11)$, т. е. число сравнимо со знакочередующейся суммой своих цифр по модулю 11, причем последняя (справа) цифра берется со знаком «+».

Проверку арифметических действий можно провести при помощи модуля 9 или модуля 11. В более сложных вычислениях проверку проводят при помощи обоих модулей.

Правильность соответствующего сравнения не гарантирует правильности вычислений, а лишь подтверждает его. Если же при вычислении допущена ошибка, кратная модулю, то обнаружить ее не удастся.

Примеры.

Проверить правильность выполнения действий с помощью модулей 9 и 11.

1. $8740297 - 561245 = 8179052$.

Проверяем с помощью $m=9$.

Суммы цифр чисел равны: $S_{8740297}=37$, $S_{561245}=23$, $S_{8179052}=32$.

Т. к. $37-23\equiv 32(\mathrm{mod}9)$ истинное сравнение, то правильность вычислений подтверждается, но не гарантируется. Если ошибка допущена, то она кратна 9.

Проверяем с помощью $m=11$.

Знакочередующиеся суммы цифр чисел равны: $G_{8740297}=5$, $G_{561245}=3$, $G_{8179052}=2$.

Т. к. $5-3\equiv 2(\mathrm{mod}11)$ истинное сравнение, то правильность вычислений подтверждается, но не гарантируется. Если ошибка допущена, то она кратна 11.

Совместная проверка по двум модулям не гарантирует правильность вычисления, если ошибка допущена, то она кратна 99.

2. $\underbrace{1443888276}_{a}:\underbrace{375426}_{b}=\underbrace{3846}_{c}$. Здесь имеем $a:b=c$, следовательно, $a=b\cdot c$.

Проверим с помощью $m=9$. $S_{1443888276}=51$, $S_{375426}=27$, $S_{3846}=21$. Получаем сравнение $27\cdot 21\equiv 51(\mathrm{mod}9)$, оно равносильно сравнению $0\cdot 3\equiv 6(\mathrm{mod}9)$, которое является ложным. Вывод: при вычислении частного допущена ошибка.

Упражнения для самостоятельного решения

Проверить правильность вычисления:

1) $4256821+231572=4488393$;
2) $7483612-60032=7423380$;
3) $1240214\cdot 3257=4039376998$;
4) $841674246056:731612=1150438$.

16. ПРИЗНАКИ ДЕЛИМОСТИ

Признак делимости целого числа на натуральное число призван облегчить задачу поиска натуральных делителей числа.

Для построения признака делимости необходимо решить следующую проблему. Пусть дано некоторое натуральное число N, которое имеет натуральный делитель d, необходимо построить некоторую числовую функцию $f(N)$, принимающую целые значения и отвечающую условиям:

1) N и $f(N)$ одновременно делятся или одновременно не делятся на d;

2) $|f(N)| < N$, кроме случаев, когда N достаточно мало;

3) при данном N значение функции $f(N)$ вычисляется достаточно просто.

Ясно, что если функция $f(N)$ будет построена, то применять ее можно будет и для определения делимости значения $|f(N)|$ на d, а именно в том случае, когда $|f(N)|$ достаточно велико, то для определения делимости $|f(N)|$ на d проверяют делимость на d значения $f(|f(N)|)$ и т. д. до тех пор, пока не получится число, для которого определяем, делится ли оно на d.

Достаточно построить признаки делимости числа на $d = p^{\alpha}$, т. к. если число N делится на $p_1^{\alpha_1}$, $p_2^{\alpha_2}$, …, $p_k^{\alpha_k}$, то оно делится на $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$, где $p_1, ..., p_k$ – различные простые числа.

Способ Паскаля[10]. Способ использует систематическую запись натурального числа в десятичной системе счисления $N = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0$, где $a_n, a_{n-1}, ..., a_1, a_0$ – цифры десятичной системы счисления, т. е. $0 \le a_i \le 9$ для $i \in \{0;1;...,n-1\}$ и $1 \le a_n \le 9$. Число N заменяют меньшим натуральным числом M, сравнимым с N по модулю d. Для построения числа M степени 10 в систематической записи числа N заменяют наименьшими неотрицательными вычетами по модулю d. Если $10^k \equiv c_k (\mathrm{mod}\, d)$, то $M = a_n \cdot c_n + a_{n-1} \cdot c_{n-1} + ... + a_1 \cdot c_1 + a_0$. Тогда $M = f(N) \equiv N (\mathrm{mod}\, d)$. Из данного сравнения видно, что если M делится на d, то и N делится на d, и

[10] Паскаль Блез (Pascal Blaise) (19.06.1623–19.08.1662) – французский философ, писатель, математик и физик.

если M не делится на d, то и N не делится на d. В том случае, когда M велико, его заменяют числом $K = f(M) = f(f(N))$.

Признак делимости на 2.

Здесь все $c_k = 0$, следовательно, $N \equiv a_0 (\mathrm{mod}\, 2)$. Число N делится на 2, если его последняя цифра a_0 делится на 2 (равна 0, 2, 4, 6 или 8, т. е. четная).

Признак делимости на 3.

Здесь все $c_k = 1$, следовательно, $N \equiv a_n + ... + a_1 + a_0 (\mathrm{mod}\, 3)$. Число N делится на 3, если сумма его цифр делится на 3.

Признак делимости на 4.

Здесь $c_1 = \pm 2$, все остальные $c_k = 0$, следовательно, $N \equiv \pm 2a_1 + a_0 (\mathrm{mod}\, 4)$. Число N делится на 4, если на 4 делится число, равное сумме (разности) последней цифры и удвоенной предпоследней цифры числа N.

Примеры.

1. Число 3568 делится на 4, т. к. $8 + 6 \cdot 2 = 20 \vdots 4$ (или $8 - 6 \cdot 2 = -4 \vdots 4$).
2. Число 1748266 не делится на 4, т. к. $6 + 6 \cdot 2 = 18 \neq 4t, t \in Z$.

Признак делимости на 5.

Здесь все $c_k = 0$, следовательно, $N \equiv a_0 (\mathrm{mod}\, 5)$. Число N делится на 5, если его последняя цифра a_0 делится на 5 (т. е. равна 0 или 5).

Признак делимости на 6.

Здесь все $c_k = -2$, следовательно, $N \equiv -2(a_n + ... + a_1) + a_0 (\mathrm{mod}\, 6)$. Число N делится на 6, если на 6 делится разность его последней цифры и удвоенной суммы остальных цифр.

Пример.

Число 166134 делится на 6, т. к. $4 - 2 \cdot (3 + 1 + 6 + 6 + 1) = 4 - 34 = -30 \vdots 6$.

Признак делимости на 7.

Здесь $c_1 = 3$, $c_2 = 2$, $c_3 = -1$, $c_4 = -3$, $c_5 = -2$, $c_6 = 1$, $c_7 = 3$, $c_8 = 2$ и т. д. периодически, следовательно, $N \equiv (a_0 + 3a_1 + 2a_2) - (a_3 + 3a_4 + 2a_5) + ... (\mathrm{mod}\, 7)$.

Примеры.

1. Число 24836 делится на 7, т. к. $6+3\cdot 3+8\cdot 2-4-3\cdot 2=21\vdots 7$.
2. Число 17335621 не делится на 7, т. к. $1+2\cdot 3+6\cdot 2-5-3\cdot 3-2\cdot 3+7+3\cdot 1=9$ не делится на 7.

Признак делимости на 8.

Здесь $c_1=2$, $c_2=\pm 4$, все остальные $c_k=0$, следовательно, $N\equiv \pm 4a_2+2a_1+a_0 (\mathrm{mod}8)$.

Примеры.

1. Число 1235792 делится на 8, т. к. $2+2\cdot 9-4\cdot 7=-8\vdots 8$.
2. Число 3255617236 не делится на 8, т. к. $6+2\cdot 3+4\cdot 2=20$ не делится на 8.

Признак делимости на 9.

Здесь все $c_k=1$, следовательно, $N\equiv a_n+\ldots+a_1+a_0 (\mathrm{mod}9)$. Число N делится на 9, если сумма его цифр делится на 9.

Признак делимости на 11.

Здесь $c_1=-1$, $c_2=+1$, $c_3=-1$, $c_4=+1$ и т. д., следовательно, $N\equiv a_0-a_1+a_2-a_3+\ldots (\mathrm{mod}11)$. Число N делится на 11, если знакочередующаяся сумма цифр его делится на 11.

Признак делимости на 13.

Здесь $c_1=-3$, $c_2=-4$, $c_3=-1$, $c_4=3$, $c_5=4$, $c_6=1$, $c_7=-3$ и т. д. периодически, следовательно, $N\equiv (a_0-3a_1-4a_2)-(a_3-3a_4-4a_5)+\ldots (\mathrm{mod}13)$.

Примеры.

1. Число 34512052 не делится на 13, т. к.

   $2-3\cdot 5-4\cdot 0-(2-3\cdot 1-4\cdot 5)+4-3\cdot 3=3$ не делится на 13.
2. Число 1503151117 делится на 13, т. к.

   $7-3\cdot 1-4\cdot 1-(1-3\cdot 5-4\cdot 1)+3-3\cdot 0-4\cdot 5-1=0\vdots 13$.

Упражнения для самостоятельного решения

Вывести признаки делимости на q:

1) $q=17$; 2) $q=19$; 3) $q=23$.

ЗАДАЧИ ДЛЯ САМОСТОЯТЕЛЬНОГО РЕШЕНИЯ

1. Даны числа $a_1, a_2, ..., a_{m-1}$. Найти такое натуральное число $a_m \le m$, чтобы числа $a_1, a_2, ..., a_m$ составили полную систему вычетов по модулю m.

$m = 8$

1) $3, -14, -1, 16, 6, 21, 28$;

2) $-77, -8, -47, -60, -10, -30, -514$;

3) $-7, 43, 71, 38, 109, -6, -16$;

4) $18, -12, 64, -5, 29, -23, -42$;

5) $-17, -10, 0, -7, 2, 3, 21$;

6) $105, -13, -26, 20, -35, 0$;

$m = 7$

7) $15, -12, -18, 77, 48, -30$;

8) $-7, -50, 30, 80, 60, 40$;

9) $18, 71, -44, 44, -36, 35$;

10) $109, -35, -65, 15, -4, 51$;

11) $-71, -69, -45, -4, 5, -70$;

12) $-7, 10, -20, 30, 55, 59$;

$m = 6$

13) $25, -34, 33, 76, -37$;

14) $-12, 43, 56, 46, -33$;

15) $241, -242, 15, 150, -82$;

16) $75, -22, 14, 11, 12$;

17) $105, 104, 103, 102, 101$;

18) $-1, -2, -3, -4, -5$;

19) $102, 115, 128, -7, -123$;

20) $1, -22, 57, -38, -31$;

$m = 9$

21) $-36, -25, 37, 105, -31, 30, 22, 43$;

22) $44, -26, 38, 106, 31, 12, 50, 63$;

23) $-80, -25, -93, 58, -180, -13, -39, 70$;

24) $62, -372, -18, -771, 230, 42, -108, 1$.

2. Найти такое натуральное число $a_n < m$, чтобы числа $a_1, a_2, ..., a_n$ составили приведенную систему вычетов по модулю m.

1) $m = 13$; $-101, 121, 31, 422, 14, 61, 50, -31, 23, 25, 20$;

2) $m = 16$; $-11, 23, 43, -65, 45, -63, 115$;

3) $m = 20$; $-39, -83, 23, -127, 105, 9, -29$;

4) $m = 15$; $37, -22, -146, -119, 44, 77, 26$;

5) $m = 16$; $105, -95, 123, -61, -19, 85, 167$;

6) $m = 22;$ $65, 41, 25, -167, -29, 45, -97, -103, 31;$

7) $m = 20;$ $37, 312, -71, -39, -93, 103;$

8) $m = 14;$ $25, -13, 17, 33, 23;$

9) $m = 15;$ $164, -43, 49, 28, -64;$

10) $m = 9;$ $11, 13, 23, 79, -116;$

11) $m = 16;$ $-47, 117, -51, -25, 89, -37, 31;$

12) $m = 20;$ $81, 23, -71, 111, -27, -193, 139;$

13) $m = 11;$ $-9, 87, 116, 122, 19, -41, 5, -51, -46;$

14) $m = 14;$ $-29, 145, -97, 53, -109;$

15) $m = 16;$ $-1, 43, -109, 17, -43, -55, 77;$

16) $m = 22;$ $23, -17, -201, 31, -103, 79, -51, 39, -23;$

17) $m = 15;$ $122, 23, -14, 43, -41, -109, 37;$

18) $m = 16;$ $21, 39, -77, -103, 273, -21, -1;$

19) $m = 20;$ $-11, -13, 3, -49, -101, -87, 219;$

20) $m = 14;$ $-25, -57, 79, -41, -73;$

21) $m = 16;$ $-37, 163, -41, 49, -33;$

22) $m = 13;$ $27, -11, 42, -931, -20, 46, 73, 179, 48, 103;$

23) $m = 22;$ $-17, -29, 45, -97, -103, 31, 65, 41, 25;$

24) $m = 15;$ $62, -94, -83, -46, 79, 68, 43.$

3. Найти значение φ функции Эйлера от числа:

1)	121;	2)	137;	3)	141;	4)	157;
5)	168;	6)	202;	7)	222;	8)	278;
9)	486;	10)	341;	11)	356;	12)	380;
13)	399;	14)	432;	15)	468;	16)	621;
17)	725;	18)	720;	19)	901;	20)	768;

21) 697; 22) 648; 23) 578; 24) 845.

4. Решить уравнение $\varphi(p^x)=a$.

1) $a=500;\ p=5;$ 2) $a=54;\ p=3;$ 3) $a=67240;\ p=41;$

4) $a=2500;\ p=5;$ 5) $a=162;\ p=3;$ 6) $a=13122;\ p=3;$

7) $a=18;\ p=3;$ 8) $a=4374;\ p=3;$ 9) $a=294;\ p=7;$

10) $a=12500;\ p=5;$ 11) $a=486;\ p=3;$ 12) $a=1296;\ p=3;$

13) $a=14406;\ p=7;$ 14) $a=1210;\ p=11;$ 15) $a=2028;\ p=13;$

16) $a=4624;\ p=17;$ 17) $a=6498;\ p=19;$ 18) $a=11638;\ p=23;$

19) $a=23548;\ p=29;$ 20) $a=28830;\ p=31;$ 21) $a=13310;\ p=11;$

22) $a=49284;\ p=37;$ 23) $a=26364;\ p=13;$ 24) $a=123462;\ p=19.$

5. Найти p^α, если $\varphi(p^\alpha)=a$.

1) $a=4970;$ 2) $a=42;$ 3) $a=110;$ 4) $a=8;$

5) $a=294;$ 6) $a=506;$ 7) $a=64;$ 8) $a=128;$

9) $a=256;$ 10) $a=512;$ 11) $a=132;$ 12) $a=100;$

13) $a=54;$ 14) $a=1640;$ 15) $a=812;$ 16) $a=156;$

17) $a=272;$ 18) $a=342;$ 19) $a=930;$ 20) $a=162;$

21) $a=1806;$ 22) $a=3422;$ 23) $a=3660;$ 24) $a=16.$

6. Найти остаток от деления a^m на b.

1) $a=126;\ m=201;\ b=67;$ 2) $a=229;\ m=127;\ b=143;$

3) $a=199;\ m=125;\ b=45;$ 4) $a=401;\ m=206;\ b=31;$

5) $a=187;\ m=88;\ b=43;$ 6) $a=225;\ m=111;\ b=53;$

7) $a=221;\ m=102;\ b=42;$ 8) $a=383;\ m=175;\ b=45;$

9) $a=343;\ m=101;\ b=64;$ 10) $a=843;\ m=326;\ b=68;$

11) $a=478;\ m=113;\ b=27;$ 12) $a=231;\ m=148;\ b=104;$

13) $a=297;\ m=79;\ b=70;$ 14) $a=217;\ m=348;\ b=66;$

15) $a=292;\ m=150;\ b=95;$ 16) $a=262;\ m=114;\ b=51;$

17) $a=137;\ m=113;\ b=45;$ 18) $a=426;\ m=101;\ b=105;$

19) $a=311;\ m=465;\ b=50;$ 20) $a=337;\ m=169;\ b=83;$

21) $a=280;\ m=183;\ b=77;$ 22) $a=257;\ m=191;\ b=61;$

23) $a=239;\ m=149;\ b=74;$ 24) $a=257;\ m=182;\ b=45.$

7. Найти остаток от деления a^m на b.

1) $a=444;\ m=144;\ b=44;$ 2) $a=333;\ m=152;\ b=39;$

3) $a=57;\ m=67;\ b=192;$ 4) $a=102;\ m=151;\ b=74;$

5) $a=445;\ m=66;\ b=65;$ 6) $a=44;\ m=126;\ b=100;$

7) $a=365;\ m=62;\ b=95;$ 8) $a=231;\ m=52;\ b=69;$

9) $a=135;\ m=41;\ b=39;$ 10) $a=400;\ m=54;\ b=68;$

11) $a=25;\ m=200;\ b=55;$ 12) $a=50;\ m=111;\ b=74;$

13) $a=195;\ m=197;\ b=85;$ 14) $a=345;\ m=147;\ b=33;$

15) $a=579;\ m=60;\ b=99;$ 16) $a=88;\ m=183;\ b=209;$

17) $a=205;\ m=127;\ b=66;$ 18) $a=180;\ m=106;\ b=105;$

19) $a=91;\ m=125;\ b=385;$ 20) $a=50;\ m=155;\ b=78;$

21) $a=147;\ m=155;\ b=117;$ 22) $a=98;\ m=147;\ b=78;$

23) $a=90;\ m=123;\ b=82;$ 24) $a=354;\ m=174;\ b=33.$

8. Найти две последние цифры числа a^b.

1) $a=221;\ b=201;$ 2) $a=241;\ b=301;$

3) $a=517;\ b=201;$ 4) $a=327;\ b=301;$

5) $a=277;\ b=501;$ 6) $a=301;\ b=303;$

7) $a=601;\ b=603;$ 8) $a=403;\ b=201;$

9) $a=113;\ b=301;$ 10) $a=289;\ b=601;$

11) $a = 387;\ b = 201;$

12) $a = 399;\ b = 201;$

13) $a = 401;\ b = 301;$

14) $a = 461;\ b = 301;$

15) $a = 497;\ b = 501;$

16) $a = 501;\ b = 52;$

17) $a = 517;\ b = 101;$

18) $a = 537;\ b = 601;$

19) $a = 317;\ b = 501;$

20) $a = 279;\ b = 101;$

21) $a = 419;\ b = 201;$

22) $a = 819;\ b = 301;$

23) $a = 717;\ b = 501;$

24) $a = 317;\ b = 601.$

9. Решить сравнения.

1) $48x \equiv 32 (\mathrm{mod} 115);$

2) $131x \equiv 82 (\mathrm{mod} 64);$

3) $60x \equiv 90 (\mathrm{mod} 203);$

4) $125x \equiv 187 (\mathrm{mod} 312);$

5) $131x \equiv 218 (\mathrm{mod} 136);$

6) $66x \equiv 99 (\mathrm{mod} 199);$

7) $113x \equiv 64 (\mathrm{mod} 312);$

8) $41x \equiv 16 (\mathrm{mod} 37);$

9) $60x \equiv 90 (\mathrm{mod} 37);$

10) $58x \equiv 80 (\mathrm{mod} 111);$

11) $23x \equiv 667 (\mathrm{mod} 963);$

12) $35x \equiv 25 (\mathrm{mod} 720);$

13) $427x \equiv 181 (\mathrm{mod} 300);$

14) $113x \equiv 89 (\mathrm{mod} 311);$

15) $221x \equiv 111 (\mathrm{mod} 360);$

16) $48x \equiv 24 (\mathrm{mod} 125);$

17) $54x \equiv 81 (\mathrm{mod} 125);$

18) $80x \equiv 40 (\mathrm{mod} 231);$

19) $80x \equiv 100 (\mathrm{mod} 121);$

20) $78x \equiv 26 (\mathrm{mod} 101);$

21) $131x \equiv 72 (\mathrm{mod} 70);$

22) $40x \equiv 100 (\mathrm{mod} 363);$

23) $20x \equiv 50 (\mathrm{mod} 91);$

24) $271x \equiv 25 (\mathrm{mod} 119).$

10. Решить сравнения.

1) $164x \equiv 68 (\mathrm{mod} 176);$

2) $138x \equiv 42 (\mathrm{mod} 76);$

3) $200x \equiv 104 (\mathrm{mod} 312);$

4) $78x \equiv 42 (\mathrm{mod} 51);$

5) $114x \equiv 42 (\mathrm{mod} 87);$

6) $543x \equiv 93 (\mathrm{mod} 582);$

7) $291x \equiv 99 (\mathrm{mod}\, 597)$;

8) $303x \equiv 93 (\mathrm{mod}\, 600)$;

9) $39x \equiv 84 (\mathrm{mod}\, 93)$;

10) $128x \equiv 84 (\mathrm{mod}\, 126)$;

11) $114x \equiv 52 (\mathrm{mod}\, 110)$;

12) $324x \equiv 88 (\mathrm{mod}\, 250)$;

13) $200x \equiv 208 (\mathrm{mod}\, 612)$;

14) $145x \equiv 390 (\mathrm{mod}\, 250)$;

15) $219x \equiv 120 (\mathrm{mod}\, 375)$;

16) $273x \equiv 99 (\mathrm{mod}\, 303)$;

17) $386x \equiv 22 (\mathrm{mod}\, 570)$;

18) $230x \equiv 190 (\mathrm{mod}\, 300)$;

19) $203x \equiv 91 (\mathrm{mod}\, 280)$;

20) $85x \equiv 45 (\mathrm{mod}\, 225)$;

21) $145x \equiv 80 (\mathrm{mod}\, 500)$;

22) $303x \equiv 78 (\mathrm{mod}\, 363)$;

23) $130x \equiv 100 (\mathrm{mod}\, 200)$;

24) $49x \equiv 55 (\mathrm{mod}\, 133)$.

11. Решить сравнения.

1) $546x \equiv 36 (\mathrm{mod}\, 600)$;

2) $88x \equiv 55 (\mathrm{mod}\, 121)$;

3) $184x \equiv 56 (\mathrm{mod}\, 320)$;

4) $260x \equiv 68 (\mathrm{mod}\, 308)$;

5) $115x \equiv 95 (\mathrm{mod}\, 150)$;

6) $63x \equiv 39 (\mathrm{mod}\, 480)$;

7) $104x \equiv 156 (\mathrm{mod}\, 486)$;

8) $100x \equiv 80 (\mathrm{mod}\, 168)$;

9) $165x \equiv 21 (\mathrm{mod}\, 312)$;

10) $465x \equiv 65 (\mathrm{mod}\, 605)$;

11) $230x \equiv 200 (\mathrm{mod}\, 285)$;

12) $172x \equiv 28 (\mathrm{mod}\, 200)$;

13) $201x \equiv 48 (\mathrm{mod}\, 183)$;

14) $124x \equiv 88 (\mathrm{mod}\, 160)$;

15) $129x \equiv 321 (\mathrm{mod}\, 471)$;

16) $115x \equiv 85 (\mathrm{mod}\, 355)$;

17) $385x \equiv 22 (\mathrm{mod}\, 570)$;

18) $230x \equiv 190 (\mathrm{mod}\, 300)$;

19) $203x \equiv 91 (\mathrm{mod}\, 280)$;

20) $85x \equiv 45 (\mathrm{mod}\, 225)$;

21) $452x \equiv 68 (\mathrm{mod}\, 488)$;

22) $82x \equiv 110 (\mathrm{mod}\, 130)$;

23) $201x \equiv 39 (\mathrm{mod}\, 261)$;

24) $500x \equiv 64 (\mathrm{mod}\, 328)$.

12. Решить сравнения.

1) $41x^{31} + 17x^{14} + 7x^2 - 3 \equiv 0 (\mathrm{mod}\, 5)$;

2) $32x^{20} + 15x^{10} - 111x^4 + x - 1 \equiv 0 (\mathrm{mod}\, 7)$;

3) $43x^{18}+27x^{14}+15x^8+3x^3+2\equiv 0(\mathrm{mod}\,7)$;

4) $26x^{20}+17x^{11}+9x^4+2x^2+1\equiv 0(\mathrm{mod}\,5)$;

5) $82x^{32}-27x^{14}+11x^5+x^2-2\equiv 0(\mathrm{mod}\,5)$;

6) $73x^{35}+24x^{15}+17x^3+8\equiv 0(\mathrm{mod}\,7)$;

7) $53x^{18}+15x^{11}+7x^5-3x+1\equiv 0(\mathrm{mod}\,7)$;

8) $81x^{29}+15x^{21}+3x^3+13x+2\equiv 0(\mathrm{mod}\,5)$;

9) $52x^{31}+21x^{14}-5x^4+x^2-1\equiv 0(\mathrm{mod}\,7)$;

10) $83x^{21}+42x^{11}-10x^{10}+x+1\equiv 0(\mathrm{mod}\,5)$;

11) $48x^8+36x^7-x^6+12x^5+3x^4-x^3+9x^2+8x-2\equiv 0(\mathrm{mod}\,5)$;

12) $31x^{20}+17x^{11}+9x^8+15x^7-6x^4+3x^2+11\equiv 0(\mathrm{mod}\,5)$;

13) $27x^{32}+17x^{21}+24x^{16}+17x^{10}+21x^6+27x^4+3x^2-1\equiv 0(\mathrm{mod}\,5)$;

14) $71x^{31}+27x^{20}-18x^{16}-3x^8+12x^7-10x^6+29x^4-17x+4\equiv 0(\mathrm{mod}\,5)$;

15) $22x^{20}-18x^{17}+73x^{10}-7x^2-1\equiv 0(\mathrm{mod}\,5)$;

16) $121x^{21}+17x^{18}-56x^{12}+31x^9-12x^5+7x^3-2\equiv 0(\mathrm{mod}\,5)$;

17) $25x^{24}-17x^{15}+29x^{11}-18x^7+11\equiv 0(\mathrm{mod}\,5)$;

18) $27x^{25}-19x^{20}-72x^{15}+28x^{12}+16x^3-1\equiv 0(\mathrm{mod}\,7)$;

19) $31x^{37}-29x^{21}+29x^{15}+3x^2+1\equiv 0(\mathrm{mod}\,5)$;

20) $29x^{31}-17x^{14}-37x^{13}+16x^2-1\equiv 0(\mathrm{mod}\,7)$;

21) $24x^{30}-16x^{26}+20x^8-x+1\equiv 0(\mathrm{mod}\,7)$;

22) $26x^{20}-50x^{16}+47x^{15}-27x^4-15x^2-2\equiv 0(\mathrm{mod}\,7)$;

23) $72x^{21}+17x^{15}-24x^{10}-x+3\equiv 0(\mathrm{mod}\,5)$;

24) $-26x^{18}+72x^{15}-24x^{10}+17x^2+6\equiv 0(\mathrm{mod}\,7)$.

13. Решить в целых числах уравнения.

1) $253x-449y=3$;

2) $73x+85y=7$;

3) $311x+28y=2$;

4) $204x-697y=51$;

5) $91x-52y=13;$ 6) $76x+114y=14;$

7) $74x+185y=111;$ 8) $58x-87y=145;$

9) $116x+174y=290;$ 10) $111x-222y=555;$

11) $25x+33y=15;$ 12) $37x-13y=5;$

13) $83x+12y=17;$ 14) $26x+91y=11;$

15) $44x-187y=22;$ 16) $33x+51y=21;$

17) $612x-85y=34;$ 18) $107x+84y=1;$

19) $73x+85y=7;$ 20) $34x+42y=16;$

21) $37x-54y=1;$ 22) $81x+52y=5;$

23) $53x-49y=5;$ 24) $15x+13y=7.$

14. Найти показатель $P_m(a)$ числа a по модулю m.

1) $P_{29}(3);$ 2) $P_{23}(10);$ 3) $P_{37}(3);$ 4) $P_{23}(4);$

5) $P_{31}(4);$ 6) $P_{11}(5);$ 7) $P_{17}(11);$ 8) $P_{23}(4);$

9) $P_{29}(8);$ 10) $P_{37}(8);$ 11) $P_{31}(10);$ 12) $P_{23}(7);$

13) $P_{11}(12);$ 14) $P_{23}(14);$ 15) $P_{29}(5);$ 16) $P_{13}(7);$

17) $P_{17}(9);$ 18) $P_{31}(4);$ 19) $P_{23}(15);$ 20) $P_{23}(20);$

21) $P_{31}(7);$ 22) $P_{17}(9);$ 23) $P_{23}(11);$ 24) $P_{19}(12).$

15. Используя индексы, решить сравнения.

1) $5x^5 \equiv 10(\mathrm{mod}17);$ 2) $4x^{11} \equiv 13(\mathrm{mod}29);$

3) $19x^7 \equiv 9(\mathrm{mod}31);$ 4) $15x^7 \equiv 9(\mathrm{mod}17);$

5) $27x^{13} \equiv 20(\mathrm{mod}31);$ 6) $9x^{11} \equiv 26(\mathrm{mod}31);$

7) $11x^5 \equiv 5(\mathrm{mod}47);$ 8) $17x^5 \equiv 2(\mathrm{mod}37);$

9) $11x^9 \equiv 9(\mathrm{mod}17);$ 10) $6x^5 \equiv 2(\mathrm{mod}19);$

11) $31x^7 \equiv 2(\mathrm{mod}37);$ 12) $11x^{13} \equiv 15(\mathrm{mod}43);$

13) $15x^{11} \equiv 52 (\mathrm{mod}\, 59)$;

14) $15x^{5} \equiv 4 (\mathrm{mod}\, 37)$;

15) $2x^{7} \equiv 12 (\mathrm{mod}\, 19)$;

16) $17x^{5} \equiv 13 (\mathrm{mod}\, 73)$;

17) $16x^{11} \equiv 11 (\mathrm{mod}\, 19)$;

18) $6x^{7} \equiv 11 (\mathrm{mod}\, 41)$;

19) $11x^{7} \equiv 5 (\mathrm{mod}\, 23)$;

20) $36x^{11} \equiv 26 (\mathrm{mod}\, 41)$;

21) $13x^{17} \equiv 28 (\mathrm{mod}\, 73)$;

22) $11x^{5} \equiv 28 (\mathrm{mod}\, 59)$;

23) $53x^{11} \equiv 72 (\mathrm{mod}\, 83)$;

24) $24x^{9} \equiv 21 (\mathrm{mod}\, 47)$.

16. Используя индексы, решить сравнения.

1) $2^{x} \equiv 13 (\mathrm{mod}\, 67)$;

2) $3^{x} \equiv 19 (\mathrm{mod}\, 79)$;

3) $2^{x} \equiv 71 (\mathrm{mod}\, 83)$;

4) $3^{x} \equiv 41 (\mathrm{mod}\, 89)$;

5) $2^{x} \equiv (\mathrm{mod}\, 31)$;

6) $2^{x} \equiv 17 (\mathrm{mod}\, 59)$;

7) $3^{x} \equiv 15 (\mathrm{mod}\, 43)$;

8) $3^{x} \equiv 18 (\mathrm{mod}\, 29)$;

9) $27^{x} \equiv 4 (\mathrm{mod}\, 17)$;

10) $2^{x} \equiv 15 (\mathrm{mod}\, 53)$;

11) $2^{x} \equiv 43 (\mathrm{mod}\, 59)$;

12) $3^{x} \equiv 18 (\mathrm{mod}\, 43)$;

13) $2^{x} \equiv 51 (\mathrm{mod}\, 67)$;

14) $3^{x} \equiv 71 (\mathrm{mod}\, 89)$;

15) $2^{x} \equiv 24 (\mathrm{mod}\, 67)$;

16) $13^{x} \equiv 12 (\mathrm{mod}\, 19)$;

17) $2^{x} \equiv 43 (\mathrm{mod}\, 53)$;

18) $3^{x} \equiv 14 (\mathrm{mod}\, 31)$;

19) $2^{x} \equiv 45 (\mathrm{mod}\, 59)$;

20) $3^{x} \equiv 24 (\mathrm{mod}\, 89)$;

21) $2^{x} \equiv 23 (\mathrm{mod}\, 67)$;

22) $3^{x} \equiv 41 (\mathrm{mod}\, 43)$;

23) $2^{x} \equiv 38 (\mathrm{mod}\, 61)$;

24) $3^{x} \equiv 47 (\mathrm{mod}\, 89)$.

17. Используя индексы, решить сравнения.

1) $36x \equiv 25 (\mathrm{mod}\, 71)$;

2) $28x \equiv 35 (\mathrm{mod}\, 79)$;

3) $43x \equiv 5 (\mathrm{mod}\, 53)$;

4) $17x \equiv 16 (\mathrm{mod}\, 71)$;

5) $17x \equiv 60 (\mathrm{mod}\, 73)$;

6) $35x \equiv 29 (\mathrm{mod}\, 53)$;

7) $19x \equiv 40 (\mathrm{mod}\, 71)$;

8) $59x \equiv 23 (\mathrm{mod}\, 73)$;

9) $36x \equiv 4 (\mathrm{mod}\, 47)$;

10) $38x \equiv 14 (\mathrm{mod}\, 67)$;

11) $65x \equiv 33 (\mathrm{mod}\, 83)$;

12) $37x \equiv 35 (\mathrm{mod}\, 47)$;

13) $25x \equiv 23 (\mathrm{mod}\, 67)$;

14) $37x \equiv 57 (\mathrm{mod}\, 83)$;

15) $39x \equiv 14 (\mathrm{mod}\, 47)$;

16) $51x \equiv 9 (\mathrm{mod}\, 67)$;

17) $16x \equiv 56 (\mathrm{mod}\, 89)$;

18) $57x \equiv 37 (\mathrm{mod}\, 59)$;

19) $33x \equiv 20 (\mathrm{mod}\, 59)$;

20) $42x \equiv 6 (\mathrm{mod}\, 59)$;

21) $41x \equiv 33 (\mathrm{mod}\, 79)$;

22) $17x \equiv 29 (\mathrm{mod}\, 31)$;

23) $19x \equiv 37 (\mathrm{mod}\, 61)$;

24) $16x \equiv 30 (\mathrm{mod}\, 29)$.

18. Найти частное q_k в разложении в цепную дробь дроби $\frac{a}{b}$.

1) $a = 250,\ b = 263,\ k = 4$;

2) $a = 241,\ b = 258,\ k = 5$;

3) $a = 261,\ b = 283,\ k = 3$;

4) $a = 301,\ b = 322,\ k = 3$;

5) $a = 233,\ b = 242,\ k = 3$;

6) $a = 311,\ b = 331,\ k = 5$;

7) $a = 334,\ b = 343,\ k = 3$;

8) $a = 783,\ b = 712,\ k = 2$;

9) $a = 410,\ b = 421,\ k = 4$;

10) $a = 423,\ b = 441,\ k = 3$;

11) $a = 431,\ b = 450,\ k = 5$;

12) $a = 448,\ b = 471,\ k = 4$;

13) $a = 483,\ b = 499,\ k = 4$;

14) $a = 512,\ b = 489,\ k = 4$;

15) $a = 531,\ b = 499,\ k = 5$;

16) $a = 542,\ b = 501,\ k = 5$;

17) $a = 582,\ b = 543,\ k = 3$;

18) $a = 599,\ b = 553,\ k = 2$;

19) $a = 621,\ b = 581,\ k = 4$;

20) $a = 644,\ b = 661,\ k = 5$;

21) $a = 699,\ b = 661,\ k = 3$;

22) $a = 499,\ b = 312,\ k = 3$;

23) $a = 712,\ b = 683,\ k = 4$;

24) $a = 741,\ b = 690,\ k = 4$.

19. Найти числитель третьей подходящей дроби для дроби $\frac{a}{b}$.

1) $\frac{483}{499}$;
2) $\frac{441}{423}$;
3) $\frac{258}{241}$;
4) $\frac{431}{450}$;
5) $\frac{512}{489}$;
6) $\frac{499}{531}$;
7) $\frac{501}{542}$;
8) $\frac{621}{581}$;

9) $\frac{699}{661}$; 10) $\frac{783}{712}$; 11) $\frac{233}{242}$; 12) $\frac{334}{343}$;
13) $\frac{361}{393}$; 14) $\frac{311}{331}$; 15) $\frac{241}{258}$; 16) $\frac{741}{690}$;
17) $\frac{662}{621}$; 18) $\frac{552}{599}$; 19) $\frac{421}{410}$; 20) $\frac{603}{644}$;
21) $\frac{322}{301}$; 22) $\frac{261}{283}$; 23) $\frac{250}{263}$; 24) $\frac{712}{683}$.

20. Найти несократимую обыкновенную дробь по данной цепной дроби.

1) $[0;1,30,5,3]$; 2) $[1;21,3,1,5]$;

3) $[1;15,1,1,2,6]$; 4) $[1;13,1,12]$;

5) $[1;1,12,46]$; 6) $[1;12,1,1,4]$;

7) $[1;14,1,1,9,2]$; 8) $[0;1,19,2,11]$;

9) $[1;15,6,1,5]$; 10) $[1;17,2,1,1,7]$;

11) $[1;23,1,1,4,3]$; 12) $[1;13,1,1,8]$;

13) $[1;10,35,2]$; 14) $[0;1,19,4,3]$;

15) $[0;1,19,2,11]$; 16) $[0;1,25,1,8]$;

17) $[0;1,11,1,6,3]$; 18) $[0;1,14,3]$;

19) $[0;15,1,1,4,2]$; 20) $[0;1,37,9]$;

21) $[0;1,11,3,1,1,4]$; 22) $[0;1,37,3,2,2]$;

23) $[0;1,23,2]$; 24) $[0;1,22,1,2,6]$.

21. Дробь $\frac{a}{b}$ заменить подходящей дробью с наименьшим знаменателем и погрешностью, не превосходящей числа α.

1) $\frac{599}{553}$, $\alpha = 0{,}0001$; 2) $\frac{621}{581}$, $\alpha = 0{,}001$;
3) $\frac{644}{603}$, $\alpha = 0{,}0001$; 4) $\frac{662}{621}$, $\alpha = 0{,}0001$;
5) $\frac{669}{661}$, $\alpha = 0{,}001$; 6) $\frac{712}{683}$, $\alpha = 0{,}001$;
7) $\frac{741}{690}$, $\alpha = \frac{1}{625}$; 8) $\frac{582}{543}$, $\alpha = \frac{1}{200}$;
9) $\frac{250}{263}$, $\alpha = 0{,}0001$; 10) $\frac{241}{258}$, $\alpha = \frac{1}{810}$;

11) $\frac{242}{233}$, $\alpha = \frac{1}{700}$;
12) $\frac{261}{283}$, $\alpha = \frac{1}{150}$;
13) $\frac{301}{322}$, $\alpha = 0{,}001$;
14) $\frac{311}{242}$, $\alpha = 0{,}001$;
15) $\frac{361}{399}$, $\alpha = \frac{1}{160}$;
16) $\frac{334}{343}$, $\alpha = 0{,}0001$;
17) $\frac{421}{410}$, $\alpha = 0{,}001$;
18) $\frac{441}{423}$, $\alpha = \frac{1}{700}$;
19) $\frac{431}{450}$, $\alpha = 0{,}001$;
20) $\frac{448}{471}$, $\alpha = 0{,}001$;
21) $\frac{483}{499}$, $\alpha = 0{,}0001$;
22) $\frac{512}{489}$, $\alpha = \frac{1}{500}$;
23) $\frac{531}{499}$, $\alpha = 0{,}001$;
24) $\frac{542}{501}$, $\alpha = \frac{1}{200}$.

22. Для рациональной дроби $\frac{a}{b}$, данной в десятичной системе счисления:

а) записать соответствующую q-ичную дробь;

б) найти длину периода и предпериода q-ичной дроби;

в) перевести q-ичную дробь в обыкновенную дробь в q-ичной системе счисления.

1) $\frac{15}{16}$, $q = 4$;
2) $\frac{31}{54}$, $q = 6$;
3) $\frac{37}{36}$, $q = 6$;
4) $\frac{11}{24}$, $q = 6$;
5) $\frac{43}{48}$, $q = 6$;
6) $\frac{12}{25}$, $q = 5$;
7) $\frac{73}{81}$, $q = 9$;
8) $\frac{17}{18}$, $q = 6$;
9) $\frac{33}{49}$, $q = 7$;
10) $\frac{17}{32}$, $q = 8$;
11) $\frac{28}{81}$, $q = 9$;
12) $\frac{11}{36}$, $q = 6$;
13) $\frac{11}{28}$, $q = 14$;
14) $\frac{46}{121}$, $q = 11$;
15) $\frac{7}{16}$, $q = 4$;
16) $\frac{13}{24}$, $q = 6$;
17) $\frac{25}{27}$, $q = 6$;
18) $\frac{5}{9}$, $q = 3$;
19) $\frac{21}{35}$, $q = 5$;
20) $\frac{59}{60}$, $q = 6$;
21) $\frac{57}{64}$, $q = 8$;
22) $\frac{11}{32}$, $q = 8$;
23) $\frac{11}{30}$, $q = 6$;
24) $\frac{53}{144}$, $q = 12$.

23. Записать в виде рациональной дроби данную десятичную дробь.

1)	$0,1(7)$;	2)	$0,(18)$;	3)	$0,(13)$;
4)	$0,58(3)$;	5)	$0,1(3)$;	6)	$0,0(15)$;
7)	$0,(14)$;	8)	$0,2(3)$;	9)	$0,7(3)$;
10)	$0,1(5)$;	11)	$0,3(8)$;	12)	$0,1(4)$;
13)	$0,141(6)$;	14)	$0,541(6)$;	15)	$0,(12)$;
16)	$0,1(8)$;	17)	$0,21(6)$;	18)	$0,3(4)$;
19)	$0,3(15)$;	20)	$0,(27)$;	21)	$0,(108)$;
22)	$0,(36)$;	23)	$0,(48)$;	24)	$0,18(4)$.

24. Записать в виде рациональной дроби десятичной системы счисления данную q-ичную дробь.

1)	$0,1(6)_8$;	2)	$0,1(3)_7$;	3)	$0,(24)_7$;
4)	$0,(23)_6$;	5)	$0,(251)_7$;	6)	$0,(61)_8$;
7)	$0,2(31)_5$;	8)	$0,3(6)_9$;	9)	$0,0(21)_4$;
10)	$0,0(4)_{12}$;	11)	$0,05(2)_6$;	12)	$0,5(1)_6$;
13)	$0,1(4)_7$;	14)	$0,(31)_5$;	15)	$0,1(13)_5$;
16)	$0,1(2)_7$;	17)	$0,0(13)_5$;	18)	$0,7(4)_9$;
19)	$0,(305)_7$;	20)	$0,6(52)_8$;	21)	$0,2(05)_6$;
22)	$0,2(30)_4$;	23)	$0,2(4)_9$;	24)	$0,(35)_9$.

ПРИЛОЖЕНИЕ

Таблицы индексов по простым модулям, меньшим 100

Числа	Модули																								Числа
	3	**5**	**7**	**11**	**13**	**17**	**19**	**23**	**29**	**31**	**37**	**41**	**43**	**47**	**53**	**59**	**61**	**67**	**71**	**73**	**79**	**83**	**89**	**97**	
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**
2	1	3	4	3	7	14	7	12	17	24	11	14	27	18	49	15	31	17	6	8	4	79	16	34	**2**
3		1	5	4	4	1	1	8	1	1	34	25	1	20	1	54	6	3	26	6	1	30	1	70	**3**
4		2	2	6	2	12	14	2	6	18	22	28	12	36	46	30	2	34	12	16	8	76	32	68	**4**
5			1	2	3	5	4	17	10	20	1	18	25	1	15	32	22	57	28	1	62	1	70	1	**5**
6			3	7	11	15	8	20	18	25	9	39	28	38	50	11	37	20	32	14	5	27	17	8	**6**
7				1	5	11	6	15	8	28	28	1	35	32	10	38	19	61	1	33	53	58	81	31	**7**
8				9	9	10	3	14	23	12	33	2	39	8	43	45	33	51	18	24	12	73	48	6	**8**
9				8	8	2	2	16	2	2	32	10	2	40	2	50	12	6	52	12	2	60	2	44	**9**
10				5	10	3	11	7	27	14	12	32	10	19	12	47	53	8	34	9	66	80	86	35	**10**
11					1	7	12	21	5	23	6	37	30	7	34	27	45	13	31	55	68	10	84	6	**11**
12					6	13	15	10	7	19	20	13	13	10	47	26	8	37	38	22	9	24	33	42	**12**
13						4	17	18	26	11	13	9	32	11	32	37	40	59	39	59	34	15	23	25	**13**
14						9	13	5	25	22	3	15	20	4	7	53	50	12	7	41	57	55	9	65	**14**
15						6	5	3	11	21	35	3	26	21	16	28	28	60	54	7	63	31	71	71	**15**
16						8	10	4	12	6	8	16	24	26	40	2	4	2	24	32	16	70	64	40	**16**
17							16	9	21	7	5	7	38	16	22	20	17	32	49	21	21	78	6	89	**17**
18							9	6	19	26	7	24	29	12	51	7	43	23	58	20	6	57	18	78	**18**
19								13	13	4	25	31	19	45	45	48	26	38	16	62	32	23	35	81	**19**
20								19	16	8	23	6	37	37	9	4	24	25	40	17	70	77	14	69	**20**
21								1	9	29	26	26	36	6	11	34	25	64	27	39	54	6	82	5	**21**
22								11	22	17	17	11	15	25	31	42	16	30	37	63	72	7	12	24	**22**
23									4	27	21	4	16	5	39	51	27	14	15	46	26	66	57	77	**23**
24									24	13	31	27	40	28	44	41	39	54	44	30	13	21	49	76	**24**
25									20	10	2	36	8	2	30	6	44	48	56	2	46	2	52	2	**25**
26									15	5	24	23	17	29	29	52	11	10	45	67	38	12	39	59	**26**
27									3	3	30	35	3	14	3	46	18	9	8	18	3	8	3	18	**27**
28									14	16	14	29	5	22	4	10	21	29	13	49	61	52	25	3	**28**
29										9	15	33	41	35	18	14	5	22	68	35	11	46	59	13	**29**
30										15	10	17	11	39	13	43	59	11	60	15	67	28	87	9	**30**
31											27	12	34	3	5	39	29	7	11	11	56	50	31	46	**31**
32											19	30	9	44	37	17	35	19	30	40	20	67	80	74	**32**
33											4	22	31	27	35	23	51	16	57	61	69	40	85	60	**33**
34											16	21	23	34	19	35	48	49	55	29	25	75	22	27	**34**
35											29	19	18	33	25	12	41	52	29	34	37	59	63	32	**35**
36											18	38	14	30	48	22	14	40	64	28	10	54	34	16	**36**
37												8	7	42	14	13	9	44	20	64	19	22	11	91	**37**
38												5	4	17	42	5	57	55	22	70	36	20	51	19	**38**
39												34	33	31	33	33	46	62	65	65	35	45	24	95	**39**
40												20	22	9	6	19	55	42	46	25	74	74	30	7	**40**
41													6	15	21	36	54	43	25	4	75	44	21	85	**41**
42													21	24	8	49	56	15	33	47	58	3	10	39	**42**
43														13	38	31	13	21	48	51	49	33	29	4	**43**
44														43	28	57	47	47	43	71	76	4	28	58	**44**
45														41	17	24	34	63	10	13	64	61	72	45	**45**
46														23	36	8	58	31	21	54	30	63	73	15	**46**
47															24	55	20	58	9	31	59	13	54	84	**47**
48															41	56	10	5	50	38	17	18	65	14	**48**
49															20	18	38	56	2	66	28	34	74	62	**49**

50	27	21	15	65	62	10	50	81	68	36	**50**
51	23	16	23	35	5	27	22	26	7	63	**51**
52	26	9	42	27	51	3	42	9	55	93	**52**
53		40	3	45	23	53	77	69	78	10	**53**
54		3	49	26	14	26	7	5	19	52	**54**
55		1	7	4	59	56	52	11	66	87	**55**
56		25	52	46	19	57	65	49	41	37	**56**
57		44	32	41	42	68	33	53	36	55	**57**
58		29	36	39	4	43	15	43	75	47	**58**
59			1	18	3	5	31	62	43	67	**59**
60			30	28	66	23	71	25	15	43	**60**
61				53	69	58	45	48	69	64	**61**
62				24	17	19	60	47	47	80	**62**
63				1	53	45	55	36	83	75	**63**
64				36	36	48	24	64	8	12	**64**
65				50	67	60	18	16	5	26	**65**
66				33	63	69	73	37	13	94	**66**
67					47	50	48	29	56	57	**67**
68					61	37	29	72	38	61	**68**
69					41	52	27	14	58	51	**69**
70					35	42	41	56	79	66	**70**
71						44	51	65	62	11	**71**
72						36	14	51	50	50	**72**
73							44	39	20	28	**73**
74							23	19	27	29	**74**
75							47	32	53	72	**75**
76							40	17	67	53	**76**
77							43	68	77	21	**77**
78							39	42	40	33	**78**
79								35	42	30	**79**
80								71	46	41	**80**
81								38	4	88	**81**
82								41	37	23	**82**
83									61	17	**83**
84									26	73	**84**
85									76	90	**85**
86									45	38	**86**
87									60	83	**87**
88									44	92	**88**
89										54	**89**
90										79	**90**
91										56	**91**
92										49	**92**
93										20	**93**
94										22	**94**
95										82	**95**
96										48	**96**

ЛИТЕРАТУРА

1. Бухштаб, А. А. Теория чисел / А. А. Бухштаб. – М. : Просвещение, 1966. – 384 с.
2. Грибанов, В. У. Сборник упражнений по теории чисел / В. У. Грибанов, П. И. Титов. – М. : Просвещение, 1964. – 144 с.
3. Казачек, Н. А. Алгебра и теория чисел / Н. А. Казачек, Г. Н. Перлатов, Н. Я. Виленкин, А. И. Бородин. – М. : Просвещение, 1984. – 192 с.
4. Куликов, Л. Я. Алгебра и теория чисел / Л. Я. Куликов. – М. : Высшая школа, 1979. – 560 с.
5. Лельчук, М. П. Практические занятия по алгебре и теории чисел / М. П. Лельчук, И. И. Полевченко, А. М. Радьков, Б. Д. Чеботаревский. – Мн. : Высшая школа, 1986. – 302 с.
6. Ляпин, Е. С. Алгебра и теория чисел / Е. С. Ляпин, А. Е. Евсеев. – Ч. I : Числа. – М. : Просвещение, 1974. – 383 с.
7. Просветов, Г. И. Теория чисел: задачи и решения / Г. И. Просветов. – М. : Альфа-Пресс, 2010. – 72 с.
8. Прохоров, Ю. В. Математический энциклопедический словарь / Гл. ред. Ю. В. Прохоров ; ред. кол. : С. И. Адян, Н. С. Бахвалов, В. И. Битюцков, А. П. Ершов, Л. Д. Кудрявцев, А. Л. Онищик, А. П. Юшкевич. – М. : Сов. энциклопедия, 1988. – 847 с.; ил.
9. Сзый, С. В. Лекции по теории чисел / С. В. Сизый. – М. : Физматлит, 2007. – 192 с.
10. Сушкевич, А. К. Теория чисел. Элементарный курс / А. К. Сушкевич. – М. : Вузовская книга, 2007. – 240 с.
11. Шнеперман, Л. Б. Сборник задач по алгебре и теории чисел / Л. Б. Шнеперман. – Мн. : Высшая школа, 1982. – 223 с.

Учебное издание

Ольга Александровна ГУЩИНА,
Тамара Архиповна НЕЕШПАПА

СРАВНЕНИЯ В КОЛЬЦЕ ЦЕЛЫХ ЧИСЕЛ

Учебно-методическое пособие

Верстка О. А. Надточий

Корректор М. Ф. Шатохина

Подписано в печать 23.10.2012. Бумага «Снегурочка».
Гарнитура «Times New Roman». Формат 60x84 1/8.
Тираж 500 экз. (1-й завод 1 – 100 экз.). Объем 12 усл. п. л. Заказ № 850-12.
Издательство Сахалинского государственного университета
693008, Южно-Сахалинск, ул. Ленина, 290, каб. 32.
Тел. (4242) 45-23-16. Тел./факс (4242) 45-23-17.
E-mail: izdatelstvo@sakhgu.ru, polygraph@sakhgu.sakhalin.ru