МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ»

Р.С. Адамова

ТЕОРИЯ ЧИСЕЛ

Часть 2

Учебно-методическое пособие

Воронеж
Издательский дом ВГУ
2017

§ 5. Сравнения

Рассмотрим делимость в кольце ц е л ы х чисел. Пусть $a, b \in \boldsymbol{Z}, , m \in \boldsymbol{N}$.

Определение 8 . Говорят, что a д е л и т с я на b, если существует $q \in \boldsymbol{Z}$ такое, что $a = b\,q$.

Определение 9. Н а и б о л ь ш и м о б щ и м д е л и т е л е м целых чисел $a_1, a_2, \ldots, a_k$ называется наибольший среди их общих делителей.

Определение 10. Два числа $a, b \in \boldsymbol{Z}$ называются с р а в н и м ы м и по модулю m, если $(a-b) \vdots m$. Это записывается выражением

$$a \equiv b \ (mod\ m)\ ,$$

которое называется сравнением по модулю.

Заметим, что каждое число сравнимо по модулю m с остатком от деления его на m.

Свойства сравнений по одному модулю.

$$a \equiv b\,(\mathrm{mod}\,m) \Rightarrow \begin{cases} k \cdot a \equiv k \cdot b\ (\mathrm{mod}\,m),\ k \in \boldsymbol{Z}, \\ a^n \equiv b^n\,(\mathrm{mod}\,m),\ n \in \boldsymbol{N}, \\ f(a) \equiv f(b)\ (\mathrm{mod}\,m),\ f \in \boldsymbol{Z}[x], \\ \dfrac{a}{d} \equiv \dfrac{b}{d}\ (\mathrm{mod}\,m),\ a,b \vdots d,\ (d,m)=1. \end{cases} \qquad (17)$$

$$\left.\begin{matrix} a \equiv b(\mathrm{mod}\,m) \\ c \equiv d(\mathrm{mod}\,m) \end{matrix}\right\} \Rightarrow \begin{cases} a + c \equiv b + d(\mathrm{mod}\,m) \\ a - c \equiv b - d(\mathrm{mod}\,m) \\ a \cdot c \equiv b \cdot d(\mathrm{mod}\,m) \end{cases} \qquad (18)$$

$$\left.\begin{matrix} a \equiv b(\mathrm{mod}\,m) \\ b \equiv c(\mathrm{mod}\,m) \end{matrix}\right\} \Rightarrow a \equiv c(\mathrm{mod}\,m) \qquad (19)$$

$$a \equiv b(\mathrm{mod}\,m) \Rightarrow (a,m) = (b,m) \qquad (20)$$

Доказательства этих свойств очень просты. Рассмотрим их применение.

2) $x^{p-1} \vdots d \Rightarrow x \vdots d$. Поскольку $(x+y) \vdots d$, то получаем, что и $y \vdots d$, и $x^p + y^p \vdots d$, откуда, в силу (26), $z^p \vdots d$, $z \vdots d$, и в результате имеем $(x, y, z) \vdots d$. Это невозможно согласно выбору решения (x, y, z).

Итак, получили противоречия, которые доказывают, что множители в правой части (27) действительно взаимно просты. Так как их произведение есть z^p, то эти сомножители являются p-ми степенями взаимно простых чисел, т. е.

$$\begin{cases} x+y = A^p, A \in \boldsymbol{Z}, \\ x^{p-1} - x^{p-2}y + \ldots + x \qquad y^{p-2} + y^{p-1} = R^p, R \in \boldsymbol{Z}, \\ (A, R) = 1. \end{cases} \tag{28}$$

Записав соотношение (26) в виде $x^p + (-z)^p = (-y)^p$, получим, в силу (52), что возможно представление:

$$x - z = B^p, \ B \in \boldsymbol{Z}. \tag{29}$$

Аналогично получим, что

$$y - z = C^p, \ C \in \boldsymbol{Z}. \tag{30}$$

Покажем, что для выбранного решения (x, y, z) произведение $xyz \vdots 2p+1$. Для краткости записи обозначим $2p+1$ через q. Согласно условию теоремы это число q – простое, поэтому

$$xyz \not\vdots q \Rightarrow \begin{cases} x \not\vdots q \\ y \not\vdots q \\ z \not\vdots q \end{cases} \Rightarrow \begin{cases} x^{q-1} \equiv 1 (\operatorname{mod} q) \\ y^{q-1} \equiv 1 (\operatorname{mod} q) \\ z^{q-1} \equiv 1 (\operatorname{mod} q) \end{cases} \Rightarrow \begin{cases} x^{2p} \equiv 1 (\operatorname{mod} q) \\ y^{2p} \equiv 1 (\operatorname{mod} q) \\ z^{2p} \equiv 1 (\operatorname{mod} q) \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} \left[\begin{array}{l} x^p \equiv 1 (\operatorname{mod} q) \\ x^p \equiv -1 (\operatorname{mod} q) \end{array} \right. \\ \left[\begin{array}{l} y^p \equiv 1 (\operatorname{mod} q) \\ y^p \equiv -1 (\operatorname{mod} q) \end{array} \right. \\ \left[\begin{array}{l} z^p \equiv 1 (\operatorname{mod} q) \\ z^p \equiv -1 (\operatorname{mod} q) \end{array} \right. \end{cases} \Rightarrow \begin{cases} x^p + y^p \equiv \left[\begin{array}{l} 2 \\ 0 \\ -2 \end{array} \right. (\operatorname{mod} p) \\ z^p \equiv \left[\begin{array}{l} 1 \\ -1 \end{array} \right. (\operatorname{mod} p) \end{cases} \Rightarrow x^p + y^p \neq z^p$$

Полученное противоречие с соотношением (26) говорит о том, что $xyz \vdots q$.

Следовательно, по крайней мере один из сомножителей x, y, z делится на q. Не ограничивая общности доказательства, предположим, что $z \vdots q$. Тогда

$$2z = (x+y) - (x-z) - (y-z) = A^p - B^p - C^p \Rightarrow \left(A^p - B^p - C^p\right) \vdots q.$$

Отсюда $A^p \equiv B^p + C^p \pmod q$. Применяя теорему Ферма как и выше, докажем, что $ABC \vdots q$. Но теперь мы сможем доказать, какой именно из сомножителей делится на q, это A. Действительно,

$$B \vdots q \Rightarrow B^p \vdots q \Rightarrow (x-z) \vdots q \Rightarrow x \vdots q \Rightarrow x^p \vdots q \Rightarrow y^p \vdots q \Rightarrow (x,y,z) \vdots q,$$

но по условию $(x,y,z)=1$. Следовательно, $B \not\vdots\, q$. Аналогично получим, что $C \not\vdots\, q$ и остается, что именно $A \vdots q$.

Выведем следствия из этой делимости :

$$\left.\begin{matrix} A \vdots q \\ x+y=A^p \end{matrix}\right\} \Rightarrow (x+y) \vdots q \Rightarrow x \equiv -y \pmod q \Rightarrow R^p \equiv px^{p-1} \pmod q. \qquad (31)$$

Далее, согласно (28) имеем $(A,R)=1$, поэтому

$$A \vdots q \Rightarrow (R,q)=1 \Rightarrow R^{q-1} \equiv 1 \pmod q \Rightarrow R^{2p} \equiv 1 \pmod q.$$

С другой стороны, из сравнения, полученного в (31), имеем

$$R^{2p} \equiv p^2 x^{2p-2} \pmod q \Rightarrow 1 \equiv p^2 x^{2(p-1)} \pmod q \qquad (32)$$

Покажем, что в последнем сравнении $x^{2(p-1)}$ можно заменить на 1:

$$\left.\begin{matrix} x-z=B^p \\ z \vdots q \\ B \not\vdots\, q \end{matrix}\right\} \Rightarrow \begin{cases} x \equiv B^p \pmod q \\ B^{q-1} \equiv 1 \pmod q \end{cases} \Rightarrow \begin{cases} x^{2(p-1)} \equiv B^{2p(p-1)} \pmod q \\ B^{2p} \equiv 1 \pmod q \end{cases} \Rightarrow$$

$$\Rightarrow x^{2(p-1)} \equiv 1 \pmod q$$

Выполнив в (32) соответствующую замену, получим $1 \equiv p^2 \pmod q$, но

$$1 \equiv p^2 \pmod q \Rightarrow (p^2-1) \vdots q \Rightarrow (p^2-1) \vdots (2p+1) \Rightarrow$$

$$\Rightarrow \left[\begin{matrix} (p-1) \vdots (2p+1) \\ (p+1) \vdots (2p+1) \end{matrix}\right. \Rightarrow \left[\begin{matrix} (p-1) \geq 2p+1 \\ (p+1) \geq 2p+1. \end{matrix}\right.$$

Полученное противоречие указывает на справедливость утверждения теоремы. ■

§ 6. Классы вычетов по модулю *m*

Отношение сравнимости двух чисел по модулю m является отношением эквивалентности, поэтому оно разбивает множество $\boldsymbol{Z}$ на классы эквивалентности, которые называются классами вычетов по модулю m.

Определение 12. К л а с с о м в ы ч е т о в числа a по модулю m называется совокупность всех целых чисел, сравнимых с ним по этому модулю, а каждое из этих чисел называется в ы ч е т о м числа a по этому модулю.

Класс вычетов числа a по модулю m будем обозначать $[a]_m$ или короче – $[a]$. Очевидно, этот класс состоит из чисел вида $a+km$, где $k \in \boldsymbol{Z}$.

Пример 11. $[3]_5=\{3+5k\}_{k\in Z}=\{\ldots, -7, -2, 3, 8, 13, 18, \ldots\}$.

Свойства классов вычетов по модулю m

1. $[a]=[b] \Leftrightarrow a\equiv b(\operatorname{mod} m)$ (33)

2. $\left.\begin{matrix}[a]=[b]\\ [c]=[d]\end{matrix}\right\} \Rightarrow \begin{cases}[a+c]=[b+d]\\ [a\cdot c]=[b\cdot d]\end{cases}$ (34)

Последнее свойство гарантирует корректность следующего определения операций сложения и умножения классов вычетов по модулю m:

$$\begin{matrix}[a]+[c]=[a+c]\\ [a]\cdot[c]=[a\,c]\end{matrix} \qquad (35)$$

Относительно этих операций множество всех классов вычетов по модулю m является кольцом. Это кольцо обозначается $\mathbf{Z}/m$. В нем операция умножения обладает свойством коммутативности, ассоциативности, наличия единичного элемента, которым оказывается класс [1].

Теорема 23. В кольце $\mathbf{Z}/m$ класс $[a]$ является обратимым элементом тогда и только тогда, когда $(a, m)=1$.

Доказательство. $[a]$ – обратим $\Leftrightarrow$ существует $[k]\in \mathbf{Z}/m$ такой, что $[k]\cdot[a] = 1 \Leftrightarrow$ существуют $k, l\in \mathbf{Z}$ такие, что $ka-1=lm \Leftrightarrow (a, m)=1$. ■

Следствие. Если $(a\ , m)\ =1$, то существует число $k\ \in\ Z$ такое, что $a\cdot k\equiv 1(\operatorname{mod} m)$. Это число k обладает свойством: $(\ k\ ,\ m)\equiv 1$. □

Правило построения обратного элемента в кольце Z/m

Чтобы построить обратный элемент к классу $[a]\in \mathbf{Z}/m$, нужно

- заменить a его наименьшим положительным вычетом по модулю m (т. е. остатком от деления на m);
- выполнить алгоритм Евклида последовательного деления m на этот вычет;
- по всем ***неполным*** частным этого алгоритма $q_1, q_2, \ldots, q_n$ вычислить дробь $\dfrac{P}{Q}=|q_1, q_2, \ldots, q_n|$,
- $[a]^{-1}=[k]$, где $k=(-1)^n\cdot P$.

Замечание. Построенное число k обладает свойством :

$$a\cdot k\equiv 1\ (\operatorname{mod} m)$$

Пример 12. Вычислить класс $[-11]^{-1}$ в кольце $\mathbf{Z}/8$.

1) $-11\equiv 5\,(\operatorname{mod} 8)$

2) $8=5\cdot 1+3$

$5=3\cdot 1+2$

$3=2\cdot 1+1$

$2=1\cdot 2$

3) $\dfrac{P}{Q} = |1,1,1| = \dfrac{3}{2}$

4) $[-11]^{-1} = [-3]$

Теорема 24. Кольцо $\mathbf{Z}/m$ является полем тогда и только тогда, когда m – простое число. Доказательство. Кольцо $\mathbf{Z}/m$ – поле $\Leftrightarrow$ в $\mathbf{Z}/m$ каждый класс $[a] \neq [0]$ – обратим $\Leftrightarrow$ каждое число $a \in \mathbf{Z}$, не делящееся на m, взаимно просто с ним $\Leftrightarrow$ m – простое. ■

§ 7. Полная и приведенная система вычетов по модулю *m*

Определение 13. Полной системой вычетов по модулю m называется совокупность чисел, взятых по одному из каждого класса вычетов по модулю m.

Пример 13.

Полная система наименьших неотрицательных вычетов по модулю m: $\{0, 1, 2, \dots, m-1\}$.

Полная система наименьших положительных вычетов по модулю m: $\{1, 2, \dots, m-1, m\}$.

Полная система наименьших по абсолютной величине вычетов (когда m – нечетное): $\left\{-\dfrac{m-1}{2}, -\dfrac{m-3}{2}, \dots, 0, 1, \dots, \dfrac{m-1}{2}\right\}$.

Полной системой вычетов по модулю 8 будет, например, система чисел $\{12, 3, -6, 9, 22, -11, 15, 0\}$.

Теорема 25. Всякая полная система A вычетов по модулю m является кольцом относительно операций сложения и умножения, выполняемых по этому модулю :

$$\begin{aligned} & a \oplus b = c, \text{если } c \in A \text{ и } c \equiv a + b \pmod{m} \\ & a \otimes b = d, \text{если } d \in A \text{ и } d \equiv ab \pmod{m} \end{aligned} . \qquad (36)$$

Доказательство. Взаимно однозначное соответствие между A и $\mathbf{Z}/m$, устанавливаемое по закону $a \to [a]$, переносит на A из $\mathbf{Z}/m$ операции сложения и умножения, которые в A выглядят именно так, как описано в формулах (36). ■

Следствие. Полная система вычетов по модулю m является полем относительно операций сложения и умножения, выполняемых по этому модулю, тогда и только тогда, когда m – простое число. □

Замечание. Полную систему наименьших неотрицательных вычетов по модулю m с операциями (36) будем обозначать $\mathbf{Z}_m$.

П р и м е р 14. В $Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ имеем, например, $5 \oplus 7 = 4$, $2 \otimes 5 = 2$, обратным к 5 будет 5, а элемент 4 не имеет обратного.

Из свойства сравнений (20) следует, что если один элемент в классе вычетов взаимно прост с модулем, то и любой другой элемент этого класса обладает этим же свойством. Это позволяет сделать следующее определение.

Определение 14. П р и в е д е н н о й с и с т е м о й в ы ч е т о в по модулю m называется совокупность чисел, взятых по одному из каждого класса вычетов, взаимно простых с этим модулем.

П р и м е р 15.

1. Приведенной системой вычетов по модулю 8 будет, например, совокупность чисел $\{3, 9, -11, 15\}$.

2. Если p – простое число, то приведенной системой наименьших неотрицательных вычетов будет система $\{1, 2, \ldots, p-1\}$.

Очевидно, что во всех приведенных системах вычетов по модулю m одно и то же число вычетов. Оно равно количеству чисел среди $1, 2, \ldots, m$, взаимно простых с m. Число этих чисел обозначается $\varphi(m)$. Оно определяет функцию от m на множестве натуральных чисел. Эта функция называется ф у н к ц и е й Э й л е р а.

П р и м е р 16. $\varphi(8) = 4$; $\varphi(p) = p-1$, если p – простое число.

Теорема 26. Функция Эйлера является мультипликативной.

Доказательство. Необходимо показать, что для натуральных чисел m и n при условии $(m, n) = 1$ будет справедливым соотношение

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n). \tag{37}$$

Выпишем в таблицу полную систему наименьших положительных вычетов по модулю mn:

1	2	…	k	…	m
$m+1$	$m+2$	…	$m+k$	…	$2m$
…	…	…	…	…	…
$(n-1)m+1$	$(n-1)m+2$	…	$(n-1)m+k$	…	mn

Выделим из них числа, взаимно простые с m, воспользовавшись соотношением (20): $(im+k, m) = 1 \Leftrightarrow (k, m) = 1$. Эти числа составляют столбцы, номера которых взаимно просты с m. Таких столбцов $\varphi(m)$. Каждый из этих столбцов представляет полную систему вычетов по модулю n. Действительно, в столбце n чисел и они попарно несравнимы по этому модулю потому, что

$$sm + k \equiv im + k \pmod{n} \Rightarrow sm \equiv im \pmod{n} \Rightarrow s \equiv i \pmod{n} \Rightarrow (s-i) \vdots n,$$