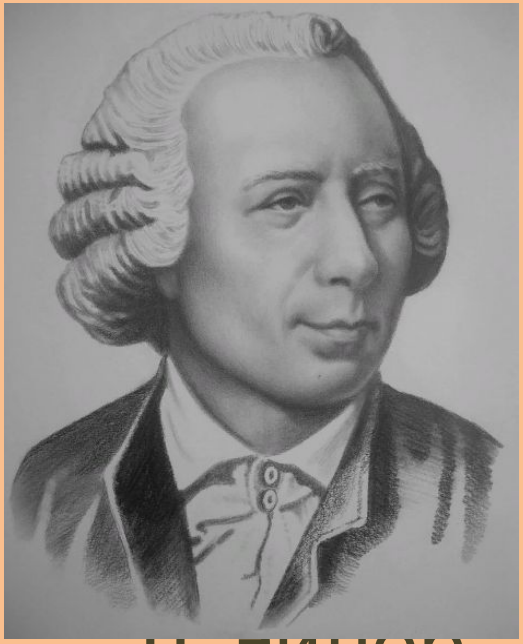
Сравнения



Л.Эйлер

П.Ферма

План

- **Сравнения: определение и свойства**

(повторение)

- **Кольцо и поле классов вычетов**
- **Теорема Эйлера. Малая теорема Ферма**

Сравнения

Определение 1. Два целых числа a и b называются *сравнимыми по модулю* m, если при делении на m они дают одинаковые остатки.

Определение 2. Два целых числа a и b называются *сравнимыми по модулю* m, если их разность делится на m.

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

Из определения 2 следует, что $a \equiv b \pmod{m} \Leftrightarrow \exists q \in Z: \ a = b + m \cdot q$.

Пример: $5 \equiv 11 \pmod{3}$, так как $5 = 3 \cdot 1 + 2$, $11 = 3 \cdot 3 + 2$, т.е. числа 5 и 11 при делении на 3 имеют одинаковый остаток 2. Можно указать бесконечно много целых чисел, сравнимых с 5 по модулю 3, например, $5 \equiv 2 \pmod{3}$, $5 \equiv 8 \pmod{3}$, $5 \equiv -1 \pmod{3}$ и т.д. Ясно, что числа, сравнимые с числом 5 по модулю 3 отличаются друг от друга на слагаемое кратное 3:

….-4,-1, 2, 5, 8, 11, 14, ….

Теорема 1. *Определения 1 и 2 равносильны.*

Доказательство.

Пусть $\begin{cases} a = m \cdot q_1 + r \\ b = m \cdot q_2 + r \end{cases}$, $0 \le r < m$, тогда $a - b = m \cdot (q_1 - q_2)$, т. е. $(a - b) \vdots m$.

Пусть теперь $\begin{cases} a = m \cdot q_1 + r_1, & 0 \le r_1 < m \\ b = m \cdot q_2 + r_2, & 0 \le r_2 < m \end{cases}$ и $(a - b) \vdots m$.

Тогда $|r_1 - r_2| < m$ и $a - b = m \cdot (q_1 - q_2) + (r_1 - r_2)$.

Так как $(a - b) \vdots m$ и $m \cdot (q_1 - q_2) \vdots m$, то и $(r_1 - r_2) \vdots m$, следовательно, $|r_1 - r_2| = 0 \Leftrightarrow r_1 = r_2$.

Теорема доказана.

Основные свойства сравнений (отношения сравнимости)

1. Сравнения по одному и тому же модулю можно почленно складывать и вычитать.

Доказательство. Пусть $a_1 \equiv b_1 (\mathrm{mod}\, m)$ и $a_2 \equiv b_2 (\mathrm{mod}\, m)$, тогда $a_1 = b_1 + m \cdot q_1$, $a_2 = b_2 + m \cdot q_2$ и $a_1 \pm a_2 = b_1 \pm b_2 + m \cdot (q_1 \pm q_2) \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 (\mathrm{mod} m)$.

2. Сравнения по одному и тому же модулю можно почленно перемножать.

Доказательство. Пусть $a_1 \equiv b_1 (\mathrm{mod}\, m)$ и $a_2 \equiv b_2 (\mathrm{mod}\, m)$, тогда $a_1 = b_1 + m \cdot q_1$, $a_2 = b_2 + m \cdot q_2$ и $a_1 a_2 = b_1 b_2 + b_1 m q_2 + m q_1 b_2 + m q_1 q_2 = b_1 b_2 + m(b_1 q_2 + q_1 b_2 + q_1 q_2) \Rightarrow a_1 a_2 \equiv b_1 b_2 (\mathrm{mod} m)$.

3. К левой, правой частям сравнения (или к обеим сразу) можно прибавлять число, кратное модулю.

Доказательство.

Пусть $a \equiv b (\mathrm{mod}\, m)$, т. е. $a - b = m \cdot q$. Покажем, что тогда $a + m \cdot t_1 \equiv b + m \cdot t_2 (\mathrm{mod}\, m)$:

$(a + m \cdot t_1) - (b + m \cdot t_2) = (a - b) + m \cdot (t_1 - t_2) = m \cdot q + m \cdot (t_1 - t_2) = m \cdot (t_1 - t_2 + q) \Leftrightarrow a + m \cdot t_1 \equiv b + m \cdot t_2 (\mathrm{mod}\, m)$

Основные свойства сравнений (отношения сравнимости)

4. Левую, правую части и модуль сравнения можно умножать на одно и то же целое число.

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

5. Левую и правую части сравнения можно умножать на одно и то же целое число.

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

6. Левую, правую части сравнения и модуль можно разделить на их НОД.

Доказательство. Пусть $a \equiv b(\mathrm{mod}\, m)$ и $(a,b,m) = d$, тогда

$$a - b = m \cdot q \Leftrightarrow \frac{a}{d} - \frac{b}{d} = \frac{m}{d} \cdot q \Leftrightarrow \frac{a}{d} \equiv \frac{b}{d}\left(\mathrm{mod}\frac{m}{d}\right).$$

7.Левую и правую части сравнения можно разделить на число, взаимно простое с модулем.

Доказательство. Пусть $a \equiv b(\mathrm{mod}\, m)$ и $a = d \cdot a_1, b = d \cdot b_1, (d,m) = 1$, тогда $a - b \vdots m$. Покажем, что $a_1 - b_1 \vdots m$: $(a-b) \vdots m \Leftrightarrow (d \cdot a_1 - d \cdot b_1) \vdots m \Leftrightarrow d \cdot (a_1 - b_1) \vdots m$. В силу $(d,m) = 1$ из последней делимости следует, что $a_1 - b_1 \vdots m$.

Делить левую и правую части неравенства на число, не взаимно простое с модулем, нельзя: $15 \equiv 3(\mathrm{mod} 3)$, но $5 \not\equiv 1(\mathrm{mod} 3)$.

II. Классы вычетов

Отношение сравнимости является отношением эквивалентности.

Определение. Пусть $a = m \cdot q + r$, где $a, q, r \in Z$, $m \in N$, тогда m называется *модулем*, а остаток r - *вычетом* (числа a) по модулю m.

Так как отношение сравнимости по модулю m, определенное на множестве целых чисел, является отношением эквивалентности, то оно разбивает множество Z на классы эквивалентности, которые называются *классами вычетов по фиксированному модулю* m. Каждый класс вычетов является множеством целых чисел, сравнимых между собой по модулю m, т. е. множеством равноостаточных целых чисел: $\bar{a} = \{b \mid b = a + m \cdot t\}$.

По теореме о делении с остатком по модулю m существует ровно m классов вычетов: $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}$

Классы вычетов не пересекаются, однозначно определяются любым своим представителем, и их объединение дает все множество целых чисел.

Системы вычетов

Определение. *Полной системой вычетов по модулю* m называется совокупность m целых чисел, содержащая ровно по одному представителю из каждого класса вычетов.

Например, $0, 1, 2, 3, 4, 5$ и $-12, 7, 14, 9, -2, 11$ - полные системы вычетов по модулю 6.

Ясно, что для каждого фиксированного модуля существует бесконечно много полных систем вычетов.

Определение. Система $0, 1, 2, 3, \ldots, m-1$ называется *системой наименьших неотрицательных вычетов по модулю* m.

Определение. Система $1, 2, 3, \ldots, m-1, m$ называется *системой наименьших положительных вычетов по модулю* m.

Определение. Система $0, \pm 1, \pm 2, \ldots, \pm\frac{m-1}{2}, \frac{m}{2}$, при четном m и $0, \pm 1, \pm 2, \ldots, \pm\frac{m-1}{2}$ при нечетном m называется *системой абсолютно наименьших вычетов по модулю* m.

Кольцо классов вычетов

Множество классов вычетов (фактор-множество) по фиксированному модулю m обозначается Z_m. В Z_m введем операции сложения и умножения классов: $\bar{a}+\bar{b}=\overline{a+b}$, $\bar{a}\cdot\bar{b}=\overline{a\cdot b}$.

Покажем корректность определения, т. е. покажем, что результат операции не зависит от выбора представителей. Пусть $a_1\in\bar{a}$, $b_1\in\bar{b}$, т. е. $a_1=a+m\cdot t_1$, $b_1=b+m\cdot t_2$. Найдем сумму классов вычетов: $\bar{a}+\bar{b}: a_1+b_1=a+m\cdot t_1+b+m\cdot t_2=a+b+m\cdot(t_1+t_2)\in\overline{a+b}$. Для произведения аналогично.

Теорема. *Множество Z_m относительно введенных операций сложения и умножения классов является коммутативным кольцом.*

Доказательство. Действительно, операции сложения и умножения классов замкнуты на Z_m по определению. Коммутативный и ассоциативный законы сложения и умножения, а также дистрибутивный закон выполняются, т. к. по существу при сложении и умножении классов мы оперируем с целыми числами.

Нейтральным элементом по сложению в Z_m является класс нуля $\bar{0}$, для произвольного $\bar{a}\in Z_m$ противоположным элементом будет класс $\overline{m-a}\in Z_m$.

Сравнение свойств кольца целых чисел и кольца классов вычетов

$<Z,+,\cdot>$	$<Z_m,+,\cdot>$
Содержит бесконечно много элементов	Содержит конечное число элементов (m)
Кольцо без делителей нуля	Если m - составное число, $m = p \cdot q$, то в кольце есть делители нуля: $\overline{p} \cdot \overline{q} = p \cdot q = m = \overline{0}$
Все элементы, кроме ± 1, необратимы	Содержит обратимые элементы, отличные от ± 1. Например, в Z_6 имеем $\overline{5} \cdot \overline{5} = \overline{25} = \overline{1}$

Приведенная система вычетов

Заметим, что если $(a, m)=1$, то $(a+m\cdot t, m)=(a, m)=1$.

Определение. Класс вычетов $\overline{a}$ по модулю m называется *взаимно простым с* m, если $(a, m)=1$.

Определение. Совокупность вычетов, взятых по одному из каждого класса, взаимно простого с модулем, называется *приведенной системой вычетов.*

Пример. Для $m=8$ приведенной системой вычетов является множество $\{1, 3, 5, 7\}$. Очевидно, что для фиксированного модуля можно составить бесконечно много приведенных систем вычетов.

Теорема. *Пусть* $\{x_1, x_2, \ldots, x_k\}$ *- приведенная система вычетов по модулю* m *и* $(a, m)=1$, *тогда* $\{a\cdot x_1, a\cdot x_2, \ldots, a\cdot x_k\}$ *- также приведенная система вычетов.*

Доказательство. 1. По условию $(a, m)=1$, следовательно, все числа $a\cdot x_i$ принадлежат приведенной системе вычетов, потому что по свойствам взаимно простых чисел. $(a\cdot x_i, m)=1$.

При этом числа $a\cdot x_i$ принадлежат различным классам. Предположим противное, т. е. среди них найдутся такие, что $a\cdot x_i \equiv a\cdot x_j (\mathrm{mod}\, m)$. Тогда по свойствам сравнений $x_i \equiv x_j (\mathrm{mod}\, m)$. Противоречие. Таким образом, система $\{a\cdot x_1, a\cdot x_2, \ldots, a\cdot x_k\}$ содержит k несравнимых между собой чисел, взаимно простых с модулем. Следовательно, она является приведенной по модулю m.

Поле классов вычетов

Теорема. *Множество классов вычетов по модулю m, взаимно простых с m, образуют мультипликативную абелеву группу.*

Доказательство. Пусть $G=\{\overline{a_1},\overline{a_2},\ldots,\overline{a_k}\}$ - множество классов вычетов по модулю m, взаимно простых с m.

1.Если $(a_i,m)=1$ и $(a_j,m)=1$, то по свойствам взаимно простых чисел $(a_i\cdot a_j,m)=1$. Следовательно, G замкнуто относительно операции умножения. При этом умножение классов вычетов ассоциативно и коммутативно.

2. Класс $\bar{1}\in G$, так как $(1,m)=1$.

3. Так как $a_1,a_2,\ldots,a_k$ - приведенная система вычетов по модулю m, то по предыдущей теореме для числа a_i, взаимно простого с m, система вычетов $a_i\cdot a_1,a_i\cdot a_2,\ldots,a_i\cdot a_k$ так же будет приведенной. Поэтому она содержит число из класса $\bar{1}$. Пусть это будет $a_i\cdot a_j$, т.е. $\overline{a_i\cdot a_j}=\bar{1}$, тогда $\overline{a_i}\cdot\overline{a_j}=a_i\cdot a_j=\overline{a_i\cdot a_j}=\bar{1}$ и классы элементов a_i и a_j являются взаимно обратными: $(\overline{a_i})^{-1}=\overline{a_j}$. Так как a_i - произвольный элемент из приведенной системы вычетов, то мы доказали обратимость всех элементов из G.

Необходимое и достаточное условие для поля классов вычетов

Теорема. *Кольцо классов вычетов по модулю m является полем тогда и только тогда, когда m - простое число.*

Доказательство.

Достаточность. Пусть $m = p$ - простое, тогда все ненулевые классы вычетов $\bar{1}, \bar{2}, \ldots, \overline{p-1}$ взаимно просты с p и по предыдущей теореме все элементы в Z_p, кроме $\bar{0}$, обратимы, следовательно, Z_p - поле.

Необходимость. Пусть Z_m - поле и m - составное, тогда $m = p \cdot q$, и в поле есть делители нуля: $\bar{p} \cdot \bar{q} = p \cdot q = m = \bar{0}$. Этого быть не может, следовательно, m - простое. Теорема доказана.

Нахождение обратных элементов с помощью подходящих дробей

Пусть $(a,m)=1$ и $\frac{m}{a}=\frac{P_n}{Q_n}$, тогда $P_n=m, Q_n=a$, так как подходящие дроби несократимы.

По свойствам подходящих дробей (см. тему Цепные дроби) имеем:

$$P_nQ_{n-1}-P_{n-1}Q_n=(-1)^{n-1} \Leftrightarrow mQ_{n-1}-aP_{n-1}=(-1)^{n-1} \Leftrightarrow aP_{n-1}=mQ_{n-1}+(-1)^n \Leftrightarrow$$

$$\Leftrightarrow (-1)^n aP_{n-1}\equiv 1(\mathrm{mod}\, m) \Leftrightarrow (-1)^n P_{n-1}\cdot a\equiv 1(\mathrm{mod}\, m)$$

Это означает, что класс $\overline{(-1)^n P_{n-1}}$ является обратным к $\bar{a}$.

Для небольших значений

$Z_5,+,\cdot>$

·	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Теорема Эйлера и малая теорема Ферма

Теорема Эйлера: $(a,m)=1 \Rightarrow a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$.

Доказательство. Пусть $\{x_1, x_2, \ldots, x_{\varphi(m)}\}$ - приведенная система вычетов по модулю m. Тогда для условия $(a,m)=1$ множество чисел $\{a \cdot x_1, a \cdot x_2, \ldots, a \cdot x_{\varphi(m)}\}$ также образует приведенную систему вычетов по модулю m.

Это означает, что $\begin{cases} ax_1 \equiv x'_1 (\mathrm{mod}\, m) \\ ax_2 \equiv x'_2 (\mathrm{mod}\, m) \\ \ldots\ldots\ldots\ldots\ldots \\ ax_{\varphi(m)} \equiv x'_{\varphi(m)} (\mathrm{mod}\, m) \end{cases}$, где $x'_i \in \{x_1, x_2, \ldots, x_{\varphi(m)}\}$.

Перемножив почленно сравнения системы, получим:

$a^{\varphi(m)}(x_1 \cdot x_2 \cdot \ldots \cdot x_{\varphi(m)}) \equiv x'_1 \cdot x'_2 \cdot \ldots \cdot x'_{\varphi(m)} (\mathrm{mod}\, m)$, но $(x_i, m)=1$ и $x_1 \cdot x_2 \cdot \ldots \cdot x_{\varphi(m)} = x'_1 \cdot x'_2 \cdot \ldots \cdot x'_{\varphi(m)}$, поэтому обе части сравнения можно сократить на этот множитель. Тогда $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$.

Следствия теоремы Эйлера

Следствием теоремы Эйлера является малая **теорема Ферма:**

Если p *- простое число и* a *– целое число, такое что* $(a, p)=1$, *то* $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.

Доказательство очевидно, т.к. $\varphi(p) = p-1$.

Следствие 2. $\forall a \in Z \quad a^p \equiv a (\mathrm{mod}\, p)$.

Доказательство. Если $(a, p)=1$, то нужное сравнение получается из сравнения

$a^{p-1} \equiv 1 (\mathrm{mod}\, p)$ умножением последнего на a. Если $a \vdots p$, то очевидно, что $a^p \equiv a (\mathrm{mod}\, p)$.

Обратные утверждения

Теорема, обратная к теореме Эйлера: $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m) \;\Rightarrow\; (a,m)=1$.

Доказательство. (Метод от противного) Пусть при условии $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$ $\mathrm{НОД}(a,m)=d>1$, тогда из сравнения $a^{\varphi(m)}-1=mc$ для некоторого целого с. В равенстве $a^{\varphi(m)}-mc=1$ левая часть кратна d, но тогда и $1 \vdots d$. Противоречие с условием $d>1$.

Однако, теорема, **обратная к малой теореме Ферма, неверна**. Формулировка обратного суждения:

Если $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$, то p - *простое число и a – целое число, такое что* $(a,p)=1$,

Например, составное число $561=3 \cdot 11 \cdot 17$ удовлетворяет сравнению $a^{560} \equiv 1 (\mathrm{mod}\, 561)$ для каждого взаимно простого с ним числа a.