Математические основы защиты информации

Онлайн-лекция 1

Пилиди Владимир Ставрович

24 марта 2020 года

Преобразованием Дирихле арифметической функции f называется арифметическая функция F, определяемая формулой

$$F(n) = \sum_{d|n} f(d), \quad n \in \mathbb{N}.$$

Ранее было доказано, что преобразование Дирихле мультипликативной функции также является мультипликативной функцией.

Преобразование Дирихле

Функция Мебиуса $\mu(n)$ определяется следующими условиями:

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если } n \text{ делится на квадрат некоторого простого числа,} \\ (-1)^k, & \text{если } n \text{ является произведением } k \text{ различных} \\ & \text{простых чисел.} \end{cases}$$

Преобразование Дирихле

Функция Мебиуса $\mu(n)$ определяется следующими условиями:

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если } n \text{ делится на квадрат некоторого простого числа,} \\ (-1)^k, & \text{если } n \text{ является произведением } k \text{ различных} \\ & \text{простых чисел.} \end{cases}$$

M — преобразование Дирихле функции Мебиуса.
Докажем, что $M = e$, где $e(1) = 1$, $e(n) = 0$ при $n > 1$.

Преобразование Дирихле

Функция Мебиуса $\mu(n)$ определяется следующими условиями:

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если } n \text{ делится на квадрат некоторого простого числа,} \\ (-1)^k, & \text{если } n \text{ является произведением } k \text{ различных} \\ & \text{простых чисел.} \end{cases}$$

M — преобразование Дирихле функции Мебиуса.
Докажем, что $M = e$, где $e(1) = 1$, $e(n) = 0$ при $n > 1$.

$$M(p^k) = \underbrace{\mu(1)}_{1} + \underbrace{\mu(p)}_{-1} + \underbrace{\mu(p^2)}_{0} + \dots + \underbrace{\mu(p^k)}_{0} = 0.$$

Преобразование Дирихле

Функция Мебиуса $\mu(n)$ определяется следующими условиями:

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если } n \text{ делится на квадрат некоторого простого числа,} \\ (-1)^k, & \text{если } n \text{ является произведением } k \text{ различных} \\ & \text{простых чисел.} \end{cases}$$

M — преобразование Дирихле функции Мебиуса.
Докажем, что $M = e$, где $e(1) = 1$, $e(n) = 0$ при $n > 1$.

$$M(p^k) = \underbrace{\mu(1)}_{1} + \underbrace{\mu(p)}_{-1} + \underbrace{\mu(p^2)}_{0} + \dots + \underbrace{\mu(p^k)}_{0} = 0.$$

$$M(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}) = \underbrace{M(p_1^{k_1})}_{0} \cdot \underbrace{M(p_2^{k_2})}_{0} \cdot \ \dots \ \cdot \underbrace{M(p_r^{k_r})}_{0} = 0,$$

Преобразование Дирихле

Функция Мебиуса $\mu(n)$ определяется следующими условиями:

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если } n \text{ делится на квадрат некоторого простого числа,} \\ (-1)^k, & \text{если } n \text{ является произведением } k \text{ различных} \\ & \text{простых чисел.} \end{cases}$$

M — преобразование Дирихле функции Мебиуса.
Докажем, что $M = e$, где $e(1) = 1$, $e(n) = 0$ при $n > 1$.

$$M(p^k) = \underbrace{\mu(1)}_{1} + \underbrace{\mu(p)}_{-1} + \underbrace{\mu(p^2)}_{0} + \dots + \underbrace{\mu(p^k)}_{0} = 0.$$

$$M(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}) = \underbrace{M(p_1^{k_1})}_{0} \cdot \underbrace{M(p_2^{k_2})}_{0} \cdot \ \dots \ \cdot \underbrace{M(p_r^{k_r})}_{0} = 0,$$

$$M(1) = 1, \quad M(n) = 0 \text{ при } n > 1, \quad M = e. \qquad \square$$

Преобразование Дирихле

Функция Эйлера $\varphi(n)$ $(n \in \mathbb{N})$ определяется как количество всех целых чисел от 1 до n включительно, взаимно простых с n.

Преобразование Дирихле

Функция Эйлера $\varphi(n)$ $(n \in \mathbb{N})$ определяется как количество всех целых чисел от 1 до n включительно, взаимно простых с n. Арифметическая функция u, $u(n) = n$, $n \geq 1$. Φ — преобразование Дирихле функции φ. Покажем, что $\Phi = u$.

Преобразование Дирихле

Функция Эйлера $\varphi(n)$ $(n \in \mathbb{N})$ определяется как количество всех целых чисел от 1 до n включительно, взаимно простых с n.
Арифметическая функция u, $u(n) = n$, $n \geq 1$. Φ — преобразование Дирихле функции φ. Покажем, что $\Phi = u$.
Проверяем для $n = p^k$.

Преобразование Дирихле

Функция Эйлера $\varphi(n)$ $(n \in \mathbb{N})$ определяется как количество всех целых чисел от 1 до n включительно, взаимно простых с n.
Арифметическая функция u, $u(n) = n$, $n \geq 1$. Φ — преобразование Дирихле функции φ. Покажем, что $\Phi = u$.
Проверяем для $n = p^k$.

$$\Phi(p^k) = \varphi(1) + \underbrace{\varphi(p)}_{p-1} + \underbrace{\varphi(p^2)}_{p^2-p} + \cdots + \underbrace{\varphi(p^k)}_{p^k-p^{k-1}} =$$

Преобразование Дирихле

Функция Эйлера $\varphi(n)$ $(n \in \mathbb{N})$ определяется как количество всех целых чисел от 1 до n включительно, взаимно простых с n.
Арифметическая функция u, $u(n) = n$, $n \geq 1$. Φ — преобразование Дирихле функции φ. Покажем, что $\Phi = u$.
Проверяем для $n = p^k$.

$$\Phi(p^k) = \varphi(1) + \underbrace{\varphi(p)}_{p-1} + \underbrace{\varphi(p^2)}_{p^2-p} + \cdots + \underbrace{\varphi(p^k)}_{p^k-p^{k-1}} =$$

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

В силу мультипликативности функций Φ и u, получаем: $\Phi = u$.

Преобразование Дирихле

$f(n) = n^s \ (s \in \mathbb{R})$.

Преобразование Дирихле

$f(n) = n^s$ $(s \in \mathbb{R})$.
Функция мультипликативная. Достаточно найти $F(p^k)$.

Преобразование Дирихле

$f(n) = n^s$ $(s \in \mathbb{R})$.
Функция мультипликативная. Достаточно найти $F(p^k)$.
Сначала рассматриваем частный случай $s = 0$, $f \equiv 1$,
$F(n) = \sum\limits_{d|n} 1$ — число делителей числа n.

Преобразование Дирихле

$f(n) = n^s$ $(s \in \mathbb{R})$.
Функция мультипликативная. Достаточно найти $F(p^k)$.
Сначала рассматриваем частный случай $s = 0$, $f \equiv 1$,
$F(n) = \sum\limits_{d|n} 1$ — число делителей числа n.

$$F(p^k) = f(1) + f(p) + f(p^2) + \cdots + f(p^k) = k + 1,$$

Преобразование Дирихле

$f(n) = n^s$ $(s \in \mathbb{R})$.
Функция мультипликативная. Достаточно найти $F(p^k)$.
Сначала рассматриваем частный случай $s = 0$, $f \equiv 1$,
$F(n) = \sum\limits_{d|n} 1$ — число делителей числа n.

$$F(p^k) = f(1) + f(p) + f(p^2) + \dots + f(p^k) = k + 1,$$

$$F(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}) = F(p_1^{k_1}) F(p_2^{k_2}) \dots F(p_r^{k_r}) =$$

Преобразование Дирихле

$f(n) = n^s$ $(s \in \mathbb{R})$.
Функция мультипликативная. Достаточно найти $F(p^k)$.
Сначала рассматриваем частный случай $s = 0$, $f \equiv 1$,
$F(n) = \sum\limits_{d|n} 1$ — число делителей числа n.

$$F(p^k) = f(1) + f(p) + f(p^2) + \dots + f(p^k) = k + 1,$$

$$F(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}) = F(p_1^{k_1}) F(p_2^{k_2}) \dots F(p_r^{k_r}) =$$

$$= (k_1 + 1)(k_2 + 1) \dots (k_r + 1).$$

Преобразование Дирихле

$f(n) = n^s$ $(s \in \mathbb{R})$.
Функция мультипликативная. Достаточно найти $F(p^k)$.
Сначала рассматриваем частный случай $s = 0$, $f \equiv 1$,
$F(n) = \sum\limits_{d|n} 1$ — число делителей числа n.

$$F(p^k) = f(1) + f(p) + f(p^2) + \cdots + f(p^k) = k + 1,$$

$$F(p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}) = F(p_1^{k_1}) F(p_2^{k_2}) \ldots F(p_r^{k_r}) =$$

$$= (k_1 + 1)(k_2 + 1) \ldots (k_r + 1).$$

Функция, равная числу делителей своего аргумента, обычно обозначается через τ или ν.

Преобразование Дирихле некоторых функций

Общий случай, $f(n) = n^s$, $s \neq 0$.

Преобразование Дирихле некоторых функций

Общий случай, $f(n) = n^s$, $s \neq 0$.

$$F(p^k) = f(1) + f(p) + f(p^2) + \cdots + f(p^k) =$$

Преобразование Дирихле некоторых функций

Общий случай, $f(n) = n^s$, $s \neq 0$.

$$F(p^k) = f(1) + f(p) + f(p^2) + \cdots + f(p^k) =$$

$$= 1 + p^s + p^{2s} + \cdots + p^{ks},$$

Преобразование Дирихле некоторых функций

Общий случай, $f(n) = n^s$, $s \neq 0$.

$$F(p^k) = f(1) + f(p) + f(p^2) + \cdots + f(p^k) =$$

$$= 1 + p^s + p^{2s} + \cdots + p^{ks},$$

$$F(p^k) = \frac{p^{(k+1)s} - 1}{p^s - 1},$$

Преобразование Дирихле некоторых функций

Общий случай, $f(n) = n^s$, $s \neq 0$.

$$F(p^k) = f(1) + f(p) + f(p^2) + \dots + f(p^k) =$$

$$= 1 + p^s + p^{2s} + \dots + p^{ks},$$

$$F(p^k) = \frac{p^{(k+1)s} - 1}{p^s - 1},$$

$$F(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}) = \tfrac{p_1^{(k_1+1)s}-1}{p_1^s-1} \cdot \ \dots \ \cdot \tfrac{p_r^{(k_r+1)s}-1}{p_r^s-1}.$$

Преобразование Дирихле некоторых функций

Общий случай, $f(n) = n^s$, $s \neq 0$.

$$F(p^k) = f(1) + f(p) + f(p^2) + \cdots + f(p^k) =$$

$$= 1 + p^s + p^{2s} + \cdots + p^{ks},$$

$$F(p^k) = \frac{p^{(k+1)s} - 1}{p^s - 1},$$

$$F(p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}) = \frac{p_1^{(k_1+1)s} - 1}{p_1^s - 1} \cdot \;\cdots\; \cdot \frac{p_r^{(k_r+1)s} - 1}{p_r^s - 1}.$$

Частный случай, $s = 1$, $F(n) = \sum\limits_{d|n} d$, это сумма всех делителей числа n. Эта функция обычно обозначается через σ.

Преобразование Дирихле некоторых функций

Общий случай, $f(n) = n^s$, $s \neq 0$.

$$F(p^k) = f(1) + f(p) + f(p^2) + \cdots + f(p^k) =$$

$$= 1 + p^s + p^{2s} + \cdots + p^{ks},$$

$$F(p^k) = \frac{p^{(k+1)s} - 1}{p^s - 1},$$

$$F(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}) = \frac{p_1^{(k_1+1)s}-1}{p_1^s-1} \cdot \ \cdots \ \cdot \frac{p_r^{(k_r+1)s}-1}{p_r^s-1}.$$

Частный случай, $s = 1$, $F(n) = \sum\limits_{d|n} d$, это сумма всех делителей числа n. Эта функция обычно обозначается через σ.

$$\sigma(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdot \ \cdots \ \cdot \frac{p_r^{k_r+1} - 1}{p_r - 1}.$$

Формула обращения Мёбиуса

Произведением Дирихле арифметических функций f и g называется арифметическая функция h, задаваемая формулой

$$h(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right), \quad n \in \mathbb{N}.$$

Формула обращения Мёбиуса

Произведением Дирихле арифметических функций f и g называется арифметическая функция h, задаваемая формулой

$$h(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right), \quad n \in \mathbb{N}.$$

Альтернативные варианты определения:

$$h(n) = \sum_{d|n} f\left(\frac{n}{d}\right) g(d), \quad n \in \mathbb{N},$$

Формула обращения Мёбиуса

Произведением Дирихле арифметических функций f и g называется арифметическая функция h, задаваемая формулой

$$h(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right), \quad n \in \mathbb{N}.$$

Альтернативные варианты определения:

$$h(n) = \sum_{d|n} f\left(\frac{n}{d}\right) g(d), \quad n \in \mathbb{N},$$

$$(f \circ g)(n) = \sum_{\substack{d_1|n,\ d_2|n, \\ d_1 d_2 = n}} f(d_1) g(d_2), \quad n \in \mathbb{N}.$$

Формула обращения Мёбиуса

Функция I: $I(n) = 1$, $n \in \mathbb{N}$.

Формула обращения Мёбиуса

Функция I: $I(n) = 1$, $n \in \mathbb{N}$.
Функция e:

$$e(n) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если } n > 1. \end{cases}$$

Формула обращения Мёбиуса

Функция I: $I(n) = 1$, $n \in \mathbb{N}$.
Функция e:

$$e(n) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если } n > 1. \end{cases}$$

$$f \circ e = e \circ f = e, \quad f \circ I = I \circ f = F.$$

Формула обращения Мёбиуса

Теорема

Пусть F — преобразование Дирихле функции f. Тогда имеет место равенство $f = F \circ \mu$.

Формула обращения Мёбиуса

Теорема

Пусть F — преобразование Дирихле функции f. Тогда имеет место равенство $f = F \circ \mu$.

$$F = f \circ I, \quad F \circ \mu = (f \circ I) \circ \mu = f \circ (I \circ \mu) = f \circ e = f. \qquad \square$$

Формула обращения Мёбиуса

Теорема

Пусть F — преобразование Дирихле функции f. Тогда имеет место равенство $f = F \circ \mu$.

$$F = f \circ I, \quad F \circ \mu = (f \circ I) \circ \mu = f \circ (I \circ \mu) = f \circ e = f. \qquad \square$$

Следствие

Если преобразование Дирихле F функции f является мультипликативной функцией, то функция f является мультипликативной.

Формула обращения Мёбиуса

Теорема

Пусть F — преобразование Дирихле функции f. Тогда имеет место равенство $f = F \circ \mu$.

$$F = f \circ I, \quad F \circ \mu = (f \circ I) \circ \mu = f \circ (I \circ \mu) = f \circ e = f. \qquad \square$$

Следствие

Если преобразование Дирихле F функции f является мультипликативной функцией, то функция f является мультипликативной.

Окончательная формулировка: арифметическая функция является мультипликативной в том и только том случае, когда мультипликативной функцией является ее преобразование Дирихле.

Сравнимость по модулю

Числа a, $b \in \mathbb{Z}$ называются сравнимыми по модулю m, если $m \mid (b - a)$. В этом случае используется запись $a \equiv b \pmod{m}$. Всегда предполагается, что $m \geq 2$.

Сравнимость по модулю

Числа a, $b \in \mathbb{Z}$ называются сравнимыми по модулю m, если $m \mid (b - a)$. В этом случае используется запись $a \equiv b \pmod{m}$.
Всегда предполагается, что $m \geq 2$.
Следующие условия являются равносильными:

Сравнимость по модулю

Числа a, $b \in \mathbb{Z}$ называются сравнимыми по модулю m, если $m \mid (b - a)$. В этом случае используется запись $a \equiv b \pmod{m}$.
Всегда предполагается, что $m \geq 2$.
Следующие условия являются равносильными:

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

Сравнимость по модулю

Числа a, $b \in \mathbb{Z}$ называются сравнимыми по модулю m, если $m \mid (b - a)$. В этом случае используется запись $a \equiv b \pmod{m}$.
Всегда предполагается, что $m \geq 2$.
Следующие условия являются равносильными:

- $a \equiv b \pmod{m}$;
- $a \bmod m = b \bmod m$;

Сравнимость по модулю

Числа a, $b \in \mathbb{Z}$ называются сравнимыми по модулю m, если $m \mid (b - a)$. В этом случае используется запись $a \equiv b \pmod{m}$.
Всегда предполагается, что $m \geq 2$.
Следующие условия являются равносильными:

- $a \equiv b \pmod{m}$;
- $a \bmod m = b \bmod m$;
- $b = a + mt$ для некоторого $t \in \mathbb{Z}$.

Сравнимость по модулю

Числа a, $b \in \mathbb{Z}$ называются сравнимыми по модулю m, если $m \mid (b - a)$. В этом случае используется запись $a \equiv b \pmod{m}$.
Всегда предполагается, что $m \geq 2$.
Следующие условия являются равносильными:

- $a \equiv b \pmod{m}$;
- $a \bmod m = b \bmod m$;
- $b = a + mt$ для некоторого $t \in \mathbb{Z}$.

$$a \equiv 0 \pmod{m} \quad \Leftrightarrow \quad m \mid a.$$

Сравнимость по модулю

Числа a, $b \in \mathbb{Z}$ называются сравнимыми по модулю m, если $m \mid (b - a)$. В этом случае используется запись $a \equiv b \pmod{m}$. Всегда предполагается, что $m \geq 2$.

Следующие условия являются равносильными:

- $a \equiv b \pmod{m}$;
- $a \bmod m = b \bmod m$;
- $b = a + mt$ для некоторого $t \in \mathbb{Z}$.

$$a \equiv 0 \pmod{m} \quad \Leftrightarrow \quad m \mid a.$$

Остатками от деления на m могут быть только числа 0, 1, ..., $m - 1$.

Сравнимость по модулю

Числа a, $b \in \mathbb{Z}$ называются сравнимыми по модулю m, если $m \mid (b - a)$. В этом случае используется запись $a \equiv b \pmod{m}$.
Всегда предполагается, что $m \geq 2$.
Следующие условия являются равносильными:

- $a \equiv b \pmod{m}$;
- $a \bmod m = b \bmod m$;
- $b = a + mt$ для некоторого $t \in \mathbb{Z}$.

$$a \equiv 0 \pmod{m} \quad \Leftrightarrow \quad m \mid a.$$

Остатками от деления на m могут быть только числа 0, 1, ..., $m - 1$.
Каждое целое число сравнимо с одним и только одним из этих чисел.

Сравнимость по модулю

Определение

Множество называется полной системой вычетов по модулю m, если каждое целое число сравнимо по этому модулю с одним и только одним числом из этого множества.

Определение

Множество называется полной системой вычетов по модулю m, если каждое целое число сравнимо по этому модулю с одним и только одним числом из этого множества.

- Числа $0, 1, \ldots, m-1$ образуют полную систему вычетов по модулю m;

Сравнимость по модулю

Определение

Множество называется полной системой вычетов по модулю m, если каждое целое число сравнимо по этому модулю с одним и только одним числом из этого множества.

- Числа $0, 1, \ldots, m-1$ образуют полную систему вычетов по модулю m;
- Любой набор из m чисел, попарно несравнимых по модулю m, является полной системой вычетов.

Сравнимость по модулю

Определение

Множество называется полной системой вычетов по модулю m, если каждое целое число сравнимо по этому модулю с одним и только одним числом из этого множества.

- Числа $0, 1, \ldots, m-1$ образуют полную систему вычетов по модулю m;
- Любой набор из m чисел, попарно несравнимых по модулю m, является полной системой вычетов.
- Любые m последовательных целых чисел образуют полную систему вычетов.

Сравнимость по модулю

Отношение сравнимость является отношением эквивалентности.

Сравнимость по модулю

Отношение сравнимость является отношением эквивалентности.

- Рефлексивность $a \equiv a \pmod{m}$.

Сравнимость по модулю

Отношение сравнимость является отношением эквивалентности.

- Рефлексивность $a \equiv a \pmod{m}$.
- Симметричность Если $a \equiv b \pmod{m}$, то $b \equiv a \pmod{m}$.

Сравнимость по модулю

Отношение сравнимость является отношением эквивалентности.

- Рефлексивность $a \equiv a \pmod{m}$.
- Симметричность Если $a \equiv b \pmod{m}$, то $b \equiv a \pmod{m}$.
- Транзитивность Если $a \equiv b \pmod{m}$ и $b \equiv c \pmod{m}$, то $a \equiv c \pmod{m}$.

Сравнимость по модулю

Отношение сравнимость является отношением эквивалентности.

- Рефлексивность $a \equiv a \pmod{m}$.
- Симметричность Если $a \equiv b \pmod{m}$, то $b \equiv a \pmod{m}$.
- Транзитивность Если $a \equiv b \pmod{m}$ и $b \equiv c \pmod{m}$, то $a \equiv c \pmod{m}$.

Множество $\mathbb{Z}$ может быть представлено в виде объединения попарно непересекающихся классов эквивалентности, таких множеств, что:

Сравнимость по модулю

Отношение сравнимость является отношением эквивалентности.

- Рефлексивность $a \equiv a \pmod{m}$.
- Симметричность Если $a \equiv b \pmod{m}$, то $b \equiv a \pmod{m}$.
- Транзитивность Если $a \equiv b \pmod{m}$ и $b \equiv c \pmod{m}$, то $a \equiv c \pmod{m}$.

Множество $\mathbb{Z}$ может быть представлено в виде объединения попарно непересекающихся классов эквивалентности, таких множеств, что:

- любые два числа, принадлежащие одному множеству, сравнимы по модулю m;

Сравнимость по модулю

Отношение сравнимость является отношением эквивалентности.

- Рефлексивность $a \equiv a \pmod{m}$.
- Симметричность Если $a \equiv b \pmod{m}$, то $b \equiv a \pmod{m}$.
- Транзитивность Если $a \equiv b \pmod{m}$ и $b \equiv c \pmod{m}$, то $a \equiv c \pmod{m}$.

Множество $\mathbb{Z}$ может быть представлено в виде объединения попарно непересекающихся классов эквивалентности, таких множеств, что:

- любые два числа, принадлежащие одному множеству, сравнимы по модулю m;
- любые два числа, сравнимые по модулю m, принадлежат одному множеству.

Сравнимость по модулю

Свойство

Если $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, то $a \pm c \equiv b \pm d \pmod{m}$.

Сравнимость по модулю

Свойство

Если $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, то $a \pm c \equiv b \pm d \pmod{m}$.

Свойство

Если $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, то $ac \equiv bd \pmod{m}$.

Сравнимость по модулю

Свойство

Если $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, то $a \pm c \equiv b \pm d \pmod{m}$.

Свойство

Если $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, то $ac \equiv bd \pmod{m}$.

$$b = a + mt, \quad d = c + m\tau, \quad t, \tau \in \mathbb{Z},$$

Сравнимость по модулю

Свойство

Если $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, то $a \pm c \equiv b \pm d \pmod{m}$.

Свойство

Если $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, то $ac \equiv bd \pmod{m}$.

$$b = a + mt, \quad d = c + m\tau, \quad t, \tau \in \mathbb{Z},$$

$$bd = (a + mt)(c + m\tau) = ac + m(tc + a\tau + mt\tau),$$

Сравнимость по модулю

Свойство

Если $a \equiv b \pmod m$ и $c \equiv d \pmod m$, то $a \pm c \equiv b \pm d \pmod m$.

Свойство

Если $a \equiv b \pmod m$ и $c \equiv d \pmod m$, то $ac \equiv bd \pmod m$.

$$b = a + mt, \quad d = c + m\tau, \quad t, \tau \in \mathbb{Z},$$

$$bd = (a + mt)(c + m\tau) = ac + m(tc + a\tau + mt\tau),$$

$$ac \equiv bd (\bmod m).$$

□

Сравнимость по модулю

Свойство

Если $a \equiv b \pmod{m}$, то для любого $k \in \mathbb{N}$ имеет место сравнение $ka \equiv kb \pmod{km}$.

Сравнимость по модулю

Свойство

Если $a \equiv b \pmod{m}$, то для любого $k \in \mathbb{N}$ имеет место сравнение $ka \equiv kb \pmod{km}$.

$$b = a + mt \quad \Rightarrow \quad kb = ka + kmt. \qquad \square$$

Сравнимость по модулю

Свойство

Если $a \equiv b \pmod{m}$, то для любого $k \in \mathbb{N}$ имеет место сравнение $ka \equiv kb \pmod{km}$.

$$b = a + mt \quad \Rightarrow \quad kb = ka + kmt. \qquad \square$$

Свойство

Если $d|a$, $d|b$, $d|m$, то соотношения $a \equiv b \pmod{m}$ и $a/d \equiv b/d \pmod{m/d}$ равносильны.

Сравнимость по модулю

Свойство

Если $a \equiv b \pmod{m}$, то для любого $k \in \mathbb{N}$ имеет место сравнение $ka \equiv kb \pmod{km}$.

$$b = a + mt \quad \Rightarrow \quad kb = ka + kmt. \qquad \square$$

Свойство

Если $d|a$, $d|b$, $d|m$, то соотношения $a \equiv b \pmod{m}$ и $a/d \equiv b/d \pmod{m/d}$ равносильны.

$$b = a + mt \quad \Leftrightarrow \quad \frac{b}{d} = \frac{a}{d} + \frac{m}{d}t. \qquad \square$$

Сравнимость по модулю

Свойство

Если $ca \equiv cb \pmod{m}$, c и m взаимно простые, то $a \equiv b \pmod{m}$.

Сравнимость по модулю

Свойство

Если $ca \equiv cb \pmod{m}$, c и m взаимно простые, то $a \equiv b \pmod{m}$.

$$ca \equiv cb \pmod{m} \Rightarrow m \mid c(b-a) \Rightarrow m \mid (b-a) \Rightarrow a \equiv b \pmod{m}. \quad \square$$

Сравнимость по модулю

Свойство

Если $ca \equiv cb \pmod{m}$, c и m взаимно простые, то $a \equiv b \pmod{m}$.

$$ca \equiv cb \pmod{m} \Rightarrow m \mid c(b-a) \Rightarrow m \mid (b-a) \Rightarrow a \equiv b \pmod{m}. \quad \square$$

Свойство

Если $a \equiv b \pmod{m}$, то $a^n \equiv b^n \pmod{m}$ для любого $n \in \mathbb{N}$.

Сравнимость по модулю

Свойство

Если $ca \equiv cb \pmod{m}$, c и m взаимно простые, то $a \equiv b \pmod{m}$.

$$ca \equiv cb \pmod{m} \Rightarrow m \mid c(b-a) \Rightarrow m \mid (b-a) \Rightarrow a \equiv b \pmod{m}. \qquad \square$$

Свойство

Если $a \equiv b \pmod{m}$, то $a^n \equiv b^n \pmod{m}$ для любого $n \in \mathbb{N}$.

Свойство

Если f — многочлен с целыми коэффициентами и $a \equiv b \pmod{m}$, то $f(a) \equiv f(b) \pmod{m}$.

Сравнимость по модулю

Свойство

Если $a \equiv b \pmod{m}$ и $d \mid m$, то $a \equiv b \pmod{d}$.

Сравнимость по модулю

Свойство

Если $a \equiv b \pmod{m}$ и $d \mid m$, то $a \equiv b \pmod{d}$.

$$a \equiv b \pmod{m} \;\Rightarrow\; m|(b-a) \;\Rightarrow\; d \mid (b-a) \;\Rightarrow\; a \equiv b \pmod{d}. \quad \square$$

Свойство

Если $a \equiv b \pmod{m}$ и $d \mid m$, то $a \equiv b \pmod{d}$.

$$a \equiv b \pmod{m} \;\Rightarrow\; m|(b-a) \;\Rightarrow\; d \mid (b-a) \;\Rightarrow\; a \equiv b \pmod{d}. \quad \square$$

Свойство

Если $a \equiv b \pmod{m_1}$ и $a \equiv b \pmod{m_2}$, то $a \equiv b \pmod{[m_1, m_2]}$.

Сравнимость по модулю

Свойство

Если $a \equiv b \pmod{m}$ и $d \mid m$, то $a \equiv b \pmod{d}$.

$$a \equiv b \pmod{m} \;\Rightarrow\; m|(b-a) \;\Rightarrow\; d \mid (b-a) \;\Rightarrow\; a \equiv b \pmod{d}. \quad \square$$

Свойство

Если $a \equiv b \pmod{m_1}$ и $a \equiv b \pmod{m_2}$, то $a \equiv b \pmod{[m_1, m_2]}$.

Обозначим $m = m_1 m_2$. Утверждение вытекает из следующей эквивалентности:

Сравнимость по модулю

Свойство

Если $a \equiv b \pmod{m}$ и $d \mid m$, то $a \equiv b \pmod{d}$.

$$a \equiv b \pmod{m} \;\Rightarrow\; m|(b-a) \;\Rightarrow\; d \mid (b-a) \;\Rightarrow\; a \equiv b \pmod{d}. \quad \square$$

Свойство

Если $a \equiv b \pmod{m_1}$ и $a \equiv b \pmod{m_2}$, то $a \equiv b \pmod{[m_1, m_2]}$.

Обозначим $m = m_1 m_2$. Утверждение вытекает из следующей эквивалентности:

$$m|(b-a) \Leftrightarrow (m_1|(b-a) \text{ и } m_2|(b-a)).$$

Сравнимость по модулю

Свойство

Если одна часть сравнения $a \equiv b \pmod{m}$ и модуль m делятся на некоторое число, то и другая часть сравнения делится на это число.

Сравнимость по модулю

Свойство

Если одна часть сравнения $a \equiv b \pmod{m}$ и модуль m делятся на некоторое число, то и другая часть сравнения делится на это число.

$$b = a + mt, \quad d \mid a, \ \ d \mid m \quad \Rightarrow \quad d \mid b. \qquad \square$$

Сравнимость по модулю

Свойство

Если одна часть сравнения $a \equiv b \pmod{m}$ и модуль m делятся на некоторое число, то и другая часть сравнения делится на это число.

$$b = a + mt, \quad d \mid a, \quad d \mid m \quad \Rightarrow \quad d \mid b. \qquad \square$$

Следствие

$$\mathcal{D}(a, m) = \mathcal{D}(b, m), \qquad (a, m) = (b, m).$$

Сравнимость по модулю

Свойство

Если одна часть сравнения $a \equiv b \pmod{m}$ и модуль m делятся на некоторое число, то и другая часть сравнения делится на это число.

$$b = a + mt, \quad d \mid a, \;\; d \mid m \quad \Rightarrow \quad d \mid b. \qquad \square$$

Следствие

$$\mathcal{D}(a, m) = \mathcal{D}(b, m), \qquad (a, m) = (b, m).$$

Следствие

Для любого фиксированного класса X чисел по модулю m величина (x, m), $x \in X$ является постоянной. В частности, все числа из любого класса взаимно просты с m или нет.

Сравнимость по модулю

Рассмотрим все классы, элементы которых взаимно простые с m. Выберем из каждого такого класса по одному элементу. Получаемая система чисел называется приведенной системой вычетов по модулю m.

Сравнимость по модулю

Рассмотрим все классы, элементы которых взаимно простые с m. Выберем из каждого такого класса по одному элементу. Получаемая система чисел называется приведенной системой вычетов по модулю m.

Алгоритм построения приведенной системы вычетов.

Рассматриваем полную систему вычетов и удаляем из нее все числа, не взаимно простые с m.

Рассмотрим все классы, элементы которых взаимно простые с m.
Выберем из каждого такого класса по одному элементу.
Получаемая система чисел называется приведенной системой вычетов по модулю m.
Алгоритм построения приведенной системы вычетов.
Рассматриваем полную систему вычетов и удаляем из нее все числа, не взаимно простые с m.

$$m = 18$$

Рассмотрим все классы, элементы которых взаимно простые с m. Выберем из каждого такого класса по одному элементу. Получаемая система чисел называется приведенной системой вычетов по модулю m.

Алгоритм построения приведенной системы вычетов.

Рассматриваем полную систему вычетов и удаляем из нее все числа, не взаимно простые с m.

$$m = 18$$

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17$$

Сравнимость по модулю

Рассмотрим все классы, элементы которых взаимно простые с m.
Выберем из каждого такого класса по одному элементу.
Получаемая система чисел называется приведенной системой вычетов по модулю m.
Алгоритм построения приведенной системы вычетов.
Рассматриваем полную систему вычетов и удаляем из нее все числа, не взаимно простые с m.

$$m = 18$$

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17$$

$$0, \textcolor{red}{1}, 2, 3, 4, \textcolor{red}{5}, 6, \textcolor{red}{7}, 8, 9, 10, \textcolor{red}{11}, 12, \textcolor{red}{13}, 14, 15, 16, \textcolor{red}{17}$$

Сравнимость по модулю

Рассмотрим все классы, элементы которых взаимно простые с m. Выберем из каждого такого класса по одному элементу. Получаемая система чисел называется приведенной системой вычетов по модулю m.

Алгоритм построения приведенной системы вычетов.

Рассматриваем полную систему вычетов и удаляем из нее все числа, не взаимно простые с m.

$$m = 18$$

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17$$

$$0, \color{red}{1}, 2, 3, 4, \color{red}{5}, 6, \color{red}{7}, 8, 9, 10, \color{red}{11}, 12, \color{red}{13}, 14, 15, 16, \color{red}{17}$$

Приведенную систему вычетов образуют 1, 5, 7, 11, 13, 17.

Сравнимость по модулю

В случае произвольного модуля m берем полную систему вычетов от 0 до $m-1$ и выделяем из нее приведенную систему, она состоит из $\varphi(m)$ элементов.

Сравнимость по модулю

В случае произвольного модуля m берем полную систему вычетов от 0 до $m-1$ и выделяем из нее приведенную систему, она состоит из $\varphi(m)$ элементов.

Свойство

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

Сравнимость по модулю

Теорема

Предположим, что числа x_1, x_2, $\ldots$, x_k попарно не сравнимы по модулю m, a, $b \in \mathbb{Z}$ и $(a, m) = 1$. Тогда числа $ax_1 + b$, $ax_2 + b$, $\ldots$, $ax_k + b$ попарно не сравнимы по модулю m.

Сравнимость по модулю

Теорема

Предположим, что числа x_1, x_2, ..., x_k попарно не сравнимы по модулю m, a, $b \in \mathbb{Z}$ и $(a, m) = 1$. Тогда числа $ax_1 + b$, $ax_2 + b$, ..., $ax_k + b$ попарно не сравнимы по модулю m.

Предположим, что

$$ax_i + b \equiv ax_j + b \pmod{m}, \quad 1 \leq i, j \leq k.$$

Теорема

Предположим, что числа x_1, x_2, $\ldots$, x_k попарно не сравнимы по модулю m, a, $b \in \mathbb{Z}$ и $(a, m) = 1$. Тогда числа $ax_1 + b$, $ax_2 + b$, $\ldots$, $ax_k + b$ попарно не сравнимы по модулю m.

Предположим, что

$$ax_i + b \equiv ax_j + b \pmod{m}, \quad 1 \leq i, j \leq k.$$

$$(ax_i + b) - (ax_j + b) = a(x_i - x_j).$$

Сравнимость по модулю

Теорема

Предположим, что числа x_1, x_2, …, x_k попарно не сравнимы по модулю m, a, $b \in \mathbb{Z}$ и $(a, m) = 1$. Тогда числа $ax_1 + b$, $ax_2 + b$, …, $ax_k + b$ попарно не сравнимы по модулю m.

Предположим, что

$$ax_i + b \equiv ax_j + b \pmod{m}, \quad 1 \leq i, j \leq k.$$

$$(ax_i + b) - (ax_j + b) = a(x_i - x_j).$$

$m \mid a(x_i - x_j)$

Сравнимость по модулю

Теорема

Предположим, что числа x_1, x_2, $\ldots$, x_k попарно не сравнимы по модулю m, a, $b \in \mathbb{Z}$ и $(a, m) = 1$. Тогда числа $ax_1 + b$, $ax_2 + b$, $\ldots$, $ax_k + b$ попарно не сравнимы по модулю m.

Предположим, что

$$ax_i + b \equiv ax_j + b \pmod{m}, \quad 1 \le i, j \le k.$$

$$(ax_i + b) - (ax_j + b) = a(x_i - x_j).$$

$$m \mid a(x_i - x_j), \quad (m, a) = 1$$

Сравнимость по модулю

Теорема

Предположим, что числа x_1, x_2, $\dots$, x_k попарно не сравнимы по модулю m, a, $b \in \mathbb{Z}$ и $(a, m) = 1$. Тогда числа $ax_1 + b$, $ax_2 + b$, $\dots$, $ax_k + b$ попарно не сравнимы по модулю m.

Предположим, что

$$ax_i + b \equiv ax_j + b \pmod{m}, \quad 1 \le i, j \le k.$$

$$(ax_i + b) - (ax_j + b) = a(x_i - x_j).$$

$$m \mid a(x_i - x_j), \quad (m, a) = 1 \quad \Rightarrow \quad m \mid (x_i - x_j),$$

Сравнимость по модулю

Теорема

Предположим, что числа x_1, x_2, $\dots$, x_k попарно не сравнимы по модулю m, a, $b \in \mathbb{Z}$ и $(a, m) = 1$. Тогда числа $ax_1 + b$, $ax_2 + b$, $\dots$, $ax_k + b$ попарно не сравнимы по модулю m.

Предположим, что

$$ax_i + b \equiv ax_j + b \pmod{m}, \quad 1 \le i, j \le k.$$

$$(ax_i + b) - (ax_j + b) = a(x_i - x_j).$$

$$m \mid a(x_i - x_j), \quad (m, a) = 1 \quad \Rightarrow \quad m \mid (x_i - x_j),$$

$$x_i \equiv x_j \pmod{m} \quad \Rightarrow \quad i = j. \qquad \square$$

Сравнимость по модулю

Теорема

Пусть a, $b \in \mathbb{Z}$ и $(a, m) = 1$. Если числа x пробегают полную систему вычетов по модулю m, то числа $ax + b$ также пробегают полную систему вычетов по этому модулю. Если числа x пробегают приведенную систему вычетов по модулю m, то числа ax также пробегают приведенную систему вычетов по этому модулю.

Сравнимость по модулю

Теорема

Пусть a, $b \in \mathbb{Z}$ и $(a, m) = 1$. Если числа x пробегают полную систему вычетов по модулю m, то числа $ax + b$ также пробегают полную систему вычетов по этому модулю. Если числа x пробегают приведенную систему вычетов по модулю m, то числа ax также пробегают приведенную систему вычетов по этому модулю.

1) Числа x пробегают полную систему вычетов.

Сравнимость по модулю

Теорема

Пусть a, $b \in \mathbb{Z}$ и $(a, m) = 1$. Если числа x пробегают полную систему вычетов по модулю m, то числа $ax + b$ также пробегают полную систему вычетов по этому модулю. Если числа x пробегают приведенную систему вычетов по модулю m, то числа ax также пробегают приведенную систему вычетов по этому модулю.

1) Числа x пробегают полную систему вычетов.
Числа $ax + b$ попарно не сравнимы по модулю m,

Сравнимость по модулю

Теорема

Пусть a, $b \in \mathbb{Z}$ и $(a, m) = 1$. Если числа x пробегают полную систему вычетов по модулю m, то числа $ax + b$ также пробегают полную систему вычетов по этому модулю. Если числа x пробегают приведенную систему вычетов по модулю m, то числа ax также пробегают приведенную систему вычетов по этому модулю.

1) Числа x пробегают полную систему вычетов.
Числа $ax + b$ попарно не сравнимы по модулю m, их количество равно m.

Сравнимость по модулю

Теорема

Пусть a, $b \in \mathbb{Z}$ и $(a, m) = 1$. Если числа x пробегают полную систему вычетов по модулю m, то числа $ax + b$ также пробегают полную систему вычетов по этому модулю. Если числа x пробегают приведенную систему вычетов по модулю m, то числа ax также пробегают приведенную систему вычетов по этому модулю.

1) Числа x пробегают полную систему вычетов.
Числа $ax + b$ попарно не сравнимы по модулю m, их количество равно m.
Значит эти числа образуют полную систему вычетов.

Сравнимость по модулю

Теорема

Пусть a, $b \in \mathbb{Z}$ и $(a, m) = 1$. Если числа x пробегают полную систему вычетов по модулю m, то числа $ax + b$ также пробегают полную систему вычетов по этому модулю. Если числа x пробегают приведенную систему вычетов по модулю m, то числа ax также пробегают приведенную систему вычетов по этому модулю.

1) Числа x пробегают полную систему вычетов.
Числа $ax + b$ попарно не сравнимы по модулю m, их количество равно m.
Значит эти числа образуют полную систему вычетов.
2) Числа x пробегают приведенную систему вычетов.

Сравнимость по модулю

Теорема

Пусть a, $b \in \mathbb{Z}$ и $(a, m) = 1$. Если числа x пробегают полную систему вычетов по модулю m, то числа $ax + b$ также пробегают полную систему вычетов по этому модулю. Если числа x пробегают приведенную систему вычетов по модулю m, то числа ax также пробегают приведенную систему вычетов по этому модулю.

1) Числа x пробегают полную систему вычетов.
Числа $ax + b$ попарно не сравнимы по модулю m, их количество равно m.
Значит эти числа образуют полную систему вычетов.
2) Числа x пробегают приведенную систему вычетов.
Количество чисел ax равно $\varphi(m)$,

Сравнимость по модулю

Теорема

Пусть a, $b \in \mathbb{Z}$ и $(a, m) = 1$. Если числа x пробегают полную систему вычетов по модулю m, то числа $ax + b$ также пробегают полную систему вычетов по этому модулю. Если числа x пробегают приведенную систему вычетов по модулю m, то числа ax также пробегают приведенную систему вычетов по этому модулю.

1) Числа x пробегают полную систему вычетов.
Числа $ax + b$ попарно не сравнимы по модулю m, их количество равно m.
Значит эти числа образуют полную систему вычетов.
2) Числа x пробегают приведенную систему вычетов.
Количество чисел ax равно $\varphi(m)$, они попарно не сравнимы по модулю m, $(ax, m) = 1$.

Сравнимость по модулю

Теорема

Пусть a, $b \in \mathbb{Z}$ и $(a, m) = 1$. Если числа x пробегают полную систему вычетов по модулю m, то числа $ax + b$ также пробегают полную систему вычетов по этому модулю. Если числа x пробегают приведенную систему вычетов по модулю m, то числа ax также пробегают приведенную систему вычетов по этому модулю.

1) Числа x пробегают полную систему вычетов.
Числа $ax + b$ попарно не сравнимы по модулю m, их количество равно m.
Значит эти числа образуют полную систему вычетов.
2) Числа x пробегают приведенную систему вычетов.
Количество чисел ax равно $\varphi(m)$, они попарно не сравнимы по модулю m, $(ax, m) = 1$.
Значит эти числа образуют приведенную систему вычетов.

Сравнимость по модулю

Теорема (Эйлера)

Предположим, что $m \geqslant 2$ и числа a, m взаимно простые. Тогда $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Сравнимость по модулю

Теорема (Эйлера)

Предположим, что $m \geqslant 2$ и числа a, m взаимно простые. Тогда $a^{\varphi(m)} \equiv 1 \pmod{m}$.

$\varphi(m) = k$

Сравнимость по модулю

Теорема (Эйлера)

Предположим, что $m \geqslant 2$ и числа a, m взаимно простые. Тогда $a^{\varphi(m)} \equiv 1 \pmod m$.

$\varphi(m) = k$

$x_1, x_2, \ldots, x_k$ — приведенная система вычетов m.

Сравнимость по модулю

Теорема (Эйлера)

Предположим, что $m \geqslant 2$ и числа a, m взаимно простые. Тогда $a^{\varphi(m)} \equiv 1 \pmod{m}$.

$\varphi(m) = k$

$x_1, x_2, \ldots, x_k$ — приведенная система вычетов m.

$ax_1, ax_2, \ldots, ax_k$ образуют приведенную систему вычетов

Сравнимость по модулю

Теорема (Эйлера)

Предположим, что $m \geqslant 2$ и числа a, m взаимно простые. Тогда $a^{\varphi(m)} \equiv 1 \pmod{m}$.

$\varphi(m) = k$

$x_1, x_2, \ldots, x_k$ — приведенная система вычетов m.

$ax_1, ax_2, \ldots, ax_k$ образуют приведенную систему вычетов

Каждое из чисел $ax_1, ax_2, \ldots, ax_k$ сравнимо по модулю m с одним и только одним из чисел $x_1, x_2, \ldots, x_k$.

Сравнимость по модулю

Теорема (Эйлера)

Предположим, что $m \geqslant 2$ и числа a, m взаимно простые. Тогда $a^{\varphi(m)} \equiv 1 \pmod{m}$.

$\varphi(m) = k$

x_1, x_2, ..., x_k — приведенная система вычетов m.

ax_1, ax_2, ..., ax_k образуют приведенную систему вычетов

Каждое из чисел ax_1, ax_2, ..., ax_k сравнимо по модулю m с одним и только одним из чисел x_1, x_2, ..., x_k.

$$ax_1 \equiv x_{i_1} \pmod{m}, \quad ax_2 \equiv x_{i_2} \pmod{m}, \ldots, ax_k \equiv x_{i_k} \pmod{m},$$

Сравнимость по модулю

Теорема (Эйлера)

Предположим, что $m \geqslant 2$ и числа a, m взаимно простые. Тогда $a^{\varphi(m)} \equiv 1 \pmod{m}$.

$\varphi(m) = k$

$x_1, x_2, \ldots, x_k$ — приведенная система вычетов m.

$ax_1, ax_2, \ldots, ax_k$ образуют приведенную систему вычетов

Каждое из чисел $ax_1, ax_2, \ldots, ax_k$ сравнимо по модулю m с одним и только одним из чисел $x_1, x_2, \ldots, x_k$.

$$ax_1 \equiv x_{i_1} \pmod{m}, \quad ax_2 \equiv x_{i_2} \pmod{m}, \ldots, ax_k \equiv x_{i_k} \pmod{m},$$

$$a^k x_1 x_2 \ldots x_k \equiv x_{i_1} x_{i_2} \ldots x_{i_k} \pmod{m},$$

Сравнимость по модулю

Теорема (Эйлера)

Предположим, что $m \geqslant 2$ и числа a, m взаимно простые. Тогда $a^{\varphi(m)} \equiv 1 \pmod m$.

$\varphi(m) = k$

x_1, x_2, …, x_k — приведенная система вычетов m.

ax_1, ax_2, …, ax_k образуют приведенную систему вычетов

Каждое из чисел ax_1, ax_2, …, ax_k сравнимо по модулю m с одним и только одним из чисел x_1, x_2, …, x_k.

$$ax_1 \equiv x_{i_1} \pmod m, \quad ax_2 \equiv x_{i_2} \pmod m, \dots, ax_k \equiv x_{i_k} \pmod m,$$

$$a^k x_1 x_2 \dots x_k \equiv x_{i_1} x_{i_2} \dots x_{i_k} \pmod m,$$

$$x_{i_1} x_{i_2} \dots x_{i_k} = x_1 x_2 \dots x_k, \quad (x_1 x_2 \dots x_k, m) = 1,$$

Сравнимость по модулю

Теорема (Эйлера)

Предположим, что $m \geqslant 2$ и числа a, m взаимно простые. Тогда $a^{\varphi(m)} \equiv 1 \pmod{m}$.

$\varphi(m) = k$
$x_1, x_2, \ldots, x_k$ — приведенная система вычетов m.
$ax_1, ax_2, \ldots, ax_k$ образуют приведенную систему вычетов
Каждое из чисел $ax_1, ax_2, \ldots, ax_k$ сравнимо по модулю m с одним и только одним из чисел $x_1, x_2, \ldots, x_k$.

$$ax_1 \equiv x_{i_1} \pmod{m}, \quad ax_2 \equiv x_{i_2} \pmod{m}, \ldots, ax_k \equiv x_{i_k} \pmod{m},$$

$$a^k x_1 x_2 \ldots x_k \equiv x_{i_1} x_{i_2} \ldots x_{i_k} \pmod{m},$$

$$x_{i_1} x_{i_2} \ldots x_{i_k} = x_1 x_2 \ldots x_k, \quad (x_1 x_2 \ldots x_k, m) = 1,$$

$$a^{\varphi(m)} \equiv 1 \pmod{m} \qquad \square$$

Уточнение теоремы Эйлера.

Уточнение теоремы Эйлера.

Следствие

Предположим, что $m \geqslant 2$. Сравнение $a^{\varphi(m)} \equiv 1 \pmod{m}$ имеет место в том и только том случае, когда числа a и m взаимно простые.

Сравнимость по модулю

Уточнение теоремы Эйлера.

Следствие

Предположим, что $m \geqslant 2$. Сравнение $a^{\varphi(m)} \equiv 1 \pmod{m}$ имеет место в том и только том случае, когда числа a и m взаимно простые.

$a^{\varphi(m)} \equiv 1 \pmod{m}$

Уточнение теоремы Эйлера.

Следствие

Предположим, что $m \geqslant 2$. Сравнение $a^{\varphi(m)} \equiv 1 \pmod{m}$ имеет место в том и только том случае, когда числа a и m взаимно простые.

$$a^{\varphi(m)} \equiv 1 \pmod{m}, \qquad d = (a, m)$$

Уточнение теоремы Эйлера.

Следствие

Предположим, что $m \geqslant 2$. Сравнение $a^{\varphi(m)} \equiv 1 \pmod{m}$ имеет место в том и только том случае, когда числа a и m взаимно простые.

$$a^{\varphi(m)} \equiv 1 \pmod{m}, \quad d = (a, m), \quad d|1$$

Сравнимость по модулю

Уточнение теоремы Эйлера.

Следствие

Предположим, что $m \geqslant 2$. Сравнение $a^{\varphi(m)} \equiv 1 \pmod{m}$ имеет место в том и только том случае, когда числа a и m взаимно простые.

$a^{\varphi(m)} \equiv 1 \pmod{m}, \quad d = (a, m), \quad d|1, \quad d = 1$

Уточнение теоремы Эйлера.

Следствие

Предположим, что $m \geqslant 2$. Сравнение $a^{\varphi(m)} \equiv 1 \pmod m$ имеет место в том и только том случае, когда числа a и m взаимно простые.

$a^{\varphi(m)} \equiv 1 \pmod m, \quad d = (a, m), \quad d|1, \quad d = 1, \quad (a, m) = 1.$ $\square$

Приводимое ниже утверждение, вытекающее из теоремы Эйлера, называется теоремой Ферма.

Приводимое ниже утверждение, вытекающее из теоремы Эйлера, называется теоремой Ферма.

Следствие

Пусть p — простое число, $a \in \mathbb{Z}$, $p \nmid a$. Тогда $a^{p-1} \equiv 1 \pmod{p}$.

Приводимое ниже утверждение, вытекающее из теоремы Эйлера, называется теоремой Ферма.

Следствие

Пусть p — простое число, $a \in \mathbb{Z}$, $p \nmid a$. Тогда $a^{p-1} \equiv 1 \pmod{p}$.

$(a, p) = 1$ и $\varphi(p) = p - 1$. $\square$