Математические основы защиты информации

Онлайн-лекция 2

Пилиди Владимир Ставрович

31 марта 2020 года

Сравнением первой степени с одним неизвестным называется соотношение $ax \equiv b \pmod{m}$.

Сравнением первой степени с одним неизвестным называется соотношение $ax \equiv b \,(\mathrm{mod}\, m)$.
Всегда предполагается, что $a \not\equiv 0 (\,\mathrm{mod}\, m)$.

Сравнением первой степени с одним неизвестным называется соотношение $ax \equiv b \,(\mathrm{mod}\, m)$.
Всегда предполагается, что $a \not\equiv 0 (\,\mathrm{mod}\, m)$.
Решение сравнения: любое числовое значение x, которое удовлетворяет этому соотношению.

Сравнением первой степени с одним неизвестным называется соотношение $ax \equiv b \,(\mathrm{mod}\, m)$.
Всегда предполагается, что $a \not\equiv 0(\,\mathrm{mod}\, m)$.
Решение сравнения: любое числовое значение x, которое удовлетворяет этому соотношению.
Если x_0 — решение сравнения, то есть $ax_0 \equiv b \,(\mathrm{mod}\, m)$, то для любого $t \in \mathbb{Z}$

Сравнением первой степени с одним неизвестным называется соотношение $ax \equiv b \,(\mathrm{mod}\, m)$.
Всегда предполагается, что $a \not\equiv 0(\,\mathrm{mod}\, m)$.
Решение сравнения: любое числовое значение x, которое удовлетворяет этому соотношению.
Если x_0 — решение сравнения, то есть $ax_0 \equiv b \,(\mathrm{mod}\, m)$, то для любого $t \in \mathbb{Z}$

$$a(x_0 + mt)$$

Сравнением первой степени с одним неизвестным называется соотношение $ax \equiv b \pmod{m}$.
Всегда предполагается, что $a \not\equiv 0 \pmod{m}$.
Решение сравнения: любое числовое значение x, которое удовлетворяет этому соотношению.
Если x_0 — решение сравнения, то есть $ax_0 \equiv b \pmod{m}$, то для любого $t \in \mathbb{Z}$

$$a(x_0 + mt) = ax_0 + \underbrace{amt}_{\equiv 0 \pmod{m}}$$

Сравнением первой степени с одним неизвестным называется соотношение $ax \equiv b \,(\mathrm{mod}\, m)$.
Всегда предполагается, что $a \not\equiv 0 (\,\mathrm{mod}\, m)$.
Решение сравнения: любое числовое значение x, которое удовлетворяет этому соотношению.
Если x_0 — решение сравнения, то есть $ax_0 \equiv b \,(\mathrm{mod}\, m)$, то для любого $t \in \mathbb{Z}$

$$a(x_0 + mt) = ax_0 + \underbrace{amt}_{\equiv 0 (\,\mathrm{mod}\, m)} \equiv b (\,\mathrm{mod}\, m).$$

Сравнением первой степени с одним неизвестным называется соотношение $ax \equiv b \,(\mathrm{mod}\, m)$.
Всегда предполагается, что $a \not\equiv 0 (\mathrm{mod}\, m)$.
Решение сравнения: любое числовое значение x, которое удовлетворяет этому соотношению.
Если x_0 — решение сравнения, то есть $ax_0 \equiv b \,(\mathrm{mod}\, m)$, то для любого $t \in \mathbb{Z}$

$$a(x_0 + mt) = ax_0 + \underbrace{amt}_{\equiv 0 (\mathrm{mod}\, m)} \equiv b (\mathrm{mod}\, m).$$

Вместе с решением x_0 сравнению удовлетворяют все значения из класса чисел по модулю m, содержащего x_0.

Сравнением первой степени с одним неизвестным называется соотношение $ax \equiv b \,(\mathrm{mod}\, m)$.
Всегда предполагается, что $a \not\equiv 0 (\mathrm{mod}\, m)$.
Решение сравнения: любое числовое значение x, которое удовлетворяет этому соотношению.
Если x_0 — решение сравнения, то есть $ax_0 \equiv b \,(\mathrm{mod}\, m)$, то для любого $t \in \mathbb{Z}$

$$a(x_0 + mt) = ax_0 + \underbrace{amt}_{\equiv 0 (\mathrm{mod}\, m)} \equiv b (\mathrm{mod}\, m).$$

Вместе с решением x_0 сравнению удовлетворяют все значения из класса чисел по модулю m, содержащего x_0.
Весь этот класс считается одним решением сравнения.

Сравнением первой степени с одним неизвестным называется соотношение $ax \equiv b \,(\mathrm{mod}\, m)$.
Всегда предполагается, что $a \not\equiv 0 (\,\mathrm{mod}\, m)$.
Решение сравнения: любое числовое значение x, которое удовлетворяет этому соотношению.
Если x_0 — решение сравнения, то есть $ax_0 \equiv b \,(\mathrm{mod}\, m)$, то для любого $t \in \mathbb{Z}$

$$a(x_0 + mt) = ax_0 + \underbrace{amt}_{\equiv 0 (\,\mathrm{mod}\, m)} \equiv b (\,\mathrm{mod}\, m).$$

Вместе с решением x_0 сравнению удовлетворяют все значения из класса чисел по модулю m, содержащего x_0.
Весь этот класс считается одним решением сравнения.
Этот класс будем называть решением сравнения по модулю m.

Сравнение $ax \equiv b \pmod{m}$, обозначение $d = (a, m)$

Сравнение $ax \equiv b \pmod{m}$, обозначение $d = (a, m)$

Теорема

Сравнение $ax \equiv b \pmod{m}$ имеет решения в том и только том случае, когда $d \mid b$. При выполнении этого условия данное сравнение имеет ровно d решений по модулю m.

Сравнение $ax \equiv b \pmod{m}$, обозначение $d = (a, m)$

Теорема

Сравнение $ax \equiv b \pmod{m}$ имеет решения в том и только том случае, когда $d \mid b$. При выполнении этого условия данное сравнение имеет ровно d решений по модулю m.

Предположим, что сравнение разрешимо.

Сравнение $ax \equiv b \pmod{m}$, обозначение $d = (a, m)$

Теорема

Сравнение $ax \equiv b \pmod{m}$ имеет решения в том и только том случае, когда $d \mid b$. При выполнении этого условия данное сравнение имеет ровно d решений по модулю m.

Предположим, что сравнение разрешимо.

$$ax_1 \equiv b \pmod{m}$$

Сравнение $ax \equiv b \pmod{m}$, обозначение $d = (a, m)$

Теорема

Сравнение $ax \equiv b \pmod{m}$ имеет решения в том и только том случае, когда $d \mid b$. При выполнении этого условия данное сравнение имеет ровно d решений по модулю m.

Предположим, что сравнение разрешимо.

$$ax_1 \equiv b \pmod{m} \Rightarrow d | ax_1$$

Сравнение $ax \equiv b \pmod{m}$, обозначение $d = (a, m)$

Теорема

Сравнение $ax \equiv b \pmod{m}$ имеет решения в том и только том случае, когда $d \mid b$. При выполнении этого условия данное сравнение имеет ровно d решений по модулю m.

Предположим, что сравнение разрешимо.

$$ax_1 \equiv b \pmod{m} \Rightarrow d|ax_1,\ d|m$$

Сравнение $ax \equiv b \pmod{m}$, обозначение $d = (a, m)$

Теорема

Сравнение $ax \equiv b \pmod{m}$ имеет решения в том и только том случае, когда $d \mid b$. При выполнении этого условия данное сравнение имеет ровно d решений по модулю m.

Предположим, что сравнение разрешимо.

$$ax_1 \equiv b \pmod{m} \Rightarrow d|ax_1,\ d|m \Rightarrow d \mid b.$$

Сравнение $ax \equiv b \pmod{m}$, обозначение $d = (a, m)$

Теорема

Сравнение $ax \equiv b \pmod{m}$ имеет решения в том и только том случае, когда $d \mid b$. При выполнении этого условия данное сравнение имеет ровно d решений по модулю m.

Предположим, что сравнение разрешимо.

$$ax_1 \equiv b \pmod{m} \Rightarrow d|ax_1,\ d|m \Rightarrow d \mid b.$$

Обратное утверждение, $d|b$.

Сравнение $ax \equiv b \pmod{m}$, обозначение $d = (a, m)$

Теорема

Сравнение $ax \equiv b \pmod{m}$ имеет решения в том и только том случае, когда $d \mid b$. При выполнении этого условия данное сравнение имеет ровно d решений по модулю m.

Предположим, что сравнение разрешимо.

$$ax_1 \equiv b \pmod{m} \Rightarrow d|ax_1,\ d|m \Rightarrow d \mid b.$$

Обратное утверждение, $d|b$. Сначала $d = 1$.

Сравнение $ax \equiv b \pmod{m}$, обозначение $d = (a, m)$

Теорема

Сравнение $ax \equiv b \pmod{m}$ имеет решения в том и только том случае, когда $d \mid b$. При выполнении этого условия данное сравнение имеет ровно d решений по модулю m.

Предположим, что сравнение разрешимо.

$$ax_1 \equiv b \pmod{m} \Rightarrow d|ax_1,\ d|m \Rightarrow d \mid b.$$

Обратное утверждение, $d|b$. Сначала $d = 1$.

$x_1, x_2, \ldots, x_m$ — полная система вычетов по модулю m.

Сравнение $ax \equiv b \pmod{m}$, обозначение $d = (a, m)$

Теорема

Сравнение $ax \equiv b \pmod{m}$ имеет решения в том и только том случае, когда $d \mid b$. При выполнении этого условия данное сравнение имеет ровно d решений по модулю m.

Предположим, что сравнение разрешимо.

$$ax_1 \equiv b \pmod{m} \Rightarrow d|ax_1,\ d|m \Rightarrow d \mid b.$$

Обратное утверждение, $d|b$. Сначала $d = 1$.

$x_1, x_2, \ldots, x_m$ — полная система вычетов по модулю m.

$ax_1, ax_2, \ldots, ax_m$ — полная система вычетов по модулю m.

Сравнение $ax \equiv b \pmod{m}$, обозначение $d = (a, m)$

Теорема

Сравнение $ax \equiv b \pmod{m}$ имеет решения в том и только том случае, когда $d \mid b$. При выполнении этого условия данное сравнение имеет ровно d решений по модулю m.

Предположим, что сравнение разрешимо.

$$ax_1 \equiv b \pmod{m} \Rightarrow d|ax_1,\ d|m \Rightarrow d \mid b.$$

Обратное утверждение, $d|b$. Сначала $d = 1$.

$x_1, x_2, \ldots, x_m$ — полная система вычетов по модулю m.

$ax_1, ax_2, \ldots, ax_m$ — полная система вычетов по модулю m.

При $d = 1$ существует единственное решение.

Случай $d > 1$

Случай $d > 1$, $\qquad a_1 = \frac{a}{d}$

Случай $d > 1$, $\quad a_1 = \frac{a}{d}$, $\quad b_1 = \frac{b}{d}$

Случай $d > 1$, $\quad a_1 = \frac{a}{d}$, $\quad b_1 = \frac{b}{d}$, $\quad m_1 = \frac{m}{d}$.

Случай $d > 1$, $\quad a_1 = \frac{a}{d}$, $\quad b_1 = \frac{b}{d}$, $\quad m_1 = \frac{m}{d}$.

$$ax \equiv b \pmod{m} \Leftrightarrow a_1 x \equiv b_1 \pmod{m_1}$$

Случай $d > 1$, $\quad a_1 = \frac{a}{d}$, $\quad b_1 = \frac{b}{d}$, $\quad m_1 = \frac{m}{d}$.

$$ax \equiv b \pmod{m} \Leftrightarrow a_1 x \equiv b_1 \pmod{m_1}$$

Новое сравнение равносильно исходному.

Случай $d > 1$, $\quad a_1 = \frac{a}{d}$, $\quad b_1 = \frac{b}{d}$, $\quad m_1 = \frac{m}{d}$.

$$ax \equiv b \pmod{m} \Leftrightarrow a_1 x \equiv b_1 \pmod{m_1}$$

Новое сравнение равносильно исходному.

Решение $a_1 x_0 \equiv b_1 \pmod{m_1}$.

Случай $d > 1$, $\quad a_1 = \frac{a}{d}$, $\quad b_1 = \frac{b}{d}$, $\quad m_1 = \frac{m}{d}$.

$$ax \equiv b \pmod{m} \Leftrightarrow a_1 x \equiv b_1 \pmod{m_1}$$

Новое сравнение равносильно исходному.

Решение $a_1 x_0 \equiv b_1 \pmod{m_1}$.

Выписываем последовательно все числа из класса по модулю m_1.

Случай $d > 1$, $\quad a_1 = \frac{a}{d}$, $\quad b_1 = \frac{b}{d}$, $\quad m_1 = \frac{m}{d}$.

$$ax \equiv b \pmod{m} \Leftrightarrow a_1 x \equiv b_1 \pmod{m_1}$$

Новое сравнение равносильно исходному.

Решение $a_1 x_0 \equiv b_1 \pmod{m_1}$.

Выписываем последовательно все числа из класса по модулю m_1.

$$\ldots, x_0, x_0 + \underbrace{m_1}_{<m}, x_0 + \underbrace{2m_1}_{<m}, \ldots, x_0 + \underbrace{(d-1)m_1}_{<m}, x_0 + \underbrace{m_1 d}_{=m}, \ldots$$

Существует d решений по модулю m. □

Алгоритм решения сравнения $ax \equiv b \pmod{m}$, случай $(a, m) = 1$.

Алгоритм решения сравнения $ax \equiv b \pmod{m}$, случай $(a, m) = 1$.

$$au + mv = 1$$

Алгоритм решения сравнения $ax \equiv b \pmod{m}$, случай $(a, m) = 1$.

$au + mv = 1$, $au \equiv 1 \pmod{m}$

Алгоритм решения сравнения $ax \equiv b \pmod{m}$, случай $(a, m) = 1$.

$au + mv = 1$, $au \equiv 1 \pmod{m}$, $a(bu) \equiv b \pmod{m}$.

Алгоритм решения сравнения $ax \equiv b \pmod{m}$, случай $(a, m) = 1$.

$au + mv = 1$, $au \equiv 1 \pmod{m}$, $a(bu) \equiv b \pmod{m}$.

Решение $x \equiv bu \pmod{m}$.

Алгоритм решения сравнения $ax \equiv b \pmod{m}$, случай $(a, m) = 1$.

$au + mv = 1$, $au \equiv 1 \pmod{m}$, $a(bu) \equiv b \pmod{m}$.

Решение $x \equiv bu \pmod{m}$.

Альтернативный метод, применяется теорема Эйлера.

Алгоритм решения сравнения $ax \equiv b \pmod{m}$, случай $(a, m) = 1$.

$au + mv = 1$, $au \equiv 1 \pmod{m}$, $a(bu) \equiv b \pmod{m}$.

Решение $x \equiv bu \pmod{m}$.

Альтернативный метод, применяется теорема Эйлера.

$x_0 = ba^{\varphi(m)-1}$

Алгоритм решения сравнения $ax \equiv b \pmod{m}$, случай $(a, m) = 1$.

$au + mv = 1$, $au \equiv 1 \pmod{m}$, $a(bu) \equiv b \pmod{m}$.

Решение $x \equiv bu \pmod{m}$.

Альтернативный метод, применяется теорема Эйлера.

$$x_0 = ba^{\varphi(m)-1},\ ax_0 = b\underbrace{a^{\varphi(m)}}_{\equiv 1} \equiv b(\bmod m)$$

Алгоритм решения сравнения $ax \equiv b \pmod{m}$, случай $(a, m) = 1$.

$au + mv = 1$, $au \equiv 1 \pmod{m}$, $a(bu) \equiv b \pmod{m}$.

Решение $x \equiv bu \pmod{m}$.

Альтернативный метод, применяется теорема Эйлера.

$$x_0 = ba^{\varphi(m)-1},\ ax_0 = b\underbrace{a^{\varphi(m)}}_{\equiv 1} \equiv b(\bmod m),\ x \equiv x_0 \pmod{m}.$$

Теорема (китайская теорема об остатках)

Пусть $m_1, m_2, \ldots, m_k$ — попарно взаимно простые модули. Тогда для любых $b_1, b_2, \ldots, b_k \in \mathbb{Z}$ система сравнений с одним неизвестным

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

имеет единственное решение по модулю $M = m_1 m_2 \ldots m_k$.

Случай $k = 1$ тривиальный.

Случай $k = 1$ тривиальный.
Доказательство по индукции при $k \geqslant 2$.

Случай $k = 1$ тривиальный.
Доказательство по индукции при $k \geqslant 2$.
База индукции: $k = 2$.

Случай $k = 1$ тривиальный.
Доказательство по индукции при $k \geqslant 2$.
База индукции: $k = 2$.

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \end{cases}$$

Случай $k = 1$ тривиальный.
Доказательство по индукции при $k \geqslant 2$.
База индукции: $k = 2$.

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \end{cases}$$

$$x = b_1 + m_1 t, \qquad t \in \mathbb{Z}.$$

Случай $k = 1$ тривиальный.
Доказательство по индукции при $k \geqslant 2$.
База индукции: $k = 2$.

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \end{cases}$$

$$x = b_1 + m_1 t, \qquad t \in \mathbb{Z}.$$

$$b_1 + m_1 t \equiv b_2 \pmod{m_2}$$

Случай $k = 1$ тривиальный.
Доказательство по индукции при $k \geqslant 2$.
База индукции: $k = 2$.

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \end{cases}$$

$$x = b_1 + m_1 t, \qquad t \in \mathbb{Z}.$$

$$b_1 + m_1 t \equiv b_2 \pmod{m_2}, \qquad m_1 t \equiv b_2 - b_1 \pmod{m_2},$$

Случай $k = 1$ тривиальный.
Доказательство по индукции при $k \geqslant 2$.
База индукции: $k = 2$.

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \end{cases}$$

$$x = b_1 + m_1 t, \qquad t \in \mathbb{Z}.$$

$$b_1 + m_1 t \equiv b_2 \pmod{m_2}, \qquad m_1 t \equiv b_2 - b_1 \pmod{m_2},$$

$$t = t_0 + m_2 \tau, \quad \tau \in \mathbb{Z},$$

Случай $k = 1$ тривиальный.
Доказательство по индукции при $k \geqslant 2$.
База индукции: $k = 2$.

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \end{cases}$$

$$x = b_1 + m_1 t, \qquad t \in \mathbb{Z}.$$

$$b_1 + m_1 t \equiv b_2 \pmod{m_2}, \qquad m_1 t \equiv b_2 - b_1 \pmod{m_2},$$

$$t = t_0 + m_2 \tau, \quad \tau \in \mathbb{Z},$$

$$x = b_1 + m_1(t_0 + m_2\tau) =$$

Случай $k = 1$ тривиальный.
Доказательство по индукции при $k \geqslant 2$.
База индукции: $k = 2$.

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \end{cases}$$

$$x = b_1 + m_1 t, \qquad t \in \mathbb{Z}.$$

$$b_1 + m_1 t \equiv b_2 \pmod{m_2}, \qquad m_1 t \equiv b_2 - b_1 \pmod{m_2},$$

$$t = t_0 + m_2 \tau, \quad \tau \in \mathbb{Z},$$

$$x = b_1 + m_1(t_0 + m_2\tau) =$$

$$= \underbrace{b_1 + m_1 t_0}_{x_0} + \underbrace{m_1 m_2}_{=M} \tau =$$

Случай $k = 1$ тривиальный.
Доказательство по индукции при $k \geqslant 2$.
База индукции: $k = 2$.

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \end{cases}$$

$$x = b_1 + m_1 t, \qquad t \in \mathbb{Z}.$$

$$b_1 + m_1 t \equiv b_2 \pmod{m_2}, \qquad m_1 t \equiv b_2 - b_1 \pmod{m_2},$$

$$t = t_0 + m_2 \tau, \quad \tau \in \mathbb{Z},$$

$$x = b_1 + m_1(t_0 + m_2\tau) =$$

$$= \underbrace{b_1 + m_1 t_0}_{x_0} + \underbrace{m_1 m_2}_{=M} \tau =$$

$$= x_0 + m_1 m_2 \tau, \quad \tau \in \mathbb{Z}.$$

Индуктивный переход.

Индуктивный переход.
Предположим, что теорема верна при некотором $k \geqslant 2$.

Индуктивный переход.

Предположим, что теорема верна при некотором $k \geqslant 2$.

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \pmod{m_k}, \\ x \equiv b_{k+1} \pmod{m_{k+1}}. \end{cases}$$

Индуктивный переход.

Предположим, что теорема верна при некотором $k \geqslant 2$.

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \pmod{m_k}, \\ x \equiv b_{k+1} \pmod{m_{k+1}}. \end{cases} \Rightarrow$$

Индуктивный переход.

Предположим, что теорема верна при некотором $k \geqslant 2$.

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \pmod{m_k}, \\ x \equiv b_{k+1} \pmod{m_{k+1}}. \end{cases} \Rightarrow \begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \pmod{m_k}. \end{cases}$$

Индуктивный переход.

Предположим, что теорема верна при некотором $k \geqslant 2$.

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \pmod{m_k}, \\ x \equiv b_{k+1} \pmod{m_{k+1}}. \end{cases} \Rightarrow \begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \pmod{m_k}. \end{cases}$$

Применяем индуктивное предположение.

Индуктивный переход.

Предположим, что теорема верна при некотором $k \geqslant 2$.

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \pmod{m_k}, \\ x \equiv b_{k+1} \pmod{m_{k+1}}. \end{cases} \Rightarrow \begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \pmod{m_k}. \end{cases}$$

Применяем индуктивное предположение.

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

Индуктивный переход.

Предположим, что теорема верна при некотором $k \geqslant 2$.

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \pmod{m_k}, \\ x \equiv b_{k+1} \pmod{m_{k+1}}. \end{cases} \Rightarrow \begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \pmod{m_k}. \end{cases}$$

Применяем индуктивное предположение.

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \pmod{m_k} \end{cases} \Leftrightarrow$$

Индуктивный переход.

Предположим, что теорема верна при некотором $k \geqslant 2$.

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \pmod{m_k}, \\ x \equiv b_{k+1} \pmod{m_{k+1}}. \end{cases} \Rightarrow \begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \pmod{m_k}. \end{cases}$$

Применяем индуктивное предположение.

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \pmod{m_k} \end{cases} \Leftrightarrow \quad x \equiv B \pmod{m_1 \ldots m_k}$$

Индуктивный переход.

Предположим, что теорема верна при некотором $k \geqslant 2$.

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \pmod{m_k}, \\ x \equiv b_{k+1} \pmod{m_{k+1}}. \end{cases} \Rightarrow \begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \pmod{m_k}. \end{cases}$$

Применяем индуктивное предположение.

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \pmod{m_k} \end{cases} \Leftrightarrow \quad x \equiv B \pmod{m_1 \ldots m_k}$$

$$M_0 = m_1 \ldots m_k.$$

$$\begin{cases} x \equiv b_1 \,(\mathrm{mod}\, m_1), \\ x \equiv b_2 \,(\mathrm{mod}\, m_2), \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \,(\mathrm{mod}\, m_k), \\ x \equiv b_{k+1} \,(\mathrm{mod}\, m_{k+1}). \end{cases}$$

$$\left\{\begin{array}{l} x \equiv b_1 \,(\mathrm{mod}\, m_1), \\ x \equiv b_2 \,(\mathrm{mod}\, m_2), \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \,(\mathrm{mod}\, m_k), \\ x \equiv b_{k+1} \,(\mathrm{mod}\, m_{k+1}). \end{array}\right. \quad \Leftrightarrow$$

$$\begin{cases} x \equiv b_1 \,(\mathrm{mod}\, m_1), \\ x \equiv b_2 \,(\mathrm{mod}\, m_2), \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \,(\mathrm{mod}\, m_k), \\ x \equiv b_{k+1} \,(\mathrm{mod}\, m_{k+1}). \end{cases} \quad \Leftrightarrow \quad \begin{cases} x \equiv B \,(\mathrm{mod}\, M_0), \\ x \equiv b_{k+1} \,(\mathrm{mod}\, m_{k+1}). \end{cases}$$

$$\begin{cases} x \equiv b_1 \,(\mathrm{mod}\, m_1), \\ x \equiv b_2 \,(\mathrm{mod}\, m_2), \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \,(\mathrm{mod}\, m_k), \\ x \equiv b_{k+1} \,(\mathrm{mod}\, m_{k+1}). \end{cases} \Leftrightarrow \begin{cases} x \equiv B \,(\mathrm{mod}\, M_0), \\ x \equiv b_{k+1} \,(\mathrm{mod}\, m_{k+1}). \end{cases}$$

По доказанному выше последняя система имеет единственное решение по модулю $M_0 m_{k+1} = M$. □

Сравнения

Алгоритм решения системы сравнений

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \dots\dots\dots\dots\dots\dots \\ x \equiv b_k \pmod{m_k}. \end{cases}$$

Сравнения

Алгоритм решения системы сравнений

$$\begin{cases} x \equiv b_1 \,(\mathrm{mod}\, m_1), \\ x \equiv b_2 \,(\mathrm{mod}\, m_2), \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \,(\mathrm{mod}\, m_k). \end{cases} \qquad \begin{cases} m_2 m_3 \ldots m_k y_1 \equiv 1 \,(\mathrm{mod}\, m_1), \\ m_1 m_3 \ldots m_k y_2 \equiv 1 \,(\mathrm{mod}\, m_2), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ m_1 m_2 \ldots m_{k-1} y_k \equiv 1 \,(\mathrm{mod}\, m_k). \end{cases}$$

Сравнения

Алгоритм решения системы сравнений

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \dots\dots\dots\dots\dots \\ x \equiv b_k \pmod{m_k}. \end{cases} \qquad \begin{cases} m_2 m_3 \dots m_k y_1 \equiv 1 \pmod{m_1}, \\ m_1 m_3 \dots m_k y_2 \equiv 1 \pmod{m_2}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ m_1 m_2 \dots m_{k-1} y_k \equiv 1 \pmod{m_k}. \end{cases}$$

$$x_0 = m_2 m_3 \dots m_k y_1 b_1 + m_1 m_3 \dots m_k y_2 b_2 + \dots + m_1 m_2 \dots m_{k-1} y_y b_k.$$

$$\begin{cases} x \equiv b_1 \,(\mathrm{mod}\, m_1), \\ x \equiv b_2 \,(\mathrm{mod}\, m_2), \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \,(\mathrm{mod}\, m_k). \end{cases} \qquad \begin{cases} m_2 m_3 \ldots m_k y_1 \equiv 1 \,(\mathrm{mod}\, m_1), \\ m_1 m_3 \ldots m_k y_2 \equiv 1 \,(\mathrm{mod}\, m_2), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ m_1 m_2 \ldots m_{k-1} y_k \equiv 1 \,(\mathrm{mod}\, m_k). \end{cases}$$

$$x_0 = m_2 m_3 \ldots m_k y_1 b_1 + m_1 m_3 \ldots m_k y_2 b_2 + \cdots + m_1 m_2 \ldots m_{k-1} y_y b_k.$$

$$x_0 = \underbrace{m_2 m_3 \ldots m_k y_1}_{\equiv 1 (\,\mathrm{mod}\, m_1)} b_1 + \underbrace{m_1 m_3 \ldots m_k y_2}_{\equiv 0 (\,\mathrm{mod}\, m_1)} b_2 + \cdots +$$

$$\begin{cases} x \equiv b_1 \,(\mathrm{mod}\, m_1), \\ x \equiv b_2 \,(\mathrm{mod}\, m_2), \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \,(\mathrm{mod}\, m_k). \end{cases} \qquad \begin{cases} m_2 m_3 \ldots m_k y_1 \equiv 1 \,(\mathrm{mod}\, m_1), \\ m_1 m_3 \ldots m_k y_2 \equiv 1 \,(\mathrm{mod}\, m_2), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ m_1 m_2 \ldots m_{k-1} y_k \equiv 1 \,(\mathrm{mod}\, m_k). \end{cases}$$

$$x_0 = m_2 m_3 \ldots m_k y_1 b_1 + m_1 m_3 \ldots m_k y_2 b_2 + \cdots + m_1 m_2 \ldots m_{k-1} y_y b_k.$$

$$x_0 = \underbrace{m_2 m_3 \ldots m_k y_1}_{\equiv 1 (\,\mathrm{mod}\, m_1)} b_1 + \underbrace{m_1 m_3 \ldots m_k y_2}_{\equiv 0 (\,\mathrm{mod}\, m_1)} b_2 + \cdots +$$

$$+ \underbrace{m_1 m_2 \ldots m_{k-1} y_k}_{\equiv 0 (\,\mathrm{mod}\, m_1)} b_k \equiv b_1 (\,\mathrm{mod}\, m_1).$$

$$\begin{cases} x \equiv b_1 \,(\mathrm{mod}\, m_1), \\ x \equiv b_2 \,(\mathrm{mod}\, m_2), \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv b_k \,(\mathrm{mod}\, m_k). \end{cases} \qquad \begin{cases} m_2 m_3 \ldots m_k y_1 \equiv 1 \,(\mathrm{mod}\, m_1), \\ m_1 m_3 \ldots m_k y_2 \equiv 1 \,(\mathrm{mod}\, m_2), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ m_1 m_2 \ldots m_{k-1} y_k \equiv 1 \,(\mathrm{mod}\, m_k). \end{cases}$$

$$x_0 = m_2 m_3 \ldots m_k y_1 b_1 + m_1 m_3 \ldots m_k y_2 b_2 + \cdots + m_1 m_2 \ldots m_{k-1} y_y b_k.$$

$$x_0 = \underbrace{m_2 m_3 \ldots m_k y_1}_{\equiv 1 (\,\mathrm{mod}\, m_1)} b_1 + \underbrace{m_1 m_3 \ldots m_k y_2}_{\equiv 0 (\,\mathrm{mod}\, m_1)} b_2 + \cdots +$$

$$+ \underbrace{m_1 m_2 \ldots m_{k-1} y_k}_{\equiv 0 (\,\mathrm{mod}\, m_1)} b_k \equiv b_1 (\,\mathrm{mod}\, m_1).$$

Число x_0 является решением данной системы сравнений.

Бинарная операция

Определение

Определение

Говорят, что на непустом множестве X задана бинарная операция, если указано правило, с помощью которого каждой упорядоченной паре элементов a, $b \in X$ ставится в соответствие однозначно определенный элемент этого же множества.

Бинарная операция

Определение

Определение

Говорят, что на непустом множестве X задана бинарная операция, если указано правило, с помощью которого каждой упорядоченной паре элементов a, $b \in X$ ставится в соответствие однозначно определенный элемент этого же множества.

Обозначения $a * b$, $a \circ b$, ab, $a + b$.

Бинарная операция

Определение

Определение

Говорят, что на непустом множестве X задана бинарная операция, если указано правило, с помощью которого каждой упорядоченной паре элементов a, $b \in X$ ставится в соответствие однозначно определенный элемент этого же множества.

Обозначения $a * b$, $a \circ b$, ab, $a + b$.

Замечание

Бинарная операция — отображение $X \times X \to X$, $(a, b) \mapsto a * b$.

Бинарная операция

Примеры

Арифметические операции на множестве $\mathbb{N}$.

Бинарная операция

Примеры

Арифметические операции на множестве $\mathbb{N}$.
Арифметические операции на множестве $\mathbb{Z}$.

Бинарная операция

Примеры

Арифметические операции на множестве $\mathbb{N}$.
Арифметические операции на множестве $\mathbb{Z}$.
Арифметические операции на множестве $\mathbb{Q}$.

Бинарная операция

Примеры

Арифметические операции на множестве $\mathbb{N}$.
Арифметические операции на множестве $\mathbb{Z}$.
Арифметические операции на множестве $\mathbb{Q}$.
Арифметические операции на множествах многочленов с числовыми элементами.

Бинарная операция

Примеры

Арифметические операции на множестве $\mathbb{N}$.
Арифметические операции на множестве $\mathbb{Z}$.
Арифметические операции на множестве $\mathbb{Q}$.
Арифметические операции на множествах многочленов с числовыми элементами.
Арифметические операции на множествах матриц с числовыми элементами.

Бинарная операция

Примеры

Арифметические операции на множестве $\mathbb{N}$.
Арифметические операции на множестве $\mathbb{Z}$.
Арифметические операции на множестве $\mathbb{Q}$.
Арифметические операции на множествах многочленов с числовыми элементами.
Арифметические операции на множествах матриц с числовыми элементами.
Множество всех обратимых квадратных матриц фиксированного порядка с вещественными коэффициентами, отображение $(A, B) \mapsto AB^{-1}$.

Бинарная операция

Примеры

Арифметические операции на множестве $\mathbb{N}$.
Арифметические операции на множестве $\mathbb{Z}$.
Арифметические операции на множестве $\mathbb{Q}$.
Арифметические операции на множествах многочленов с числовыми элементами.
Арифметические операции на множествах матриц с числовыми элементами.
Множество всех обратимых квадратных матриц фиксированного порядка с вещественными коэффициентами, отображение $(A, B) \mapsto AB^{-1}$.
Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

Бинарная операция

Примеры

Арифметические операции на множестве $\mathbb{N}$.
Арифметические операции на множестве $\mathbb{Z}$.
Арифметические операции на множестве $\mathbb{Q}$.
Арифметические операции на множествах многочленов с числовыми элементами.
Арифметические операции на множествах матриц с числовыми элементами.
Множество всех обратимых квадратных матриц фиксированного порядка с вещественными коэффициентами, отображение $(A, B) \mapsto AB^{-1}$.
Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».
Множество 2^X, бинарные операции $(A, B) \mapsto A \cup B$, $(A, B) \mapsto A \cap B$, $(A, B) \mapsto A \setminus B$.

Бинарная операция

Примеры

Арифметические операции на множестве $\mathbb{N}$.
Арифметические операции на множестве $\mathbb{Z}$.
Арифметические операции на множестве $\mathbb{Q}$.
Арифметические операции на множествах многочленов с числовыми элементами.
Арифметические операции на множествах матриц с числовыми элементами.
Множество всех обратимых квадратных матриц фиксированного порядка с вещественными коэффициентами, отображение $(A, B) \mapsto AB^{-1}$.
Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».
Множество 2^X, бинарные операции $(A, B) \mapsto A \cup B$, $(A, B) \mapsto A \cap B$, $(A, B) \mapsto A \setminus B$.
Множество всех векторов в пространстве, бинарная операция $(\vec{a}, \vec{b}) \mapsto \vec{a} \times \vec{b}$.

Определение

Бинарная операция, определенная на множестве X, называется коммутативной, если для любых элементов a, $b \in X$ выполняется равенство $a * b = b * a$.

Определение

Бинарная операция, определенная на множестве X, называется коммутативной, если для любых элементов a, $b \in X$ выполняется равенство $a * b = b * a$.

Анализ коммутативности.

Определение

Бинарная операция, определенная на множестве X, называется коммутативной, если для любых элементов a, $b \in X$ выполняется равенство $a * b = b * a$.

Анализ коммутативности.
$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение.

Определение

Бинарная операция, определенная на множестве X, называется коммутативной, если для любых элементов a, $b \in X$ выполняется равенство $a * b = b * a$.

Анализ коммутативности.
$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

Определение

Бинарная операция, определенная на множестве X, называется коммутативной, если для любых элементов a, $b \in X$ выполняется равенство $a * b = b * a$.

Анализ коммутативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение.

Определение

Бинарная операция, определенная на множестве X, называется коммутативной, если для любых элементов a, $b \in X$ выполняется равенство $a * b = b * a$.

Анализ коммутативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

Определение

Бинарная операция, определенная на множестве X, называется коммутативной, если для любых элементов a, $b \in X$ выполняется равенство $a * b = b * a$.

Анализ коммутативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

Определение

Бинарная операция, определенная на множестве X, называется коммутативной, если для любых элементов a, $b \in X$ выполняется равенство $a * b = b * a$.

Анализ коммутативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

$$a - b = b - a$$

Определение

Бинарная операция, определенная на множестве X, называется коммутативной, если для любых элементов a, $b \in X$ выполняется равенство $a * b = b * a$.

Анализ коммутативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

$$a - b = b - a,\ 2a = 2b$$

Определение

Бинарная операция, определенная на множестве X, называется коммутативной, если для любых элементов a, $b \in X$ выполняется равенство $a * b = b * a$.

Анализ коммутативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

$$a - b = b - a,\ 2a = 2b,\ a = b$$

Определение

Бинарная операция, определенная на множестве X, называется коммутативной, если для любых элементов a, $b \in X$ выполняется равенство $a * b = b * a$.

Анализ коммутативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

$$a - b = b - a,\ 2a = 2b,\ a = b\ ,\ -$$

Определение

Бинарная операция, определенная на множестве X, называется коммутативной, если для любых элементов a, $b \in X$ выполняется равенство $a * b = b * a$.

Анализ коммутативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

$$a - b = b - a,\ 2a = 2b,\ a = b\ , -$$

$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $(a, b) \mapsto a : b$.

Определение

Бинарная операция, определенная на множестве X, называется коммутативной, если для любых элементов a, $b \in X$ выполняется равенство $a * b = b * a$.

Анализ коммутативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

$$a - b = b - a,\ 2a = 2b,\ a = b\ , -$$

$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $(a, b) \mapsto a : b$.

$$a : b = b : a$$

Определение

Бинарная операция, определенная на множестве X, называется коммутативной, если для любых элементов a, $b \in X$ выполняется равенство $a * b = b * a$.

Анализ коммутативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

$$a - b = b - a,\ 2a = 2b,\ a = b\ , -$$

$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $(a, b) \mapsto a : b$.

$$a : b = b : a,\ a^2 = b^2$$

Определение

Бинарная операция, определенная на множестве X, называется коммутативной, если для любых элементов a, $b \in X$ выполняется равенство $a * b = b * a$.

Анализ коммутативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

$$a - b = b - a,\ 2a = 2b,\ a = b\ , -$$

$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $(a, b) \mapsto a : b$.

$$a : b = b : a,\ a^2 = b^2,\ a = \pm b$$

Определение

Бинарная операция, определенная на множестве X, называется коммутативной, если для любых элементов a, $b \in X$ выполняется равенство $a * b = b * a$.

Анализ коммутативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

$$a - b = b - a,\ 2a = 2b,\ a = b\ , -$$

$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $(a, b) \mapsto a : b$.

$$a : b = b : a,\ a^2 = b^2,\ a = \pm b,\ -$$

Определение

Бинарная операция, определенная на множестве X, называется коммутативной, если для любых элементов a, $b \in X$ выполняется равенство $a * b = b * a$.

Анализ коммутативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

$$a - b = b - a,\ 2a = 2b,\ a = b\ , -$$

$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $(a, b) \mapsto a : b$.

$$a : b = b : a,\ a^2 = b^2,\ a = \pm b,\ -$$

Операция умножения геометрических векторов некоммутативная: всегда $\vec{a} \times \vec{b} = -\vec{b} \times \vec{a}$

Определение

Бинарная операция, определенная на множестве X, называется коммутативной, если для любых элементов a, $b \in X$ выполняется равенство $a * b = b * a$.

Анализ коммутативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

$$a - b = b - a,\ 2a = 2b,\ a = b\ , -$$

$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $(a, b) \mapsto a : b$.

$$a : b = b : a,\ a^2 = b^2,\ a = \pm b,\ -$$

Операция умножения геометрических векторов некоммутативная: всегда $\vec{a} \times \vec{b} = -\vec{b} \times \vec{a}$

Определение

Бинарная операция, определенная на множестве X, называется коммутативной, если для любых элементов a, $b \in X$ выполняется равенство $a * b = b * a$.

Анализ коммутативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

$$a - b = b - a,\ 2a = 2b,\ a = b\ ,\ -$$

$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $(a, b) \mapsto a : b$.

$$a : b = b : a,\ a^2 = b^2,\ a = \pm b,\ -$$

Операция умножения геометрических векторов некоммутативная: всегда $\vec{a} \times \vec{b} = -\vec{b} \times \vec{a}$, если векторы $\vec{a}$ и $\vec{b}$ неколлинеарные, то $\vec{a} \times \vec{b} \neq \vec{0}$, $\vec{a} \times \vec{b} \neq \vec{b} \times \vec{a}$. $-$

Бинарная операция

Коммутативность

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

Бинарная операция

Коммутативность

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a, b) = (b, a)$$

Бинарная операция

Коммутативность

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a, b) = (b, a), \ [a, b] = [b, a],$$

Бинарная операция

Коммутативность

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a, b) = (b, a), [a, b] = [b, a], +$$

Бинарная операция

Коммутативность

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a, b) = (b, a), \ [a, b] = [b, a], \ +$$

Множество 2^X, бинарные операции $(A, B) \mapsto A \cup B$, $(A, B) \mapsto A \cap B$

Бинарная операция

Коммутативность

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a, b) = (b, a),\ [a, b] = [b, a],\ +$$

Множество 2^X, бинарные операции $(A, B) \mapsto A \cup B$, $(A, B) \mapsto A \cap B$, $+$

Бинарная операция

Коммутативность

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a, b) = (b, a), [a, b] = [b, a], +$$

Множество 2^X, бинарные операции $(A, B) \mapsto A \cup B$, $(A, B) \mapsto A \cap B$, $+$

Множество 2^X, бинарная операция $(A, B) \mapsto A \setminus B$

Бинарная операция

Коммутативность

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a, b) = (b, a),\ [a, b] = [b, a],\ +$$

Множество 2^X, бинарные операции $(A, B) \mapsto A \cup B$, $(A, B) \mapsto A \cap B$, $+$

Множество 2^X, бинарная операция $(A, B) \mapsto A \setminus B$, $-$

Бинарная операция

Коммутативность

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a, b) = (b, a),\ [a, b] = [b, a],\ +$$

Множество 2^X, бинарные операции $(A, B) \mapsto A \cup B$,
$(A, B) \mapsto A \cap B$, $+$

Множество 2^X, бинарная операция $(A, B) \mapsto A \setminus B$, $-$
$A = \{a\}$, $B = \varnothing$,

Бинарная операция

Коммутативность

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a, b) = (b, a),\ [a, b] = [b, a],\ +$$

Множество 2^X, бинарные операции $(A, B) \mapsto A \cup B$,
$(A, B) \mapsto A \cap B$, $+$

Множество 2^X, бинарная операция $(A, B) \mapsto A \setminus B$, $-$

$A = \{a\},\ B = \varnothing, \quad A \setminus B = A$

Бинарная операция

Коммутативность

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a, b) = (b, a),\ [a, b] = [b, a],\ +$$

Множество 2^X, бинарные операции $(A, B) \mapsto A \cup B$,
$(A, B) \mapsto A \cap B$, $+$

Множество 2^X, бинарная операция $(A, B) \mapsto A \setminus B$, $-$

$A = \{a\},\ B = \varnothing, \quad A \setminus B = A \quad , B \setminus A = \varnothing.$

Бинарная операция

Коммутативность

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a, b) = (b, a),\ [a, b] = [b, a],\ +$$

Множество 2^X, бинарные операции $(A, B) \mapsto A \cup B$,
$(A, B) \mapsto A \cap B$, $+$

Множество 2^X, бинарная операция $(A, B) \mapsto A \setminus B$, $-$

$A = \{a\},\ B = \varnothing,\quad A \setminus B = A \quad,\ B \setminus A = \varnothing.$

В случае конечных множеств бинарная операция иногда задается таблицей Кэли.

Множество $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$, бинарная операция $(a, b) \mapsto (ab) \bmod 5$.

Бинарная операция

Коммутативность

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a,b) = (b,a),\ [a,b] = [b,a],\ +$$

Множество 2^X, бинарные операции $(A,B) \mapsto A \cup B$,
$(A,B) \mapsto A \cap B$, $+$

Множество 2^X, бинарная операция $(A,B) \mapsto A \setminus B$, $-$

$A = \{a\},\ B = \varnothing,\quad A \setminus B = A \quad ,\ B \setminus A = \varnothing.$

В случае конечных множеств бинарная операция иногда задается таблицей Кэли.

Множество $\mathbb{Z}_5^* = \{1,2,3,4\}$, бинарная операция $(a,b) \mapsto (ab) \bmod 5$.

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Бинарная операция

Коммутативность

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a,b) = (b,a),\ [a,b] = [b,a],\ +$$

Множество 2^X, бинарные операции $(A,B) \mapsto A \cup B$,
$(A,B) \mapsto A \cap B$, $+$

Множество 2^X, бинарная операция $(A,B) \mapsto A \setminus B$, $-$

$A = \{a\},\ B = \varnothing,\quad A \setminus B = A \quad ,\ B \setminus A = \varnothing.$

В случае конечных множеств бинарная операция иногда задается таблицей Кэли.

Множество $\mathbb{Z}_5^* = \{1,2,3,4\}$, бинарная операция $(a,b) \mapsto (ab) \bmod 5$.

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

Бинарная операция

Коммутативность

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a,b) = (b,a),\ [a,b] = [b,a],\ +$$

Множество 2^X, бинарные операции $(A,B) \mapsto A \cup B$,
$(A,B) \mapsto A \cap B$, $+$

Множество 2^X, бинарная операция $(A,B) \mapsto A \setminus B$, $-$

$A = \{a\},\ B = \varnothing,\quad A \setminus B = A \quad,\ B \setminus A = \varnothing.$

В случае конечных множеств бинарная операция иногда задается таблицей Кэли.

Множество $\mathbb{Z}_5^* = \{1,2,3,4\}$, бинарная операция $(a,b) \mapsto (ab) \bmod 5$.

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

Операция коммутативная.

Определение

Бинарная операция, определенная на множестве X, называется ассоциативной, если для любых элементов a, b, $c \in X$ выполняется равенство $(a * b) * c = a * (b * c)$.

Определение

Бинарная операция, определенная на множестве X, называется ассоциативной, если для любых элементов a, b, $c \in X$ выполняется равенство $(a * b) * c = a * (b * c)$.

Анализ ассоциативности.

Определение

Бинарная операция, определенная на множестве X, называется ассоциативной, если для любых элементов a, b, $c \in X$ выполняется равенство $(a * b) * c = a * (b * c)$.

Анализ ассоциативности.
$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение.

Определение

Бинарная операция, определенная на множестве X, называется ассоциативной, если для любых элементов a, b, $c \in X$ выполняется равенство $(a * b) * c = a * (b * c)$.

Анализ ассоциативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

Определение

Бинарная операция, определенная на множестве X, называется ассоциативной, если для любых элементов a, b, $c \in X$ выполняется равенство $(a * b) * c = a * (b * c)$.

Анализ ассоциативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение.

Определение

Бинарная операция, определенная на множестве X, называется ассоциативной, если для любых элементов a, b, $c \in X$ выполняется равенство $(a * b) * c = a * (b * c)$.

Анализ ассоциативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

Определение

Бинарная операция, определенная на множестве X, называется ассоциативной, если для любых элементов a, b, $c \in X$ выполняется равенство $(a * b) * c = a * (b * c)$.

Анализ ассоциативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

Определение

Бинарная операция, определенная на множестве X, называется ассоциативной, если для любых элементов a, b, $c \in X$ выполняется равенство $(a * b) * c = a * (b * c)$.

Анализ ассоциативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

$$(a - b) - c = a - (b - c)$$

Определение

Бинарная операция, определенная на множестве X, называется ассоциативной, если для любых элементов a, b, $c \in X$ выполняется равенство $(a * b) * c = a * (b * c)$.

Анализ ассоциативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

$$(a - b) - c = a - (b - c)\,,\ a - b - c = a - b + c$$

Определение

Бинарная операция, определенная на множестве X, называется ассоциативной, если для любых элементов a, b, $c \in X$ выполняется равенство $(a * b) * c = a * (b * c)$.

Анализ ассоциативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

$$(a-b)-c = a-(b-c)\,,\ a-b-c = a-b+c\,,\ 2c = 0,\ c = 0.$$

Определение

Бинарная операция, определенная на множестве X, называется ассоциативной, если для любых элементов a, b, $c \in X$ выполняется равенство $(a * b) * c = a * (b * c)$.

Анализ ассоциативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

$(a - b) - c = a - (b - c)$, $a - b - c = a - b + c$, $2c = 0$, $c = 0$. $-$

Определение

Бинарная операция, определенная на множестве X, называется ассоциативной, если для любых элементов a, b, $c \in X$ выполняется равенство $(a * b) * c = a * (b * c)$.

Анализ ассоциативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

$(a - b) - c = a - (b - c)$, $a - b - c = a - b + c$, $2c = 0$, $c = 0$. $-$

$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $(a, b) \mapsto a : b$.

Определение

Бинарная операция, определенная на множестве X, называется ассоциативной, если для любых элементов a, b, $c \in X$ выполняется равенство $(a * b) * c = a * (b * c)$.

Анализ ассоциативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

$(a - b) - c = a - (b - c)$, $a - b - c = a - b + c$, $2c = 0$, $c = 0$. $-$

$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $(a, b) \mapsto a : b$.

$$(a : b) : c = a : (b : c)$$

Определение

Бинарная операция, определенная на множестве X, называется ассоциативной, если для любых элементов a, b, $c \in X$ выполняется равенство $(a * b) * c = a * (b * c)$.

Анализ ассоциативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

$(a-b)-c = a-(b-c)$, $a-b-c = a-b+c$, $2c = 0$, $c = 0$. $-$

$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $(a, b) \mapsto a : b$.

$(a : b) : c = a : (b : c)$, $\dfrac{\frac{a}{b}}{c} = \dfrac{a}{\frac{b}{c}}$

Определение

Бинарная операция, определенная на множестве X, называется ассоциативной, если для любых элементов a, b, $c \in X$ выполняется равенство $(a * b) * c = a * (b * c)$.

Анализ ассоциативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

$(a-b)-c=a-(b-c)$, $a-b-c=a-b+c$, $2c=0$, $c=0$. $-$

$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $(a,b) \mapsto a:b$.

$(a:b):c=a:(b:c)$, $\dfrac{\frac{a}{b}}{c} = \dfrac{a}{\frac{b}{c}}$, $\dfrac{a}{bc} = \dfrac{ac}{b}$

Определение

Бинарная операция, определенная на множестве X, называется ассоциативной, если для любых элементов a, b, $c \in X$ выполняется равенство $(a * b) * c = a * (b * c)$.

Анализ ассоциативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

$(a - b) - c = a - (b - c)$, $a - b - c = a - b + c$, $2c = 0$, $c = 0$. $-$

$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $(a, b) \mapsto a : b$.

$(a : b) : c = a : (b : c)$, $\dfrac{\frac{a}{b}}{c} = \dfrac{a}{\frac{b}{c}}$, $\dfrac{a}{bc} = \dfrac{ac}{b}$, $c^2 = 1$

Определение

Бинарная операция, определенная на множестве X, называется ассоциативной, если для любых элементов a, b, $c \in X$ выполняется равенство $(a * b) * c = a * (b * c)$.

Анализ ассоциативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

$(a-b)-c = a-(b-c)$, $a-b-c = a-b+c$, $2c = 0$, $c = 0$. $-$

$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $(a, b) \mapsto a : b$.

$(a : b) : c = a : (b : c)$, $\dfrac{\frac{a}{b}}{c} = \dfrac{a}{\frac{b}{c}}$, $\dfrac{a}{bc} = \dfrac{ac}{b}$, $c^2 = 1$, $c = \pm 1$. $-$

Определение

Бинарная операция, определенная на множестве X, называется ассоциативной, если для любых элементов a, b, $c \in X$ выполняется равенство $(a * b) * c = a * (b * c)$.

Анализ ассоциативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

$(a-b)-c = a-(b-c)$, $a-b-c = a-b+c$, $2c = 0$, $c = 0$. $-$

$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $(a, b) \mapsto a : b$.

$(a : b) : c = a : (b : c)$, $\dfrac{\frac{a}{b}}{c} = \dfrac{a}{\frac{b}{c}}$, $\dfrac{a}{bc} = \dfrac{ac}{b}$, $c^2 = 1$, $c = \pm 1$. $-$

Множество всех квадратных матриц фиксированного размера с операцией умножения

Определение

Бинарная операция, определенная на множестве X, называется ассоциативной, если для любых элементов a, b, $c \in X$ выполняется равенство $(a * b) * c = a * (b * c)$.

Анализ ассоциативности.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — сложение. $+$

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — умножение. $+$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — вычитание.

$(a-b)-c = a-(b-c)$, $a-b-c = a-b+c$, $2c = 0$, $c = 0$. $-$

$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $(a,b) \mapsto a : b$.

$(a:b):c = a:(b:c)$, $\dfrac{\frac{a}{b}}{c} = \dfrac{a}{\frac{b}{c}}$, $\dfrac{a}{bc} = \dfrac{ac}{b}$, $c^2 = 1$, $c = \pm 1$. $-$

Множество всех квадратных матриц фиксированного размера с операцией умножения , операция ассоциативная.

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a, b, c) = ((a, b), c) = (a, (b, c))$$

Бинарная операция

Ассоциативность

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a, b, c) = ((a, b), c) = (a, (b, c)) \ , \ +$$

Бинарная операция

Ассоциативность

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a, b, c) = ((a, b), c) = (a, (b, c)) \ , +$$
$$[a, b, c] = [[a, b], c] = [a, [b, c]]$$

Бинарная операция

Ассоциативность

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a, b, c) = ((a, b), c) = (a, (b, c)) \ , +$$
$$[a, b, c] = [[a, b], c] = [a, [b, c]] \ , +$$

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a, b, c) = ((a, b), c) = (a, (b, c)) \ , +$$
$$[a, b, c] = [[a, b], c] = [a, [b, c]] \ , +$$

Множество 2^X, бинарные операции $(A, B) \mapsto A \cup B$, $(A, B) \mapsto A \cap B$

Бинарная операция

Ассоциативность

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a, b, c) = ((a, b), c) = (a, (b, c)) \ , +$$
$$[a, b, c] = [[a, b], c] = [a, [b, c]] \ , +$$

Множество 2^X, бинарные операции $(A, B) \mapsto A \cup B$, $(A, B) \mapsto A \cap B$, $+$

Бинарная операция

Ассоциативность

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a, b, c) = ((a, b), c) = (a, (b, c)) \ , +$$
$$[a, b, c] = [[a, b], c] = [a, [b, c]] \ , +$$

Множество 2^X, бинарные операции $(A, B) \mapsto A \cup B$, $(A, B) \mapsto A \cap B$, $+$

Множество 2^X, бинарная операция $(A, B) \mapsto A \setminus B$

Бинарная операция

Ассоциативность

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a, b, c) = ((a, b), c) = (a, (b, c)) \ , \ +$$
$$[a, b, c] = [[a, b], c] = [a, [b, c]] \ , \ +$$

Множество 2^X, бинарные операции $(A, B) \mapsto A \cup B$, $(A, B) \mapsto A \cap B$, $+$

Множество 2^X, бинарная операция $(A, B) \mapsto A \setminus B$, $-$

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a, b, c) = ((a, b), c) = (a, (b, c)) \ , \ +$$
$$[a, b, c] = [[a, b], c] = [a, [b, c]] \ , \ +$$

Множество 2^X, бинарные операции $(A, B) \mapsto A \cup B$, $(A, B) \mapsto A \cap B$, $+$

Множество 2^X, бинарная операция $(A, B) \mapsto A \setminus B$, $-$

$$A = B = C = \{x\}$$

Бинарная операция

Ассоциативность

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a, b, c) = ((a, b), c) = (a, (b, c)) \ , +$$

$$[a, b, c] = [[a, b], c] = [a, [b, c]] \ , +$$

Множество 2^X, бинарные операции $(A, B) \mapsto A \cup B$,
$(A, B) \mapsto A \cap B$, $+$

Множество 2^X, бинарная операция $(A, B) \mapsto A \setminus B$, $-$

$$A = B = C = \{x\}$$

$$(A \setminus B) \setminus C = \varnothing \setminus C = \varnothing$$

Бинарная операция

Ассоциативность

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a, b, c) = ((a, b), c) = (a, (b, c)) \ , +$$

$$[a, b, c] = [[a, b], c] = [a, [b, c]] \ , +$$

Множество 2^X, бинарные операции $(A, B) \mapsto A \cup B$, $(A, B) \mapsto A \cap B$, $+$

Множество 2^X, бинарная операция $(A, B) \mapsto A \setminus B$, $-$

$$A = B = C = \{x\}$$

$$(A \setminus B) \setminus C = \varnothing \setminus C = \varnothing$$

$$A \setminus (B \setminus C) = A \setminus \varnothing = A$$

Множество $\mathbb{N}$, бинарные операции «наибольший общий делитель» и «наименьшее общее кратное».

$$(a, b, c) = ((a, b), c) = (a, (b, c)) \ , +$$

$$[a, b, c] = [[a, b], c] = [a, [b, c]] \ , +$$

Множество 2^X, бинарные операции $(A, B) \mapsto A \cup B$,
$(A, B) \mapsto A \cap B$, $+$

Множество 2^X, бинарная операция $(A, B) \mapsto A \setminus B$, $-$

$$A = B = C = \{x\}$$

$$(A \setminus B) \setminus C = \varnothing \setminus C = \varnothing$$

$$A \setminus (B \setminus C) = A \setminus \varnothing = A$$

$(A \setminus B) \setminus C \neq A \setminus (B \setminus C)$, операция неассоциативная.

Бинарная операция

Ассоциативность

Множество всех обратимых квадратных матриц фиксированного порядка с вещественными коэффициентами, бинарная операция $(A, B) \mapsto AB^{-1}$.

Бинарная операция

Ассоциативность

Множество всех обратимых квадратных матриц фиксированного порядка с вещественными коэффициентами, бинарная операция $(A, B) \mapsto AB^{-1}$.
Операция неассоциативная, можно рассмотреть скалярные матрицы aE.

Бинарная операция

Ассоциативность

Множество всех обратимых квадратных матриц фиксированного порядка с вещественными коэффициентами, бинарная операция $(A, B) \mapsto AB^{-1}$.
Операция неассоциативная, можно рассмотреть скалярные матрицы aE.

$$A = aE, B = bE \Rightarrow AB^{-1} = (a : b)E.$$

Множество всех обратимых квадратных матриц фиксированного порядка с вещественными коэффициентами, бинарная операция $(A, B) \mapsto AB^{-1}$.
Операция неассоциативная, можно рассмотреть скалярные матрицы aE.

$$A = aE, B = bE \Rightarrow AB^{-1} = (a : b)E.$$

$$A = aE, B = bE, C = cE, (AB^{-1})C^{-1} = A(BC^{-1})$$

Бинарная операция

Ассоциативность

Множество всех обратимых квадратных матриц фиксированного порядка с вещественными коэффициентами, бинарная операция $(A, B) \mapsto AB^{-1}$.
Операция неассоциативная, можно рассмотреть скалярные матрицы aE.

$$A = aE, B = bE \Rightarrow AB^{-1} = (a : b)E.$$

$$A = aE, B = bE, C = cE, (AB^{-1})C^{-1} = A(BC^{-1})$$

$$(a : b) : c = a : (b : c)$$

Бинарная операция

Ассоциативность

Множество всех обратимых квадратных матриц фиксированного порядка с вещественными коэффициентами, бинарная операция $(A, B) \mapsto AB^{-1}$.
Операция неассоциативная, можно рассмотреть скалярные матрицы aE.

$$A = aE, B = bE \Rightarrow AB^{-1} = (a : b)E.$$

$$A = aE, B = bE, C = cE, (AB^{-1})C^{-1} = A(BC^{-1})$$

$$(a : b) : c = a : (b : c)$$

Операция векторного умножения геометрических векторов.

Бинарная операция

Ассоциативность

Множество всех обратимых квадратных матриц фиксированного порядка с вещественными коэффициентами, бинарная операция $(A, B) \mapsto AB^{-1}$.
Операция неассоциативная, можно рассмотреть скалярные матрицы aE.

$$A = aE, B = bE \Rightarrow AB^{-1} = (a : b)E.$$

$$A = aE, B = bE, C = cE, (AB^{-1})C^{-1} = A(BC^{-1})$$

$$(a : b) : c = a : (b : c)$$

Операция векторного умножения геометрических векторов.
Берем стандартный ортонормированный базис $\vec{i}$, $\vec{j}$, $\vec{k}$.

Бинарная операция

Ассоциативность

Множество всех обратимых квадратных матриц фиксированного порядка с вещественными коэффициентами, бинарная операция $(A, B) \mapsto AB^{-1}$.
Операция неассоциативная, можно рассмотреть скалярные матрицы aE.

$$A = aE, B = bE \Rightarrow AB^{-1} = (a : b)E.$$

$$A = aE, B = bE, C = cE, (AB^{-1})C^{-1} = A(BC^{-1})$$

$$(a : b) : c = a : (b : c)$$

Операция векторного умножения геометрических векторов.
Берем стандартный ортонормированный базис $\vec{i}$, $\vec{j}$, $\vec{k}$.

$$\underbrace{(\vec{i} \times \vec{i})}_{\vec{0}} \times \vec{j} = \vec{0} \times \vec{j} = \vec{0}$$

Бинарная операция

Ассоциативность

Множество всех обратимых квадратных матриц фиксированного порядка с вещественными коэффициентами, бинарная операция $(A, B) \mapsto AB^{-1}$.
Операция неассоциативная, можно рассмотреть скалярные матрицы aE.

$$A = aE, B = bE \Rightarrow AB^{-1} = (a : b)E.$$

$$A = aE, B = bE, C = cE, (AB^{-1})C^{-1} = A(BC^{-1})$$

$$(a : b) : c = a : (b : c)$$

Операция векторного умножения геометрических векторов.
Берем стандартный ортонормированный базис $\vec{i}$, $\vec{j}$, $\vec{k}$.

$$\underbrace{(\vec{i} \times \vec{i})}_{\vec{0}} \times \vec{j} = \vec{0} \times \vec{j} = \vec{0}\ ,\ \vec{i} \times \underbrace{(\vec{i} \times \vec{j})}_{\vec{k}} = \vec{i} \times \vec{k} = -\vec{j}.$$

Бинарная операция

Ассоциативность

Множество всех обратимых квадратных матриц фиксированного порядка с вещественными коэффициентами, бинарная операция $(A, B) \mapsto AB^{-1}$.
Операция неассоциативная, можно рассмотреть скалярные матрицы aE.

$$A = aE, B = bE \Rightarrow AB^{-1} = (a : b)E.$$

$$A = aE, B = bE, C = cE, (AB^{-1})C^{-1} = A(BC^{-1})$$

$$(a : b) : c = a : (b : c)$$

Операция векторного умножения геометрических векторов.
Берем стандартный ортонормированный базис $\vec{i}$, $\vec{j}$, $\vec{k}$.

$$\underbrace{(\vec{i} \times \vec{i})}_{\vec{0}} \times \vec{j} = \vec{0} \times \vec{j} = \vec{0}\ ,\ \vec{i} \times \underbrace{(\vec{i} \times \vec{j})}_{\vec{k}} = \vec{i} \times \vec{k} = -\vec{j}.$$

Операция неассоциативная.