

## *Лекция 7*

Неразрешимость исчисления предикатов  
Аксиоматика Пеано и формальная арифметика

# Машина Тьюринга

## Определение

*Машина Тьюринга — упорядоченная тройка:*

1. *Внешний алфавит  $q_1, \dots, q_n$*
2. *Внутренний алфавит (состояний)  $s_1, \dots, s_k$ ;  $s_s$  — начальное,  $s_f$  — конечное.*
3. *Таблица переходов  $\langle k, s \rangle \Rightarrow \langle k', s', \leftrightarrow \rangle$*

## Определение

*Состояние машины Тьюринга — упорядоченная тройка:*

1. *Бесконечная лента с символом-заполнителем  $q_\epsilon$ , текст конечной длины.*
2. *Головка над определённым символом*
3. *Символ состояния (состояние в узком смысле) — символ внутреннего алфавита.*

## Машина, меняющая все 0 на 1, а все 1 — на 0

1. Внешний алфавит  $\varepsilon, 0, 1$ .
2. Внутренний алфавит  $s_s, s_f$  (начальное и завершающее состояния соответственно).
3. Переходы:

	$\varepsilon$	0	1
$s_s$	$\langle s_f, \varepsilon, \cdot \rangle$	$\langle s_s, 1, \rightarrow \rangle$	$\langle s_s, 0, \rightarrow \rangle$
$s_f$	$\langle s_f, \varepsilon, \cdot \rangle$	$\langle s_f, 0, \cdot \rangle$	$\langle s_f, 1, \cdot \rangle$

## Машина, меняющая все 0 на 1, а все 1 — на 0

1. Внешний алфавит  $\varepsilon, 0, 1$ .
2. Внутренний алфавит  $s_s, s_f$  (начальное и завершающее состояния соответственно).
3. Переходы:

	$\varepsilon$	0	1
$s_s$	$\langle s_f, \varepsilon, \cdot \rangle$	$\langle s_s, 1, \rightarrow \rangle$	$\langle s_s, 0, \rightarrow \rangle$
$s_f$	$\langle s_f, \varepsilon, \cdot \rangle$	$\langle s_f, 0, \cdot \rangle$	$\langle s_f, 1, \cdot \rangle$

### Пример

Головка — на первом символе 011, состояние  $s_s$ .

## Машина, меняющая все 0 на 1, а все 1 — на 0

1. Внешний алфавит  $\varepsilon, 0, 1$ .
2. Внутренний алфавит  $s_s, s_f$  (начальное и завершающее состояния соответственно).
3. Переходы:

	$\varepsilon$	0	1
$s_s$	$\langle s_f, \varepsilon, \cdot \rangle$	$\langle s_s, 1, \rightarrow \rangle$	$\langle s_s, 0, \rightarrow \rangle$
$s_f$	$\langle s_f, \varepsilon, \cdot \rangle$	$\langle s_f, 0, \cdot \rangle$	$\langle s_f, 1, \cdot \rangle$

### Пример

Головка — на первом символе 011, состояние  $s_s$ .

011

## Машина, меняющая все 0 на 1, а все 1 — на 0

1. Внешний алфавит  $\varepsilon, 0, 1$ .
2. Внутренний алфавит  $s_s, s_f$  (начальное и завершающее состояния соответственно).
3. Переходы:

	$\varepsilon$	0	1
$s_s$	$\langle s_f, \varepsilon, \cdot \rangle$	$\langle s_s, 1, \rightarrow \rangle$	$\langle s_s, 0, \rightarrow \rangle$
$s_f$	$\langle s_f, \varepsilon, \cdot \rangle$	$\langle s_f, 0, \cdot \rangle$	$\langle s_f, 1, \cdot \rangle$

### Пример

Головка — на первом символе 011, состояние  $s_s$ .

011  $\Rightarrow$  111

## Машина, меняющая все 0 на 1, а все 1 — на 0

1. Внешний алфавит  $\varepsilon, 0, 1$ .
2. Внутренний алфавит  $s_s, s_f$  (начальное и завершающее состояния соответственно).
3. Переходы:

	$\varepsilon$	0	1
$s_s$	$\langle s_f, \varepsilon, \cdot \rangle$	$\langle s_s, 1, \rightarrow \rangle$	$\langle s_s, 0, \rightarrow \rangle$
$s_f$	$\langle s_f, \varepsilon, \cdot \rangle$	$\langle s_f, 0, \cdot \rangle$	$\langle s_f, 1, \cdot \rangle$

### Пример

Головка — на первом символе 011, состояние  $s_s$ .

011  $\Rightarrow$  111  $\Rightarrow$  101

## Машина, меняющая все 0 на 1, а все 1 — на 0

1. Внешний алфавит  $\varepsilon, 0, 1$ .
2. Внутренний алфавит  $s_s, s_f$  (начальное и завершающее состояния соответственно).
3. Переходы:

	$\varepsilon$	0	1
$s_s$	$\langle s_f, \varepsilon, \cdot \rangle$	$\langle s_s, 1, \rightarrow \rangle$	$\langle s_s, 0, \rightarrow \rangle$
$s_f$	$\langle s_f, \varepsilon, \cdot \rangle$	$\langle s_f, 0, \cdot \rangle$	$\langle s_f, 1, \cdot \rangle$

### Пример

Головка — на первом символе 011, состояние  $s_s$ .

011  $\Rightarrow$  111  $\Rightarrow$  101  $\Rightarrow$  100 $\varepsilon$



## Машина, меняющая все 0 на 1, а все 1 — на 0

1. Внешний алфавит  $\varepsilon, 0, 1$ .
2. Внутренний алфавит  $s_s, s_f$  (начальное и завершающее состояния соответственно).
3. Переходы:

	$\varepsilon$	0	1
$s_s$	$\langle s_f, \varepsilon, \cdot \rangle$	$\langle s_s, 1, \rightarrow \rangle$	$\langle s_s, 0, \rightarrow \rangle$
$s_f$	$\langle s_f, \varepsilon, \cdot \rangle$	$\langle s_f, 0, \cdot \rangle$	$\langle s_f, 1, \cdot \rangle$

### Пример

Головка — на первом символе 011, состояние  $s_s$ .

011  $\Rightarrow$  111  $\Rightarrow$  101  $\Rightarrow$  100 $\varepsilon$

Состояние  $s_f$ , завершающее.

# Разрешимость

## Определение

*Язык — множество строк*

## Определение

*Язык  $L$  разрешим, если существует машина Тьюринга, которая для любого слова  $w$  возвращает ответ «да», если  $w \in L$ , и «нет», если  $w \notin L$ .*

# Неразрешимость задачи останова

## Определение

*Рассмотрим все возможные описания машин Тьюринга. Составим упорядоченные пары: описание машины Тьюринга и входная строка. Из них выделим язык останавливающихся на данном входе машин Тьюринга.*

## Теорема

*Язык всех останавливающихся машин Тьюринга неразрешим*

## Доказательство.

От противного. Пусть  $S(x, y)$  — машина Тьюринга, определяющая, остановится ли машина  $x$ , примененная к строке  $y$ .

# Неразрешимость задачи останова

## Определение

*Рассмотрим все возможные описания машин Тьюринга. Составим упорядоченные пары: описание машины Тьюринга и входная строка. Из них выделим язык останавливающихся на данном входе машин Тьюринга.*

## Теорема

*Язык всех останавливающихся машин Тьюринга неразрешим*

## Доказательство.

От противного. Пусть  $S(x, y)$  — машина Тьюринга, определяющая, остановится ли машина  $x$ , примененная к строке  $y$ .

$$W(x) = \text{if } (S(x,x)) \{ \text{while (true); return 0; } \} \text{ else } \{ \text{return 1; } \}$$

# Неразрешимость задачи останова

## Определение

*Рассмотрим все возможные описания машин Тьюринга. Составим упорядоченные пары: описание машины Тьюринга и входная строка. Из них выделим язык останавливающихся на данном входе машин Тьюринга.*

## Теорема

*Язык всех останавливающихся машин Тьюринга неразрешим*

## Доказательство.

От противного. Пусть  $S(x, y)$  — машина Тьюринга, определяющая, остановится ли машина  $x$ , примененная к строке  $y$ .

$$W(x) = \text{if } (S(x, x)) \{ \text{while } (\text{true}); \text{return } 0; \} \text{ else } \{ \text{return } 1; \}$$

Что вернёт  $S(\text{code}(W), \text{code}(W))$ ?



## Кодируем состояние

1. внешний алфавит:  $n$  0-местных функциональных символов  $q_1, \dots, q_n$ ;  $q_\varepsilon$  — символ-заполнитель.
2. список:  $\varepsilon$  и  $c(l, s)$ ; «abc» представим как  $c(q_a, c(q_b, c(q_c, \varepsilon)))$ .
3. положение головки: «ab.pq» как  $(c(q_b, c(q_a, \varepsilon)), c(q_p, c(q_q, \varepsilon)))$ .
4. внутренний алфавит:  $k$  0-местных функциональных символов  $s_1, \dots, s_k$ . Из них выделенные  $s_s$  — начальное и  $s_f$  — завершающее состояние.

## Достижимые состояния

Предикатный символ  $F_{x,y}(w_l, w_r, s)$ : если у машины  $x$  с начальной строкой  $y$  состояние  $s$  достижимо на строке  $rev(w_l)@w_r$ .

## Достижимые состояния

Предикатный символ  $F_{x,y}(w_l, w_r, s)$ : если у машины  $x$  с начальной строкой  $y$  состояние  $s$  достижимо на строке  $\text{rev}(w_l)@w_r$ . Будем накладывать условия: семейство формул  $C_m$ .



## Достижимые состояния

Предикатный символ  $F_{x,y}(w_l, w_r, s)$ : если у машины  $x$  с начальной строкой  $y$  состояние  $s$  достижимо на строке  $rev(w_l)@w_r$ . Будем накладывать условия: семейство формул  $C_m$ . Очевидно, начальное состояние достижимо:

$$C_0 = F_{x,y}(\varepsilon, x, s_s)$$

# Кодируем переходы

1. Занумеруем переходы.

## Кодируем переходы

1. Занумеруем переходы.
2. Закодируем переход  $m$ :

$$\langle k, s \rangle \Rightarrow \langle k', s', \rightarrow \rangle$$

$$C_m = \forall w_l. \forall w_r. F_{x,y}(w_l, c(q_k, w_r), s_s) \rightarrow F_{x,y}(c(q_{k'}, w_l), w_r, s_{s'})$$

## Кодируем переходы

1. Занумеруем переходы.
2. Закодируем переход  $m$ :

$$\langle k, s \rangle \Rightarrow \langle k', s', \rightarrow \rangle$$

$$C_m = \forall w_l. \forall w_r. F_{x,y}(w_l, c(q_k, w_r), s_s) \rightarrow F_{x,y}(c(q_{k'}, w_l), w_r, s_{s'})$$

3. Переход посложнее:

$$\langle k, s \rangle \Rightarrow \langle k', s', \leftarrow \rangle$$

$$C_m = \forall w_l. \forall w_r. \forall t. F_{x,y}(c(t, w_l), c(q_k, w_r), s_s) \rightarrow F_{x,y}(w_l, c(t, c(q_{k'}, w_r)), s_{s'}) \ \& \\ \forall w_l. \forall w_r. F_{x,y}(\varepsilon, c(q_k, w_r), s_s) \rightarrow F_{x,y}(\varepsilon, c(q_{\varepsilon}, c(q_{k'}, w_r)), s_{s'})$$

## Кодируем переходы

1. Занумеруем переходы.
2. Закодируем переход  $m$ :

$$\langle k, s \rangle \Rightarrow \langle k', s', \rightarrow \rangle$$

$$C_m = \forall w_l. \forall w_r. F_{x,y}(w_l, c(q_k, w_r), s_s) \rightarrow F_{x,y}(c(q_{k'}, w_l), w_r, s_{s'})$$

3. Переход посложнее:

$$\langle k, s \rangle \Rightarrow \langle k', s', \leftarrow \rangle$$

$$C_m = \forall w_l. \forall w_r. \forall t. F_{x,y}(c(t, w_l), c(q_k, w_r), s_s) \rightarrow F_{x,y}(w_l, c(t, c(q_{k'}, w_r)), s_{s'}) \ \& \\ \forall w_l. \forall w_r. F_{x,y}(\varepsilon, c(q_k, w_r), s_s) \rightarrow F_{x,y}(\varepsilon, c(q_{\varepsilon}, c(q_{k'}, w_r)), s_{s'})$$

4. и т.п.

## Итоговая формула

$$C = C_0 \& C_1 \& \dots \& C_n$$

«правильное начальное состояние и правильные переходы между состояниями»

## Итоговая формула

$$C = C_0 \& C_1 \& \dots \& C_n$$

«правильное начальное состояние и правильные переходы между состояниями»

### Теорема

*состояние  $s$  со строкой  $rev(w_l)@w_r$  достижимо тогда и только тогда, когда*  
 $C \vdash F_{x,y}(w_l, w_r, s)$

## Итоговая формула

$$C = C_0 \& C_1 \& \dots \& C_n$$

«правильное начальное состояние и правильные переходы между состояниями»

### Теорема

*состояние  $s$  со строкой  $rev(w_l)@w_r$  достижимо тогда и только тогда, когда*  
 $C \vdash F_{x,y}(w_l, w_r, s)$

### Доказательство.

$(\Leftarrow)$  Рассмотрим модель: предикат  $F_{x,y}(w_l, w_r, s)$  положим истинным, если состояние достижимо.



## Итоговая формула

$$C = C_0 \& C_1 \& \dots \& C_n$$

«правильное начальное состояние и правильные переходы между состояниями»

### Теорема

*состояние  $s$  со строкой  $rev(w_l)@w_r$  достижимо тогда и только тогда, когда*  
 $C \vdash F_{x,y}(w_l, w_r, s)$

### Доказательство.

$(\Leftarrow)$  Рассмотрим модель: предикат  $F_{x,y}(w_l, w_r, s)$  положим истинным, если состояние достижимо. Это — модель для  $C$  (по построению  $C_m$ ).

## Итоговая формула

$$C = C_0 \& C_1 \& \dots \& C_n$$

«правильное начальное состояние и правильные переходы между состояниями»

### Теорема

*состояние  $s$  со строкой  $rev(w_l)@w_r$  достижимо тогда и только тогда, когда*  
 $C \vdash F_{x,y}(w_l, w_r, s)$

### Доказательство.

( $\Leftarrow$ ) Рассмотрим модель: предикат  $F_{x,y}(w_l, w_r, s)$  положим истинным, если состояние достижимо. Это — модель для  $C$  (по построению  $C_m$ ). Значит, доказуемость влечёт истинность (по корректности).

## Итоговая формула

$$C = C_0 \& C_1 \& \dots \& C_n$$

«правильное начальное состояние и правильные переходы между состояниями»

### Теорема

*состояние  $s$  со строкой  $rev(w_l)@w_r$  достижимо тогда и только тогда, когда*  
 $C \vdash F_{x,y}(w_l, w_r, s)$

### Доказательство.

( $\Leftarrow$ ) Рассмотрим модель: предикат  $F_{x,y}(w_l, w_r, s)$  положим истинным, если состояние достижимо. Это — модель для  $C$  (по построению  $C_m$ ). Значит, доказуемость влечёт истинность (по корректности).

( $\Rightarrow$ ) Индукция по длине лога исполнения.



# Неразрешимость исчисления предикатов: доказательство

## Теорема

*Язык всех доказуемых формул исчисления предикатов неразрешим*

Т.е. нет машины Тьюринга, которая бы по любой формуле  $s$  определяла, доказуема ли она.

# Неразрешимость исчисления предикатов: доказательство

## Теорема

*Язык всех доказуемых формул исчисления предикатов неразрешим*

Т.е. нет машины Тьюринга, которая бы по любой формуле  $s$  определяла, доказуема ли она.

## Доказательство.

$s_f$  — завершающее состояние.

# Неразрешимость исчисления предикатов: доказательство

## Теорема

*Язык всех доказуемых формул исчисления предикатов неразрешим*

Т.е. нет машины Тьюринга, которая бы по любой формуле  $s$  определяла, доказуема ли она.

## Доказательство.

$s_f$  — завершающее состояние.

Умение определять истинность формулы  $\exists w_l. \exists w_r. F_{x,y}(w_l, w_r, s_f)$  разрешает задачу останова. □

# Аксиоматика Пеано и формальная арифметика

# Какие мы знаем числа?

1. Вещественные ( $\mathbb{R}$ ).



## Какие мы знаем числа?

1. Вещественные ( $\mathbb{R}$ ).  $X = \{A, B\}$ , где  $A, B \subseteq \mathbb{Q}$  — дедекиндово сечение, если:

# Какие мы знаем числа?

1. Вещественные ( $\mathbb{R}$ ).  $X = \{A, B\}$ , где  $A, B \subseteq \mathbb{Q}$  — дедекиндово сечение, если:

1.1  $A \cup B = \mathbb{Q}$

# Какие мы знаем числа?

1. Вещественные ( $\mathbb{R}$ ).  $X = \{A, B\}$ , где  $A, B \subseteq \mathbb{Q}$  — дедекиндово сечение, если:
  - 1.1  $A \cup B = \mathbb{Q}$
  - 1.2 Если  $a \in A$ ,  $x \in \mathbb{Q}$  и  $x \leq a$ , то  $x \in A$

## Какие мы знаем числа?

1. Вещественные ( $\mathbb{R}$ ).  $X = \{A, B\}$ , где  $A, B \subseteq \mathbb{Q}$  — дедекиндово сечение, если:
  - 1.1  $A \cup B = \mathbb{Q}$
  - 1.2 Если  $a \in A$ ,  $x \in \mathbb{Q}$  и  $x \leq a$ , то  $x \in A$
  - 1.3 Если  $b \in B$ ,  $x \in \mathbb{Q}$  и  $b \leq x$ , то  $x \in B$

## Какие мы знаем числа?

1. Вещественные ( $\mathbb{R}$ ).  $X = \{A, B\}$ , где  $A, B \subseteq \mathbb{Q}$  — дедекиндово сечение, если:
  - 1.1  $A \cup B = \mathbb{Q}$
  - 1.2 Если  $a \in A$ ,  $x \in \mathbb{Q}$  и  $x \leq a$ , то  $x \in A$
  - 1.3 Если  $b \in B$ ,  $x \in \mathbb{Q}$  и  $b \leq x$ , то  $x \in B$
  - 1.4  $A$  не содержит наибольшего.

## Какие мы знаем числа?

1. Вещественные ( $\mathbb{R}$ ).  $X = \{A, B\}$ , где  $A, B \subseteq \mathbb{Q}$  — дедекиндово сечение, если:

1.1  $A \cup B = \mathbb{Q}$

1.2 Если  $a \in A$ ,  $x \in \mathbb{Q}$  и  $x \leq a$ , то  $x \in A$

1.3 Если  $b \in B$ ,  $x \in \mathbb{Q}$  и  $b \leq x$ , то  $x \in B$

1.4  $A$  не содержит наибольшего.

$\mathbb{R}$  — множество всех возможных дедекиндовых сечений.

## Какие мы знаем числа?

1. Вещественные ( $\mathbb{R}$ ).  $X = \{A, B\}$ , где  $A, B \subseteq \mathbb{Q}$  — дедекиндово сечение, если:

1.1  $A \cup B = \mathbb{Q}$

1.2 Если  $a \in A$ ,  $x \in \mathbb{Q}$  и  $x \leq a$ , то  $x \in A$

1.3 Если  $b \in B$ ,  $x \in \mathbb{Q}$  и  $b \leq x$ , то  $x \in B$

1.4  $A$  не содержит наибольшего.

$\mathbb{R}$  — множество всех возможных дедекиндовых сечений.

2. Рациональные ( $\mathbb{Q}$ ).

## Какие мы знаем числа?

1. Вещественные ( $\mathbb{R}$ ).  $X = \{A, B\}$ , где  $A, B \subseteq \mathbb{Q}$  — дедекиндово сечение, если:

1.1  $A \cup B = \mathbb{Q}$

1.2 Если  $a \in A$ ,  $x \in \mathbb{Q}$  и  $x \leq a$ , то  $x \in A$

1.3 Если  $b \in B$ ,  $x \in \mathbb{Q}$  и  $b \leq x$ , то  $x \in B$

1.4  $A$  не содержит наибольшего.

$\mathbb{R}$  — множество всех возможных дедекиндовых сечений.

2. Рациональные ( $\mathbb{Q}$ ).

$Q = \mathbb{Z} \times \mathbb{N}$  — множество всех простых дробей.



## Какие мы знаем числа?

1. Вещественные ( $\mathbb{R}$ ).  $X = \{A, B\}$ , где  $A, B \subseteq \mathbb{Q}$  — дедекиндово сечение, если:

1.1  $A \cup B = \mathbb{Q}$

1.2 Если  $a \in A$ ,  $x \in \mathbb{Q}$  и  $x \leq a$ , то  $x \in A$

1.3 Если  $b \in B$ ,  $x \in \mathbb{Q}$  и  $b \leq x$ , то  $x \in B$

1.4  $A$  не содержит наибольшего.

$\mathbb{R}$  — множество всех возможных дедекиндовых сечений.

2. Рациональные ( $\mathbb{Q}$ ).

$Q = \mathbb{Z} \times \mathbb{N}$  — множество всех простых дробей.

$\langle p, q \rangle$  — то же, что  $\frac{p}{q}$

## Какие мы знаем числа?

1. Вещественные ( $\mathbb{R}$ ).  $X = \{A, B\}$ , где  $A, B \subseteq \mathbb{Q}$  — дедекиндово сечение, если:

1.1  $A \cup B = \mathbb{Q}$

1.2 Если  $a \in A$ ,  $x \in \mathbb{Q}$  и  $x \leq a$ , то  $x \in A$

1.3 Если  $b \in B$ ,  $x \in \mathbb{Q}$  и  $b \leq x$ , то  $x \in B$

1.4  $A$  не содержит наибольшего.

$\mathbb{R}$  — множество всех возможных дедекиндовых сечений.

2. Рациональные ( $\mathbb{Q}$ ).

$Q = \mathbb{Z} \times \mathbb{N}$  — множество всех простых дробей.

$\langle p, q \rangle$  — то же, что  $\frac{p}{q}$

$\langle p_1, q_1 \rangle \equiv \langle p_2, q_2 \rangle$ , если  $p_1 q_2 = p_2 q_1$

## Какие мы знаем числа?

1. Вещественные ( $\mathbb{R}$ ).  $X = \{A, B\}$ , где  $A, B \subseteq \mathbb{Q}$  — дедекиндово сечение, если:

1.1  $A \cup B = \mathbb{Q}$

1.2 Если  $a \in A$ ,  $x \in \mathbb{Q}$  и  $x \leq a$ , то  $x \in A$

1.3 Если  $b \in B$ ,  $x \in \mathbb{Q}$  и  $b \leq x$ , то  $x \in B$

1.4  $A$  не содержит наибольшего.

$\mathbb{R}$  — множество всех возможных дедекиндовых сечений.

2. Рациональные ( $\mathbb{Q}$ ).

$Q = \mathbb{Z} \times \mathbb{N}$  — множество всех простых дробей.

$\langle p, q \rangle$  — то же, что  $\frac{p}{q}$

$\langle p_1, q_1 \rangle \equiv \langle p_2, q_2 \rangle$ , если  $p_1 q_2 = p_2 q_1$

$$\mathbb{Q} = Q / \equiv$$

# Целые числа

*«Бог создал целые числа, всё остальное — дело рук человека.»*  
*Леопольд Кронеккер*

## Целые числа

*«Бог создал целые числа, всё остальное — дело рук человека.»*  
*Леопольд Кронеккер*

$$\mathbb{Z} : \dots - 3, -2, -1, 0, 1, 2, 3, \dots$$

# Целые числа

*«Бог создал целые числа, всё остальное — дело рук человека.»  
Леопольд Кронеккер*

$$\mathbb{Z} : \dots - 3, -2, -1, 0, 1, 2, 3, \dots$$

►  $Z = \{\langle x, y \rangle \mid x, y \in \mathbb{N}_0\}$

# Целые числа

*«Бог создал целые числа, всё остальное — дело рук человека.»  
Леопольд Кронеккер*

$$\mathbb{Z} : \dots - 3, -2, -1, 0, 1, 2, 3, \dots$$

- ▶  $Z = \{\langle x, y \rangle \mid x, y \in \mathbb{N}_0\}$
- ▶ Интуиция:  $\langle x, y \rangle = x - y$

# Целые числа

*«Бог создал целые числа, всё остальное — дело рук человека.»*  
Леопольд Кронеккер

$$\mathbb{Z} : \dots - 3, -2, -1, 0, 1, 2, 3, \dots$$

- ▶  $Z = \{\langle x, y \rangle \mid x, y \in \mathbb{N}_0\}$
- ▶ Интуиция:  $\langle x, y \rangle = x - y$
- ▶

$$\langle a, b \rangle + \langle c, d \rangle = \langle a + c, b + d \rangle$$



# Целые числа

*«Бог создал целые числа, всё остальное — дело рук человека.»  
Леопольд Кронеккер*

$$\mathbb{Z} : \dots - 3, -2, -1, 0, 1, 2, 3, \dots$$

- ▶  $Z = \{\langle x, y \rangle \mid x, y \in \mathbb{N}_0\}$
- ▶ Интуиция:  $\langle x, y \rangle = x - y$
- ▶

$$\begin{aligned}\langle a, b \rangle + \langle c, d \rangle &= \langle a + c, b + d \rangle \\ \langle a, b \rangle - \langle c, d \rangle &= \langle a + d, b + c \rangle\end{aligned}$$

# Целые числа

*«Бог создал целые числа, всё остальное — дело рук человека.»  
Леопольд Кронеккер*

$$\mathbb{Z} : \dots - 3, -2, -1, 0, 1, 2, 3, \dots$$

- ▶  $Z = \{\langle x, y \rangle \mid x, y \in \mathbb{N}_0\}$
- ▶ Интуиция:  $\langle x, y \rangle = x - y$
- ▶

$$\begin{aligned}\langle a, b \rangle + \langle c, d \rangle &= \langle a + c, b + d \rangle \\ \langle a, b \rangle - \langle c, d \rangle &= \langle a + d, b + c \rangle\end{aligned}$$

- ▶ Пусть  $\langle a, b \rangle \equiv \langle c, d \rangle$ , если  $a + d = b + c$ . Тогда  $\mathbb{Z} = Z / \equiv$

# Целые числа

*«Бог создал целые числа, всё остальное — дело рук человека.»  
Леопольд Кронеккер*

$$\mathbb{Z} : \dots - 3, -2, -1, 0, 1, 2, 3, \dots$$

- ▶  $Z = \{\langle x, y \rangle \mid x, y \in \mathbb{N}_0\}$
- ▶ Интуиция:  $\langle x, y \rangle = x - y$
- ▶

$$\begin{aligned}\langle a, b \rangle + \langle c, d \rangle &= \langle a + c, b + d \rangle \\ \langle a, b \rangle - \langle c, d \rangle &= \langle a + d, b + c \rangle\end{aligned}$$

- ▶ Пусть  $\langle a, b \rangle \equiv \langle c, d \rangle$ , если  $a + d = b + c$ . Тогда  $\mathbb{Z} = Z / \equiv$
- ▶  $0 = [\langle 0, 0 \rangle]$ ,  $1 = [\langle 1, 0 \rangle]$ ,  $-7 = [\langle 0, 7 \rangle]$

## Натуральные числа

$\mathbb{N} : 1, 2, \dots$  или  $\mathbb{N}_0 : 0, 1, 2, \dots$

# Натуральные числа

$\mathbb{N} : 1, 2, \dots$  или  $\mathbb{N}_0 : 0, 1, 2, \dots$

## Определение

$N$  (или, более точно,  $\langle N, 0, (') \rangle$ ) соответствует аксиоматике Пеано, если следующее определено/выполнено:

# Натуральные числа

$\mathbb{N} : 1, 2, \dots$  или  $\mathbb{N}_0 : 0, 1, 2, \dots$

## Определение

$N$  (или, более точно,  $\langle N, 0, (') \rangle$ ) соответствует аксиоматике Пеано, если следующее определено/выполнено:

1. Операция «штрих»  $(') : N \rightarrow N$ , причём нет  $a, b \in N$ , что  $a \neq b$ , но  $a' = b'$ .

# Натуральные числа

$\mathbb{N} : 1, 2, \dots$  или  $\mathbb{N}_0 : 0, 1, 2, \dots$

## Определение

$N$  (или, более точно,  $\langle N, 0, (') \rangle$ ) соответствует аксиоматике Пеано, если следующее определено/выполнено:

1. Операция «штрих»  $(') : N \rightarrow N$ , причём нет  $a, b \in N$ , что  $a \neq b$ , но  $a' = b'$ .  
Если  $x = y'$ , то  $x$  назовём следующим за  $y$ , а  $y$  — предшествующим  $x$ .

# Натуральные числа

$\mathbb{N} : 1, 2, \dots$  или  $\mathbb{N}_0 : 0, 1, 2, \dots$

## Определение

$N$  (или, более точно,  $\langle N, 0, (') \rangle$ ) соответствует аксиоматике Пеано, если следующее определено/выполнено:

1. Операция «штрих»  $(') : N \rightarrow N$ , причём нет  $a, b \in N$ , что  $a \neq b$ , но  $a' = b'$ .  
Если  $x = y'$ , то  $x$  назовём следующим за  $y$ , а  $y$  — предшествующим  $x$ .
2. Константа  $0 \in N$ : нет  $x \in N$ , что  $x' = 0$ .



# Натуральные числа

$\mathbb{N} : 1, 2, \dots$  или  $\mathbb{N}_0 : 0, 1, 2, \dots$

## Определение

$N$  (или, более точно,  $\langle N, 0, (') \rangle$ ) соответствует аксиоматике Пеано, если следующее определено/выполнено:

1. Операция «штрих»  $(') : N \rightarrow N$ , причём нет  $a, b \in N$ , что  $a \neq b$ , но  $a' = b'$ .  
Если  $x = y'$ , то  $x$  назовём следующим за  $y$ , а  $y$  — предшествующим  $x$ .
2. Константа  $0 \in N$ : нет  $x \in N$ , что  $x' = 0$ .
3. Индукция. Каково бы ни было свойство («предикат»)  $P : N \rightarrow V$ , если:
  - 3.1  $P(0)$
  - 3.2 При любом  $x \in N$  из  $P(x)$  следует  $P(x')$то при любом  $x \in N$  выполнено  $P(x)$ .

# Натуральные числа

$\mathbb{N} : 1, 2, \dots$  или  $\mathbb{N}_0 : 0, 1, 2, \dots$

## Определение

$N$  (или, более точно,  $\langle N, 0, (') \rangle$ ) соответствует аксиоматике Пеано, если следующее определено/выполнено:

1. Операция «штрих»  $(') : N \rightarrow N$ , причём нет  $a, b \in N$ , что  $a \neq b$ , но  $a' = b'$ .  
Если  $x = y'$ , то  $x$  назовём следующим за  $y$ , а  $y$  — предшествующим  $x$ .
2. Константа  $0 \in N$ : нет  $x \in N$ , что  $x' = 0$ .
3. Индукция. Каково бы ни было свойство («предикат»)  $P : N \rightarrow V$ , если:
  - 3.1  $P(0)$
  - 3.2 При любом  $x \in N$  из  $P(x)$  следует  $P(x')$то при любом  $x \in N$  выполнено  $P(x)$ .

Как построить? Например, в стиле алгебры Линденбаума:

# Натуральные числа

$\mathbb{N} : 1, 2, \dots$  или  $\mathbb{N}_0 : 0, 1, 2, \dots$

## Определение

$N$  (или, более точно,  $\langle N, 0, (') \rangle$ ) соответствует аксиоматике Пеано, если следующее определено/выполнено:

1. Операция «штрих»  $(') : N \rightarrow N$ , причём нет  $a, b \in N$ , что  $a \neq b$ , но  $a' = b'$ .  
Если  $x = y'$ , то  $x$  назовём следующим за  $y$ , а  $y$  — предшествующим  $x$ .
2. Константа  $0 \in N$ : нет  $x \in N$ , что  $x' = 0$ .
3. Индукция. Каково бы ни было свойство («предикат»)  $P : N \rightarrow V$ , если:
  - 3.1  $P(0)$
  - 3.2 При любом  $x \in N$  из  $P(x)$  следует  $P(x')$то при любом  $x \in N$  выполнено  $P(x)$ .

Как построить? Например, в стиле алгебры Линденбаума:

1.  $N$  — язык, порождённый грамматикой  $\nu ::= 0 \mid \nu \langle ' \rangle$

# Натуральные числа

$\mathbb{N} : 1, 2, \dots$  или  $\mathbb{N}_0 : 0, 1, 2, \dots$

## Определение

$N$  (или, более точно,  $\langle N, 0, (') \rangle$ ) соответствует аксиоматике Пеано, если следующее определено/выполнено:

1. Операция «штрих»  $(') : N \rightarrow N$ , причём нет  $a, b \in N$ , что  $a \neq b$ , но  $a' = b'$ .  
Если  $x = y'$ , то  $x$  назовём следующим за  $y$ , а  $y$  — предшествующим  $x$ .
2. Константа  $0 \in N$ : нет  $x \in N$ , что  $x' = 0$ .
3. Индукция. Каково бы ни было свойство («предикат»)  $P : N \rightarrow V$ , если:
  - 3.1  $P(0)$
  - 3.2 При любом  $x \in N$  из  $P(x)$  следует  $P(x')$то при любом  $x \in N$  выполнено  $P(x)$ .

Как построить? Например, в стиле алгебры Линденбаума:

1.  $N$  — язык, порождённый грамматикой  $\nu ::= 0 \mid \nu \langle ' \rangle$
2.  $0$  — это «0»,  $x'$  — это  $x \dashv \langle ' \rangle$

## Примеры: что не соответствует аксиомам Пеано

1.  $\mathbb{Z}$ , где  $x' = x^2$

## Примеры: что не соответствует аксиомам Пеано

1.  $\mathbb{Z}$ , где  $x' = x^2$

Функция «штрих» не инъективна:  $-3^2 = 3^2 = 9$

## Примеры: что не соответствует аксиомам Пеано

1.  $\mathbb{Z}$ , где  $x' = x^2$

Функция «штрих» не инъективна:  $-3^2 = 3^2 = 9$

2. Кольцо вычетов  $\mathbb{Z}/7\mathbb{Z}$ , где  $x' = x + 1$

## Примеры: что не соответствует аксиомам Пеано

1.  $\mathbb{Z}$ , где  $x' = x^2$

Функция «штрих» не инъективна:  $-3^2 = 3^2 = 9$

2. Кольцо вычетов  $\mathbb{Z}/7\mathbb{Z}$ , где  $x' = x + 1$

$6' = 0$ , что нарушает свойства 0



## Примеры: что не соответствует аксиомам Пеано

1.  $\mathbb{Z}$ , где  $x' = x^2$

Функция «штрих» не инъективна:  $-3^2 = 3^2 = 9$

2. Кольцо вычетов  $\mathbb{Z}/7\mathbb{Z}$ , где  $x' = x + 1$

$6' = 0$ , что нарушает свойства 0

3.  $\mathbb{R}^+ \cup \{0\}$ , где  $x' = x + 1$

## Примеры: что не соответствует аксиомам Пеано

1.  $\mathbb{Z}$ , где  $x' = x^2$

Функция «штрих» не инъективна:  $-3^2 = 3^2 = 9$

2. Кольцо вычетов  $\mathbb{Z}/7\mathbb{Z}$ , где  $x' = x + 1$

$6' = 0$ , что нарушает свойства 0

3.  $\mathbb{R}^+ \cup \{0\}$ , где  $x' = x + 1$

пусть  $P(x)$  означает « $x \in \mathbb{Z}$ »:

## Примеры: что не соответствует аксиомам Пеано

1.  $\mathbb{Z}$ , где  $x' = x^2$

Функция «штрих» не инъективна:  $-3^2 = 3^2 = 9$

2. Кольцо вычетов  $\mathbb{Z}/7\mathbb{Z}$ , где  $x' = x + 1$

$6' = 0$ , что нарушает свойства 0

3.  $\mathbb{R}^+ \cup \{0\}$ , где  $x' = x + 1$

пусть  $P(x)$  означает « $x \in \mathbb{Z}$ »:

3.1  $P(0)$  выполнено:  $0 \in \mathbb{Z}$ .

## Примеры: что не соответствует аксиомам Пеано

1.  $\mathbb{Z}$ , где  $x' = x^2$

Функция «штрих» не инъективна:  $-3^2 = 3^2 = 9$

2. Кольцо вычетов  $\mathbb{Z}/7\mathbb{Z}$ , где  $x' = x + 1$

$6' = 0$ , что нарушает свойства 0

3.  $\mathbb{R}^+ \cup \{0\}$ , где  $x' = x + 1$

пусть  $P(x)$  означает « $x \in \mathbb{Z}$ »:

3.1  $P(0)$  выполнено:  $0 \in \mathbb{Z}$ .

3.2 Если  $P(x)$ , то есть  $x \in \mathbb{Z}$ , то и  $x + 1 \in \mathbb{Z}$  — так что и  $P(x')$  выполнено.

## Примеры: что не соответствует аксиомам Пеано

1.  $\mathbb{Z}$ , где  $x' = x^2$

Функция «штрих» не инъективна:  $-3^2 = 3^2 = 9$

2. Кольцо вычетов  $\mathbb{Z}/7\mathbb{Z}$ , где  $x' = x + 1$

$6' = 0$ , что нарушает свойства 0

3.  $\mathbb{R}^+ \cup \{0\}$ , где  $x' = x + 1$

пусть  $P(x)$  означает « $x \in \mathbb{Z}$ »:

3.1  $P(0)$  выполнено:  $0 \in \mathbb{Z}$ .

3.2 Если  $P(x)$ , то есть  $x \in \mathbb{Z}$ , то и  $x + 1 \in \mathbb{Z}$  — так что и  $P(x')$  выполнено.

Однако,  $P(0.5)$  ложно.

## Пример доказательства

### Теорема

*0 единственен: если  $t$  таков, что при любом  $y$  выполнено  $y' \neq t$ , то  $t = 0$ .*

## Пример доказательства

### Теорема

*0 единственен: если  $t$  таков, что при любом  $y$  выполнено  $y' \neq t$ , то  $t = 0$ .*

### Доказательство.

- Определим  $P(x)$  как «либо  $x = 0$ , либо  $x = y'$  для некоторого  $y \in N$ ».

# Пример доказательства

## Теорема

*0 единственен: если  $t$  таков, что при любом  $y$  выполнено  $y' \neq t$ , то  $t = 0$ .*

## Доказательство.

- ▶ Определим  $P(x)$  как «либо  $x = 0$ , либо  $x = y'$  для некоторого  $y \in N$ ».
- 1.  $P(0)$  выполнено, так как  $0 = 0$ .



# Пример доказательства

## Теорема

*0 единственен: если  $t$  таков, что при любом  $y$  выполнено  $y' \neq t$ , то  $t = 0$ .*

## Доказательство.

- ▶ Определим  $P(x)$  как «либо  $x = 0$ , либо  $x = y'$  для некоторого  $y \in N$ ».
  1.  $P(0)$  выполнено, так как  $0 = 0$ .
  2. Если  $P(x)$  выполнено, то возьмём  $x$  в качестве  $y$ : тогда для  $P(x')$  будет выполнено  $x' = y'$ .

# Пример доказательства

## Теорема

*0 единственен: если  $t$  таков, что при любом  $y$  выполнено  $y' \neq t$ , то  $t = 0$ .*

## Доказательство.

- ▶ Определим  $P(x)$  как «либо  $x = 0$ , либо  $x = y'$  для некоторого  $y \in N$ ».
  1.  $P(0)$  выполнено, так как  $0 = 0$ .
  2. Если  $P(x)$  выполнено, то возьмём  $x$  в качестве  $y$ : тогда для  $P(x')$  будет выполнено  $x' = y'$ .

Значит,  $P(x)$  для любого  $x \in N$ .

# Пример доказательства

## Теорема

*0 единственен: если  $t$  таков, что при любом  $y$  выполнено  $y' \neq t$ , то  $t = 0$ .*

## Доказательство.

- ▶ Определим  $P(x)$  как «либо  $x = 0$ , либо  $x = y'$  для некоторого  $y \in N$ ».
  1.  $P(0)$  выполнено, так как  $0 = 0$ .
  2. Если  $P(x)$  выполнено, то возьмём  $x$  в качестве  $y$ : тогда для  $P(x')$  будет выполнено  $x' = y'$ .

Значит,  $P(x)$  для любого  $x \in N$ .

- ▶ Рассмотрим  $P(t)$ : «либо  $t = 0$ , либо  $t = y'$  для некоторого  $y \in N$ ». Но так как такого  $y$  нет, то неизбежно  $t = 0$ .



## Обозначения и определения

### Определение

$$1 = 0', 2 = 0'', 3 = 0''', 4 = 0'''', 5 = 0''''', 6 = 0'''''', 7 = 0''''''', 8 = 0'''''''', 9 = 0'''''''''$$

## Обозначения и определения

### Определение

$$1 = 0', 2 = 0'', 3 = 0''', 4 = 0'''', 5 = 0''''', 6 = 0'''''', 7 = 0''''''', 8 = 0'''''''', 9 = 0'''''''''$$

### Определение

$$a + b = \begin{cases} a, & \text{если } b = 0 \\ (a + c)', & \text{если } b = c' \end{cases}$$

## Обозначения и определения

### Определение

$$1 = 0', 2 = 0'', 3 = 0''', 4 = 0'''', 5 = 0''''', 6 = 0'''''', 7 = 0''''''', 8 = 0'''''''', 9 = 0'''''''''$$

### Определение

$$a + b = \begin{cases} a, & \text{если } b = 0 \\ (a + c)', & \text{если } b = c' \end{cases}$$

Например,

$$2 + 2 = 0'' + 0'' =$$

## Обозначения и определения

### Определение

$$1 = 0', 2 = 0'', 3 = 0''', 4 = 0'''', 5 = 0''''', 6 = 0'''''', 7 = 0''''''', 8 = 0'''''''', 9 = 0'''''''''$$

### Определение

$$a + b = \begin{cases} a, & \text{если } b = 0 \\ (a + c)', & \text{если } b = c' \end{cases}$$

Например,

$$2 + 2 = 0'' + 0'' = (0'' + 0')' =$$

## Обозначения и определения

### Определение

$$1 = 0', 2 = 0'', 3 = 0''', 4 = 0'''', 5 = 0''''', 6 = 0'''''', 7 = 0''''''', 8 = 0'''''''', 9 = 0'''''''''$$

### Определение

$$a + b = \begin{cases} a, & \text{если } b = 0 \\ (a + c)', & \text{если } b = c' \end{cases}$$

Например,

$$2 + 2 = 0'' + 0'' = (0'' + 0')' = ((0'' + 0)')' =$$



## Обозначения и определения

### Определение

$$1 = 0', 2 = 0'', 3 = 0''', 4 = 0'''', 5 = 0''''', 6 = 0'''''', 7 = 0''''''', 8 = 0'''''''', 9 = 0'''''''''$$

### Определение

$$a + b = \begin{cases} a, & \text{если } b = 0 \\ (a + c)', & \text{если } b = c' \end{cases}$$

Например,

$$2 + 2 = 0'' + 0'' = (0'' + 0')' = ((0'' + 0)')' = ((0'')')' = 0''' = 4$$

## Обозначения и определения

### Определение

$$1 = 0', 2 = 0'', 3 = 0''', 4 = 0'''', 5 = 0''''', 6 = 0'''''', 7 = 0''''''', 8 = 0'''''''', 9 = 0'''''''''$$

### Определение

$$a + b = \begin{cases} a, & \text{если } b = 0 \\ (a + c)', & \text{если } b = c' \end{cases}$$

Например,

$$2 + 2 = 0'' + 0'' = (0'' + 0')' = ((0'' + 0)')' = ((0'')')' = 0''' = 4$$

### Определение

$$a \cdot b = \begin{cases} 0, & \text{если } b = 0 \\ a \cdot c + a, & \text{если } b = c' \end{cases}$$

## Пример: коммутативность сложения (лемма 1)

Лемма (1)

$$a + 0 = 0 + a$$

## Пример: коммутативность сложения (лемма 1)

Лемма (1)

$$a + 0 = 0 + a$$

$$a + b = \begin{cases} a, & \text{если } b = 0 \\ (a + c)', & \text{если } b = c' \end{cases}$$

## Пример: коммутативность сложения (лемма 1)

Лемма (1)

$$a + 0 = 0 + a$$

Доказательство.

Пусть  $P(x)$  — это  $x + 0 = 0 + x$ .

$$a + b = \begin{cases} a, & \text{если } b = 0 \\ (a + c)', & \text{если } b = c' \end{cases}$$

## Пример: коммутативность сложения (лемма 1)

### Лемма (1)

$$a + 0 = 0 + a$$

### Доказательство.

Пусть  $P(x)$  — это  $x + 0 = 0 + x$ .

1. Покажем  $P(0)$ .  $0 + 0 = 0 + 0$

$$a + b = \begin{cases} a, & \text{если } b = 0 \\ (a + c)', & \text{если } b = c' \end{cases}$$

## Пример: коммутативность сложения (лемма 1)

### Лемма (1)

$$a + 0 = 0 + a$$

$$a + b = \begin{cases} a, & \text{если } b = 0 \\ (a + c)', & \text{если } b = c' \end{cases}$$

### Доказательство.

Пусть  $P(x)$  — это  $x + 0 = 0 + x$ .

1. Покажем  $P(0)$ .  $0 + 0 = 0 + 0$
2. Покажем, что если  $P(x)$ , то  $P(x')$ . Покажем  $P(x')$ , то есть  $x' + 0 = \dots$

## Пример: коммутативность сложения (лемма 1)

### Лемма (1)

$$a + 0 = 0 + a$$

$$a + b = \begin{cases} a, & \text{если } b = 0 \\ (a + c)', & \text{если } b = c' \end{cases}$$

### Доказательство.

Пусть  $P(x)$  — это  $x + 0 = 0 + x$ .

1. Покажем  $P(0)$ .  $0 + 0 = 0 + 0$

2. Покажем, что если  $P(x)$ , то  $P(x')$ . Покажем  $P(x')$ , то есть  $x' + 0 = \dots$

$$\dots = x' \qquad a = x', b = 0: \quad x' + 0 \Rightarrow x'$$



## Пример: коммутативность сложения (лемма 1)

### Лемма (1)

$$a + 0 = 0 + a$$

$$a + b = \begin{cases} a, & \text{если } b = 0 \\ (a + c)', & \text{если } b = c' \end{cases}$$

### Доказательство.

Пусть  $P(x)$  — это  $x + 0 = 0 + x$ .

1. Покажем  $P(0)$ .  $0 + 0 = 0 + 0$

2. Покажем, что если  $P(x)$ , то  $P(x')$ . Покажем  $P(x')$ , то есть  $x' + 0 = \dots$

$$\dots = x' \qquad a = x', b = 0: \quad x' + 0 \Rightarrow x'$$

$$\dots = (x)'$$

## Пример: коммутативность сложения (лемма 1)

### Лемма (1)

$$a + 0 = 0 + a$$

$$a + b = \begin{cases} a, & \text{если } b = 0 \\ (a + c)', & \text{если } b = c' \end{cases}$$

### Доказательство.

Пусть  $P(x)$  — это  $x + 0 = 0 + x$ .

1. Покажем  $P(0)$ .  $0 + 0 = 0 + 0$

2. Покажем, что если  $P(x)$ , то  $P(x')$ . Покажем  $P(x')$ , то есть  $x' + 0 = \dots$

$$\dots = x' \quad a = x', b = 0: \quad x' + 0 \Rightarrow x'$$

$$\dots = (x)'$$

$$\dots = (x + 0)' \quad a = x, b = 0: \quad (x + 0) \Leftarrow (x)$$

## Пример: коммутативность сложения (лемма 1)

### Лемма (1)

$$a + 0 = 0 + a$$

$$a + b = \begin{cases} a, & \text{если } b = 0 \\ (a + c)', & \text{если } b = c' \end{cases}$$

### Доказательство.

Пусть  $P(x)$  — это  $x + 0 = 0 + x$ .

1. Покажем  $P(0)$ .  $0 + 0 = 0 + 0$

2. Покажем, что если  $P(x)$ , то  $P(x')$ . Покажем  $P(x')$ , то есть  $x' + 0 = \dots$

$$\dots = x' \quad a = x', b = 0: \quad x' + 0 \Rightarrow x'$$

$$\dots = (x)'$$

$$\dots = (x + 0)' \quad a = x, b = 0: \quad (x + 0) \Leftarrow (x)$$

$$\dots = (0 + x)' \quad P(x): \quad (x + 0) \Rightarrow (0 + x)$$

## Пример: коммутативность сложения (лемма 1)

### Лемма (1)

$$a + 0 = 0 + a$$

$$a + b = \begin{cases} a, & \text{если } b = 0 \\ (a + c)', & \text{если } b = c' \end{cases}$$

### Доказательство.

Пусть  $P(x)$  — это  $x + 0 = 0 + x$ .

1. Покажем  $P(0)$ .  $0 + 0 = 0 + 0$

2. Покажем, что если  $P(x)$ , то  $P(x')$ . Покажем  $P(x')$ , то есть  $x' + 0 = \dots$

$$\dots = x' \quad a = x', b = 0: \quad x' + 0 \Rightarrow x'$$

$$\dots = (x)'$$

$$\dots = (x + 0)' \quad a = x, b = 0: \quad (x + 0) \Leftarrow (x)$$

$$\dots = (0 + x)' \quad P(x): \quad (x + 0) \Rightarrow (0 + x)$$

$$\dots = 0 + x' \quad a = 0, b = x': \quad 0 + x' \Leftarrow (0 + x)'$$

## Пример: коммутативность сложения (лемма 1)

### Лемма (1)

$$a + 0 = 0 + a$$

$$a + b = \begin{cases} a, & \text{если } b = 0 \\ (a + c)', & \text{если } b = c' \end{cases}$$

### Доказательство.

Пусть  $P(x)$  — это  $x + 0 = 0 + x$ .

1. Покажем  $P(0)$ .  $0 + 0 = 0 + 0$

2. Покажем, что если  $P(x)$ , то  $P(x')$ . Покажем  $P(x')$ , то есть  $x' + 0 = \dots$

$$\dots = x' \quad a = x', b = 0: \quad x' + 0 \Rightarrow x'$$

$$\dots = (x)'$$

$$\dots = (x + 0)' \quad a = x, b = 0: \quad (x + 0) \Leftarrow (x)$$

$$\dots = (0 + x)' \quad P(x): \quad (x + 0) \Rightarrow (0 + x)$$

$$\dots = 0 + x' \quad a = 0, b = x': \quad 0 + x' \Leftarrow (0 + x)'$$

Значит,  $P(a)$  выполнено для любого  $a \in N$ .



## Пример: коммутативность сложения (завершение)

Лемма (2)

$$a + b' = a' + b$$

## Пример: коммутативность сложения (завершение)

Лемма (2)

$$a + b' = a' + b$$

Доказательство.

$$P(x) \text{ — это } a + x' = a' + x$$

## Пример: коммутативность сложения (завершение)

Лемма (2)

$$a + b' = a' + b$$

Доказательство.

$P(x)$  — это  $a + x' = a' + x$

1.  $a + 0' = (a + 0)' = (a)' = a' = a' + 0$



## Пример: коммутативность сложения (завершение)

Лемма (2)

$$a + b' = a' + b$$

Доказательство.

$P(x)$  — это  $a + x' = a' + x$

1.  $a + 0' = (a + 0)' = (a)' = a' = a' + 0$

2. Покажем, что  $P(x')$  следует из  $P(x)$ :  $a + x'' = (a + x')' = (a' + x)' = a' + x'$



## Пример: коммутативность сложения (завершение)

### Лемма (2)

$$a + b' = a' + b$$

### Доказательство.

$P(x)$  — это  $a + x' = a' + x$

1.  $a + 0' = (a + 0)' = (a)' = a' = a' + 0$

2. Покажем, что  $P(x')$  следует из  $P(x)$ :  $a + x'' = (a + x')' = (a' + x)' = a' + x'$



### Теорема

$$a + b = b + a$$

## Пример: коммутативность сложения (завершение)

### Лемма (2)

$$a + b' = a' + b$$

### Доказательство.

$P(x)$  — это  $a + x' = a' + x$

1.  $a + 0' = (a + 0)' = (a)' = a' = a' + 0$

2. Покажем, что  $P(x')$  следует из  $P(x)$ :  $a + x'' = (a + x')' = (a' + x)' = a' + x'$



### Теорема

$$a + b = b + a$$

Доказательство индукцией по  $b$ :  $P(x)$  — это  $a + x = x + a$ .

1.  $a + 0 = 0 + a$  (лемма 1)

## Пример: коммутативность сложения (завершение)

### Лемма (2)

$$a + b' = a' + b$$

### Доказательство.

$P(x)$  — это  $a + x' = a' + x$

1.  $a + 0' = (a + 0)' = (a)' = a' = a' + 0$
2. Покажем, что  $P(x')$  следует из  $P(x)$ :  $a + x'' = (a + x')' = (a' + x)' = a' + x'$



### Теорема

$$a + b = b + a$$

Доказательство индукцией по  $b$ :  $P(x)$  — это  $a + x = x + a$ .

1.  $a + 0 = 0 + a$  (лемма 1)
2.  $a + x' = (a + x)' = (x + a)' = x + a' = x' + a$



## Уточнение исчисления предикатов

- ▶ Пусть требуется доказывать утверждения про равенство. Введём  $E(p, q)$  — предикат «равенство».

## Уточнение исчисления предикатов

- ▶ Пусть требуется доказывать утверждения про равенство. Введём  $E(p, q)$  — предикат «равенство».
- ▶ Однако,  $\not\models E(p, q) \rightarrow E(q, p)$ : если  $D = \{0, 1\}$  и  $E(p, q) ::= (p > q)$ , то  $\not\models E(p, q) \rightarrow E(q, p)$ .

## Уточнение исчисления предикатов

- ▶ Пусть требуется доказывать утверждения про равенство. Введём  $E(p, q)$  — предикат «равенство».
- ▶ Однако,  $\not\models E(p, q) \rightarrow E(q, p)$ : если  $D = \{0, 1\}$  и  $E(p, q) ::= (p > q)$ , то  $\not\models E(p, q) \rightarrow E(q, p)$ .
- ▶ Конечно, можем указывать  $\forall p. \forall q. E(p, q) \rightarrow E(q, p) \vdash \varphi$ .

## Уточнение исчисления предикатов

- ▶ Пусть требуется доказывать утверждения про равенство. Введём  $E(p, q)$  — предикат «равенство».
- ▶ Однако,  $\not\models E(p, q) \rightarrow E(q, p)$ : если  $D = \{0, 1\}$  и  $E(p, q) ::= (p > q)$ , то  $\not\models E(p, q) \rightarrow E(q, p)$ .
- ▶ Конечно, можем указывать  $\forall p. \forall q. E(p, q) \rightarrow E(q, p) \vdash \varphi$ .
- ▶ Но лучше добавим аксиому  $\forall p. \forall q. E(p, q) \rightarrow E(q, p)$ .



## Уточнение исчисления предикатов

- ▶ Пусть требуется доказывать утверждения про равенство. Введём  $E(p, q)$  — предикат «равенство».
- ▶ Однако,  $\not\models E(p, q) \rightarrow E(q, p)$ : если  $D = \{0, 1\}$  и  $E(p, q) ::= (p > q)$ , то  $\not\models E(p, q) \rightarrow E(q, p)$ .
- ▶ Конечно, можем указывать  $\forall p. \forall q. E(p, q) \rightarrow E(q, p) \vdash \varphi$ .
- ▶ Но лучше добавим аксиому  $\forall p. \forall q. E(p, q) \rightarrow E(q, p)$ .
- ▶ Добавив необходимые аксиомы, получим *теорию первого порядка*.

# Теория первого порядка

## Определение

*Теорией первого порядка назовём исчисление предикатов с дополнительными («нелогическими» или «математическими»):*

- ▶ *предикатными и функциональными символами;*
- ▶ *аксиомами.*

*Сущности, взятые из исходного исчисления предикатов, назовём логическими*

## Порядок логики/теории

Порядок	Кванторы	Формализует суждения о...	Пример
нулевой	запрещены	об отдельных значениях	И.В.
первый	по предметным переменным	о множествах $S = \{t \mid \psi[x := t]\}$	И.П.
второй	по предикатным переменным	о множествах множеств $S = \{\{t \mid P(t)\} \mid \varphi[p := P]\}$	
	...		

# Формальная арифметика

## Определение

*Формальная арифметика — теория первого порядка, со следующими добавленными нелогическими ...*

- ▶ *двуместными функциональными символами  $(+)$ ,  $(\cdot)$ ; одноместным функциональным символом  $(')$ , нульместным функциональным символом  $0$ ;*

# Формальная арифметика

## Определение

*Формальная арифметика — теория первого порядка, со следующими добавленными нелогическими ...*

- ▶ *двуместными функциональными символами  $(+)$ ,  $(\cdot)$ ; одноместным функциональным символом  $(')$ , нульместным функциональным символом  $0$ ;*
- ▶ *двуместным предикатным символом  $(=)$ ;*

# Формальная арифметика

## Определение

Формальная арифметика — теория первого порядка, со следующими добавленными нелогическими ...

- ▶ двуместными функциональными символами  $(+)$ ,  $(\cdot)$ ; одноместным функциональным символом  $(')$ , нульместным функциональным символом  $0$ ;
- ▶ двуместным предикатным символом  $(=)$ ;
- ▶ восемью нелогическими аксиомами:

$(A1) a = b \rightarrow a = c \rightarrow b = c$	$(A5) a + 0 = a$
$(A2) a = b \rightarrow a' = b'$	$(A6) a + b' = (a + b)'$
$(A3) a' = b' \rightarrow a = b$	$(A7) a \cdot 0 = 0$
$(A4) \neg a' = 0$	$(A8) a \cdot b' = a \cdot b + a$

# Формальная арифметика

## Определение

Формальная арифметика — теория первого порядка, со следующими добавленными нелогическими ...

- ▶ двуместными функциональными символами  $(+)$ ,  $(\cdot)$ ; одноместным функциональным символом  $(')$ , нульместным функциональным символом  $0$ ;
- ▶ двуместным предикатным символом  $(=)$ ;
- ▶ восемью нелогическими аксиомами:
  - (A1)  $a = b \rightarrow a = c \rightarrow b = c$       (A5)  $a + 0 = a$
  - (A2)  $a = b \rightarrow a' = b'$               (A6)  $a + b' = (a + b)'$
  - (A3)  $a' = b' \rightarrow a = b$               (A7)  $a \cdot 0 = 0$
  - (A4)  $\neg a' = 0$                           (A8)  $a \cdot b' = a \cdot b + a$
- ▶ нелогической схемой аксиом индукции  $\psi[x := 0] \ \& \ (\forall x. \psi \rightarrow \psi[x := x']) \rightarrow \psi$ , с метапеременными  $x$  и  $\psi$ .

Докажем, что  $a = a$

Пусть  $\top ::= 0 = 0 \rightarrow 0 = 0 \rightarrow 0 = 0$ , тогда:



Докажем, что  $a = a$

Пусть  $\top ::= 0 = 0 \rightarrow 0 = 0 \rightarrow 0 = 0$ , тогда:

- (1)  $a = b \rightarrow a = c \rightarrow b = c$  (Акс. A1)
- (2)  $(a = b \rightarrow a = c \rightarrow b = c) \rightarrow \top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$  (Сх. акс. 1)
- (3)  $\top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$  (М.Р. 1, 2)
- (4)  $\top \rightarrow (\forall c. a = b \rightarrow a = c \rightarrow b = c)$  (Введ.  $\forall$ )

Докажем, что  $a = a$

Пусть  $\top ::= 0 = 0 \rightarrow 0 = 0 \rightarrow 0 = 0$ , тогда:

- |     |                                                                                                                        |                    |
|-----|------------------------------------------------------------------------------------------------------------------------|--------------------|
| (1) | $a = b \rightarrow a = c \rightarrow b = c$                                                                            | (Акс. A1)          |
| (2) | $(a = b \rightarrow a = c \rightarrow b = c) \rightarrow \top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$ | (Сх. акс. 1)       |
| (3) | $\top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$                                                         | (М.Р. 1, 2)        |
| (4) | $\top \rightarrow (\forall c. a = b \rightarrow a = c \rightarrow b = c)$                                              | (Введ. $\forall$ ) |
| (5) | $\top \rightarrow (\forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$                                   | (Введ. $\forall$ ) |
| (6) | $\top \rightarrow (\forall a. \forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$                        | (Введ. $\forall$ ) |

Докажем, что  $a = a$

Пусть  $\top ::= 0 = 0 \rightarrow 0 = 0 \rightarrow 0 = 0$ , тогда:

- |     |                                                                                                                        |                    |
|-----|------------------------------------------------------------------------------------------------------------------------|--------------------|
| (1) | $a = b \rightarrow a = c \rightarrow b = c$                                                                            | (Акс. A1)          |
| (2) | $(a = b \rightarrow a = c \rightarrow b = c) \rightarrow \top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$ | (Сх. акс. 1)       |
| (3) | $\top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$                                                         | (М.Р. 1, 2)        |
| (4) | $\top \rightarrow (\forall c. a = b \rightarrow a = c \rightarrow b = c)$                                              | (Введ. $\forall$ ) |
| (5) | $\top \rightarrow (\forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$                                   | (Введ. $\forall$ ) |
| (6) | $\top \rightarrow (\forall a. \forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$                        | (Введ. $\forall$ ) |
| (7) | $\top$                                                                                                                 | (Сх. акс 1)        |
| (8) | $(\forall a. \forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$                                         | (М.Р. 7, 6)        |

Докажем, что  $a = a$

Пусть  $\top ::= 0 = 0 \rightarrow 0 = 0 \rightarrow 0 = 0$ , тогда:

- |     |                                                                                                                                                                                       |                    |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| (1) | $a = b \rightarrow a = c \rightarrow b = c$                                                                                                                                           | (Акс. A1)          |
| (2) | $(a = b \rightarrow a = c \rightarrow b = c) \rightarrow \top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$                                                                | (Сх. акс. 1)       |
| (3) | $\top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$                                                                                                                        | (М.Р. 1, 2)        |
| (4) | $\top \rightarrow (\forall c. a = b \rightarrow a = c \rightarrow b = c)$                                                                                                             | (Введ. $\forall$ ) |
| (5) | $\top \rightarrow (\forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$                                                                                                  | (Введ. $\forall$ ) |
| (6) | $\top \rightarrow (\forall a. \forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$                                                                                       | (Введ. $\forall$ ) |
| (7) | $\top$                                                                                                                                                                                | (Сх. акс 1)        |
| (8) | $(\forall a. \forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$                                                                                                        | (М.Р. 7, 6)        |
| (9) | $(\forall a. \forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c) \rightarrow$<br>$\rightarrow (\forall b. \forall c. a + 0 = b \rightarrow a + 0 = c \rightarrow b = c)$ | (Сх. акс. 11)      |

Докажем, что  $a = a$

Пусть  $\top ::= 0 = 0 \rightarrow 0 = 0 \rightarrow 0 = 0$ , тогда:

- |      |                                                                                                                                                                                       |                    |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| (1)  | $a = b \rightarrow a = c \rightarrow b = c$                                                                                                                                           | (Акс. A1)          |
| (2)  | $(a = b \rightarrow a = c \rightarrow b = c) \rightarrow \top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$                                                                | (Сх. акс. 1)       |
| (3)  | $\top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$                                                                                                                        | (М.Р. 1, 2)        |
| (4)  | $\top \rightarrow (\forall c. a = b \rightarrow a = c \rightarrow b = c)$                                                                                                             | (Введ. $\forall$ ) |
| (5)  | $\top \rightarrow (\forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$                                                                                                  | (Введ. $\forall$ ) |
| (6)  | $\top \rightarrow (\forall a. \forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$                                                                                       | (Введ. $\forall$ ) |
| (7)  | $\top$                                                                                                                                                                                | (Сх. акс 1)        |
| (8)  | $(\forall a. \forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$                                                                                                        | (М.Р. 7, 6)        |
| (9)  | $(\forall a. \forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c) \rightarrow$<br>$\rightarrow (\forall b. \forall c. a + 0 = b \rightarrow a + 0 = c \rightarrow b = c)$ | (Сх. акс. 11)      |
| (10) | $\forall b. \forall c. a + 0 = b \rightarrow a + 0 = c \rightarrow b = c$                                                                                                             | (М.Р. 8, 9)        |

Докажем, что  $a = a$

Пусть  $\top ::= 0 = 0 \rightarrow 0 = 0 \rightarrow 0 = 0$ , тогда:

- |      |                                                                                                                                                                                       |                    |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| (1)  | $a = b \rightarrow a = c \rightarrow b = c$                                                                                                                                           | (Акс. A1)          |
| (2)  | $(a = b \rightarrow a = c \rightarrow b = c) \rightarrow \top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$                                                                | (Сх. акс. 1)       |
| (3)  | $\top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$                                                                                                                        | (М.Р. 1, 2)        |
| (4)  | $\top \rightarrow (\forall c. a = b \rightarrow a = c \rightarrow b = c)$                                                                                                             | (Введ. $\forall$ ) |
| (5)  | $\top \rightarrow (\forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$                                                                                                  | (Введ. $\forall$ ) |
| (6)  | $\top \rightarrow (\forall a. \forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$                                                                                       | (Введ. $\forall$ ) |
| (7)  | $\top$                                                                                                                                                                                | (Сх. акс 1)        |
| (8)  | $(\forall a. \forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$                                                                                                        | (М.Р. 7, 6)        |
| (9)  | $(\forall a. \forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c) \rightarrow$<br>$\rightarrow (\forall b. \forall c. a + 0 = b \rightarrow a + 0 = c \rightarrow b = c)$ | (Сх. акс. 11)      |
| (10) | $\forall b. \forall c. a + 0 = b \rightarrow a + 0 = c \rightarrow b = c$                                                                                                             | (М.Р. 8, 9)        |
| (12) | $\forall c. a + 0 = a \rightarrow a + 0 = c \rightarrow a = c$                                                                                                                        | (М.Р. 10, 11)      |

Докажем, что  $a = a$

Пусть  $\top ::= 0 = 0 \rightarrow 0 = 0 \rightarrow 0 = 0$ , тогда:

- |      |                                                                                                                                                                                       |                    |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| (1)  | $a = b \rightarrow a = c \rightarrow b = c$                                                                                                                                           | (Акс. A1)          |
| (2)  | $(a = b \rightarrow a = c \rightarrow b = c) \rightarrow \top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$                                                                | (Сх. акс. 1)       |
| (3)  | $\top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$                                                                                                                        | (М.Р. 1, 2)        |
| (4)  | $\top \rightarrow (\forall c. a = b \rightarrow a = c \rightarrow b = c)$                                                                                                             | (Введ. $\forall$ ) |
| (5)  | $\top \rightarrow (\forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$                                                                                                  | (Введ. $\forall$ ) |
| (6)  | $\top \rightarrow (\forall a. \forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$                                                                                       | (Введ. $\forall$ ) |
| (7)  | $\top$                                                                                                                                                                                | (Сх. акс 1)        |
| (8)  | $(\forall a. \forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$                                                                                                        | (М.Р. 7, 6)        |
| (9)  | $(\forall a. \forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c) \rightarrow$<br>$\rightarrow (\forall b. \forall c. a + 0 = b \rightarrow a + 0 = c \rightarrow b = c)$ | (Сх. акс. 11)      |
| (10) | $\forall b. \forall c. a + 0 = b \rightarrow a + 0 = c \rightarrow b = c$                                                                                                             | (М.Р. 8, 9)        |
| (12) | $\forall c. a + 0 = a \rightarrow a + 0 = c \rightarrow a = c$                                                                                                                        | (М.Р. 10, 11)      |
| (14) | $a + 0 = a \rightarrow a + 0 = a \rightarrow a = a$                                                                                                                                   | (М.Р. 12, 13)      |

Докажем, что  $a = a$

Пусть  $\top ::= 0 = 0 \rightarrow 0 = 0 \rightarrow 0 = 0$ , тогда:

- |      |                                                                                                                                                                                       |                    |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| (1)  | $a = b \rightarrow a = c \rightarrow b = c$                                                                                                                                           | (Акс. A1)          |
| (2)  | $(a = b \rightarrow a = c \rightarrow b = c) \rightarrow \top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$                                                                | (Сх. акс. 1)       |
| (3)  | $\top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$                                                                                                                        | (М.Р. 1, 2)        |
| (4)  | $\top \rightarrow (\forall c. a = b \rightarrow a = c \rightarrow b = c)$                                                                                                             | (Введ. $\forall$ ) |
| (5)  | $\top \rightarrow (\forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$                                                                                                  | (Введ. $\forall$ ) |
| (6)  | $\top \rightarrow (\forall a. \forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$                                                                                       | (Введ. $\forall$ ) |
| (7)  | $\top$                                                                                                                                                                                | (Сх. акс 1)        |
| (8)  | $(\forall a. \forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$                                                                                                        | (М.Р. 7, 6)        |
| (9)  | $(\forall a. \forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c) \rightarrow$<br>$\rightarrow (\forall b. \forall c. a + 0 = b \rightarrow a + 0 = c \rightarrow b = c)$ | (Сх. акс. 11)      |
| (10) | $\forall b. \forall c. a + 0 = b \rightarrow a + 0 = c \rightarrow b = c$                                                                                                             | (М.Р. 8, 9)        |
| (12) | $\forall c. a + 0 = a \rightarrow a + 0 = c \rightarrow a = c$                                                                                                                        | (М.Р. 10, 11)      |
| (14) | $a + 0 = a \rightarrow a + 0 = a \rightarrow a = a$                                                                                                                                   | (М.Р. 12, 13)      |
| (15) | $a + 0 = a$                                                                                                                                                                           | (Акс. A5)          |
| (16) | $a + 0 = a \rightarrow a = a$                                                                                                                                                         | (М.Р. 15, 14)      |
| (17) | $a = a$                                                                                                                                                                               | (М.Р. 15, 16)      |