# Теория алгоритмов и сложности вычислений

Данил Заблоцкий

12 марта 2024 г.

# Оглавление

# Глава 1

# Введение

### Лекция 1: Начало

от 13 фев 12:45

**Примечание** (История). ?

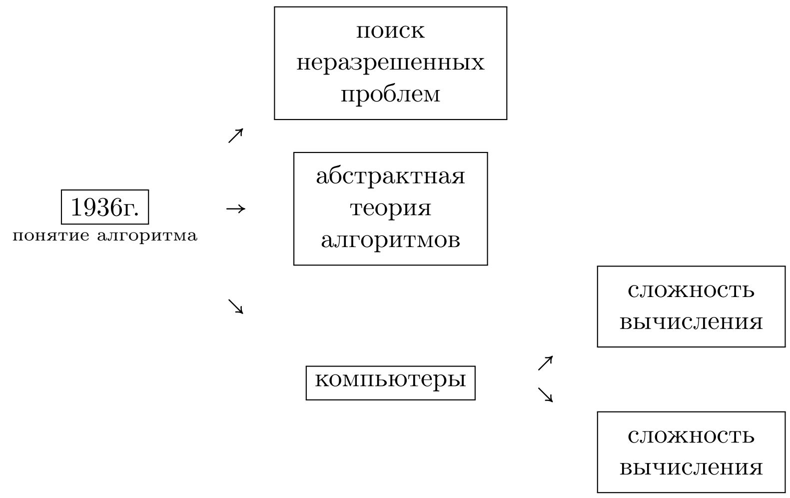
$\boxed{\text{1936г.}}$ алгоритм Евклида (>2 тыс.)
алгоритм сложения, умножения (>1 тыс.)
метод Гаусса
⋮

$\boxed{\text{1900г.}}$ Гильберт

$$\underline{\text{аксиомы}} \longrightarrow \text{теоремы}$$

$\boxed{\text{1931г.}}$ Гёдель

$\boxed{\text{1936г.}}$ формализация понятия алгоритма: модели вычислений
Чёрч – $\lambda$-исчисление
Тьюринг – машина Тьюринга
Пост – машина Поста
Марков – алгорифмы Маркова
Клини – рекурсивные функции

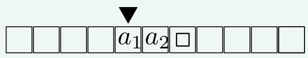



**Примечание.**

$$A = \{a_1, \dots, a_m\} \text{ – рабочий алфавит}$$

**Определение 1** (Машина Тьюринга)**.** *Машина Тьюринга* (МТ) над алфавитом $A$ состоит из:

1. Бесконечной в обе стороны ленты, разбитой на ячейки. Ячейка может быть пустой (записан $\square$), или содержать символ из $A$.




2. Каретка, которая двигается над лентой, читает и пишет символы в ячейки.
3. Внутренние состояния:

$$q_0, q_1, q_2, \dots, q_n \quad \left| \begin{array}{l} q_0 \text{ – конечное} \\ q_1 \text{ – начальное} \end{array} \right.$$

4. Программа – набор правил вида:

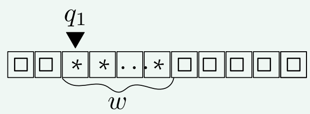
$$(q_i, a) \longrightarrow (q_j, b, S),$$

где $\begin{array}{l} q_i \text{ – любое состояние } \neq q_0 \\ a, b \text{ – символы из } A \cup \{\square\} \\ q_j \text{ – набор состояний} \\ S \text{ – сдвиг } R \text{ и } L \end{array}$, по одному правилу: $\forall$ комбинации $(q_i, a)$

$$q_i \neq q_0, \quad a \in A \cup \{\square\}.$$

**Определение 2** (Работа МТ). *Работа МТ* $M$ на слове $w \in A^*$:

1. (на рисунке)




2. Согласно программе $M$ работает.

3. $M$ останавливается, если она нападает в $q_0$

$$\big(M(w)\downarrow\big)$$

и результат работы $M(w)$ – это слово, которое остается записанным. Иначе $M$ не останавливается на $w$

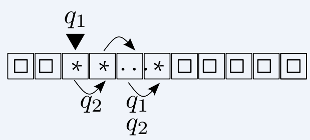
$$\big(M(w)\uparrow\big).$$

**Определение 3** (Вычисление фукнкции МТ). МТ $M$ *вычисляет функцию* $f_M : A^* \longrightarrow A^*$, если $\forall w \in A^*$ если $f_M(w)$ определена, то $M(w)\downarrow$ и $M(w) = f_M(w)$, а если $f_M(w)$ не определена, то $M(W)\uparrow$.

**Примечание** (Тезис Тьюринга). Если $f : A^* \longrightarrow A^*$ вычислима интуитивно, то $\exists$ МТ $M$, которая ее вычисляет.

**Пример.**

$$f(w) = \begin{cases} 1, & \text{если } |w| \text{ – \textit{четная длина} } w \\ 0, & \text{иначе} \end{cases}$$




$$\begin{aligned} q_1 &\Rightarrow \text{четная} \\ q_2 &\Rightarrow \text{нечетная} \end{aligned}$$

$$\begin{array}{ll} (q_1, 0) \longrightarrow (q_2, \square, R) & (q_2, 0) \longrightarrow (q_1, \square, R) \\ (q_1, 1) \longrightarrow (q_2, \square, R) & (q_2, 1) \longrightarrow (q_1, \square, R) \\ (q_1, \square) \longrightarrow (q_0, 1, L) & (q_2, \square) \longrightarrow (q_0, 0, R) \end{array}$$

## Лекция ?: Продолжение

от 12 мар 12:45

## 1.1 Неразрешимые проблемы

**Примечание** (Проблема истинности в арифметике)**.** Гильберт, 1900.

$$\mathfrak{N} = < \mathbb{N}, +, \cdot, 1 >,$$

$$\forall x \exists y \ (x = y + y), \quad \exists x \exists y \ (x = y + y),$$

$$P(z) = \forall x \forall y \ \Big((z = xy) \to \big((x = 1) \lor (y = 1)\big)\Big) \land \neg(z = 1) \text{ -- простое число},$$

$$\forall x \exists y \exists z \ \Big(\neg(x = 2) \to \big(P(y) \land P(z) \land (x + x = y + z)\big)\Big) \text{ -- гипотеза Гольдбака.}$$

- $\boxed{\text{ВХОД}}$ арифметическое утверждение $\Phi$;
- $\boxed{\text{ВЫХОД}}$ 1, если $\Phi$ истинно над $\mathfrak{N}$ ($\mathfrak{N} \models \Phi$),
  0 иначе.

**Теорема 1** (Чери, 1936)**.** Проблема истинности в арифметике неразрешима.

**Примечание** (Проблема истинности в геометрии)**.**

$$\mathfrak{R} = < \mathbb{R}, +, -, \cdot, /, 0, 1 >,$$

- $\boxed{\text{ВХОД}}$ утверждение $\Phi$;
- $\boxed{\text{ВЫХОД}}$ 1, если $\Phi$ истинно над $\mathfrak{R}$ ($\mathfrak{R} \models \Phi$),
  0 иначе.

**Теорема 2** (Тарекий, 1940-е)**.** Проблема истинности в геометрии *разрешима.*

**Примечание** (Десятая проблема Гильберта)**.** 23 проблем, 1900.

- $\boxed{\text{ВХОД}}$ диофантово уравнение $P(x_1, \dots, x_n) = 0$;
- $\boxed{\text{ВЫХОД}}$ 1, если $\exists$ решение $a_1, \dots, a_n \in \mathbb{Z} \quad P(a_1, \dots, a_n) = 0$,
  0 иначе.

**Теорема 3** (1970, М.Дэвис, Х.Пантнем, Дж.Робинсон, Ю.В. Матиясевич)**.** 10-я проблема Гильберта неразрешима.

# Литература


[1] И.В. Ашаев – «Основы теории алгоритмов»

[2] Верещагин, Вялый, Шень – «Вычислимые функции»

[3] Китаев, Вялый, Шень – «Классические и квантовые вычисления»