

# **Коллоквиум**

«Алгоритмы и структуры данных»

Если найдете опечатки или неправильность пишите

Автор

18 декабря 2025 г.

## Содержание

<b>1 Понятие временной и пространственной (по памяти) сложности алгоритма. Определение асимптотических сравнений <math>O</math>, <math>\Theta</math>, <math>\Omega</math>. Примеры</b>	<b>4</b>
1.1 Временная и пространственная сложности алгоритма . . . . .	4
1.2 Асимптотические сравнения . . . . .	4
1.3 Примеры . . . . .	5
<b>2 Бинарный поиск. Бинарный поиск по ответу. Временная сложность</b>	<b>6</b>
2.1 Бинарный поиск . . . . .	6
2.2 Бинарный поиск по ответу . . . . .	6
2.3 Временная сложность . . . . .	7
<b>3 Вещественномзначный бинарный поиск (по ответу). Временная сложность</b>	<b>8</b>
3.1 Вещественный бинарный поиск . . . . .	8
3.2 Вещественный бинарный поиск по ответу . . . . .	8
3.3 Сложность вещественного бинарного поиска . . . . .	8
<b>4 Префиксные суммы. Обобщение на произвольную обратимую операцию</b>	<b>9</b>
4.1 Префиксные суммы на массиве . . . . .	9
4.2 Двумерные префиксные суммы . . . . .	9
4.3 Обобщение на многомерный случай . . . . .	10
4.4 Обобщение на произвольную обратимую операцию . . . . .	10
<b>5 Факторизация числа. Функция Эйлера. Сводимость вычисления функции Эйлера к факторизации</b>	<b>11</b>
5.1 Факторизация числа . . . . .	11
5.2 Функция Эйлера . . . . .	11
5.3 Сводимость вычисления функции Эйлера к факторизации . . . . .	12
<b>6 Классическое решето Эратосфена за <math>O(n \log \log n)</math> (время работы б/д). Линейное решето Эратосфена</b>	<b>13</b>
6.1 Решето Эратосфена, время работы . . . . .	13
6.2 Линейное решето Эратосфена . . . . .	13
<b>7 Арифметика в <math>\mathbb{Z}_m</math>. Малая теорема Ферма и теорема Эйлера (б/д). Критерий существования обратного по модулю. Поиск обратного по модулю.</b>	<b>15</b>
7.1 Модульная арифметика . . . . .	15
7.2 Малая теорема Ферма и теорема Эйлера (б/д) . . . . .	16
7.3 Критерий существования обратного по модулю . . . . .	16
7.4 Поиск обратного по модулю . . . . .	16
<b>8 Критерий существования обратного по модулю. Поиск обратного по модулю. Алгоритм Евклида (классический, б/д)</b>	<b>17</b>
8.1 Критерий существования обратного по модулю . . . . .	17
8.2 Поиск обратного по модулю . . . . .	17
8.3 Алгоритм Евклида (классический, б/д) . . . . .	17
<b>9 Амортизированный анализ. Метод монеток. Метод потенциалов. Применение на примере <code>push_back</code> в динамическом массиве</b>	<b>18</b>
9.1 Амортизационный анализ . . . . .	18
9.2 Метод монет . . . . .	18
9.2.1 Принцип . . . . .	18
9.2.2 Пример . . . . .	18
9.3 Метод потенциалов . . . . .	18
9.3.1 Принцип . . . . .	18
9.3.2 Пример . . . . .	19

<b>10 Линейные контейнеры. Односвязный и двусвязный списки. Стек, очередь, дек (через списки и через кольцевой буффер)</b>	<b>20</b>
10.1 Односвязный и двусвязный списки . . . . .	20
10.2 Стек, очередь, дек (через списки и через кольцевой буффер) . . . . .	21
<b>11 Линейные контейнеры. Очередь с поддержкой произвольной ассоциативной операции</b>	<b>23</b>
11.1 Стек с поддержкой минимума . . . . .	23
11.2 Очередь на двух стеках: . . . . .	23
11.3 Очередь с минимумом: . . . . .	23
11.4 Обобщение до произвольной ассоциативной операции . . . . .	24
<b>12 Сортировки. Теорема о нижней границе времени сортировки. Стабильные сортировки</b>	<b>25</b>
12.1 Сортировки . . . . .	25
12.2 Теорема о нижней границе времени сортировки . . . . .	25
12.3 Стабильные сортировки . . . . .	25
<b>13 Сортировка слиянием. Посчёт количества инверсий</b>	<b>26</b>
13.1 Сортировка слиянием . . . . .	26
13.2 Подсчёт количества инверсий . . . . .	26
<b>14 Бинарная пирамида. Определение. Поддержка свойства пирамиды. Основные операции. Пирамидальная сортировка</b>	<b>28</b>
14.1 Определение . . . . .	28
14.2 Основные операции . . . . .	28
14.3 Пирамидальная сортировка . . . . .	30
<b>15 Быстрая сортировка. Процедура Partition <math>O(1)</math> доппамяти. Оценка времени со случайным pivot (б/д)</b>	<b>31</b>
15.1 Быстрая сортировка . . . . .	31
15.2 Разбиения . . . . .	31
15.3 Оценка времени с случайным pivot (б/д) . . . . .	32
<b>16 Поиск порядковой статистики. Оценка времени с случайным pivot</b>	<b>33</b>
<b>17 Медиана медиан. Время поиска медианы медиан. Работа алгоритмов быстрой сортировки и порядковой статистики с использованием медианы медиан</b>	<b>34</b>
17.1 Медиана медиан как pivot. Время работы . . . . .	34
<b>18 Сортировка подсчётом. Стабильный вариант. Алгоритм LSD</b>	<b>36</b>
18.1 Сортировка подсчётом (Counting Sort): . . . . .	36
18.2 Стабильный вариант . . . . .	36
18.3 LSD (Least Significant Digit Sort): . . . . .	36
<b>19 Дополнительные знания, не требуемые для сдачи экзамена</b>	<b>38</b>
19.1 Мастер-теорема о рекурсии . . . . .	38
19.2 Доказательство основной теоремы алгоритма Евклида . . . . .	38

# 1 Понятие временной и пространственной (по памяти) сложности алгоритма. Определение асимптотических сравнений $O$ , $\Theta$ , $\Omega$ . Примеры

## 1.1 Временная и пространственная сложности алгоритма

### Определение 1.1: Временная сложность алгоритма

Временное сложность называется количество операций, выполняемых алгоритмом, в зависимости от входных данных.

### Определение 1.2: Пространственная (по памяти) сложность алгоритма

Пространственной сложностью называется количество памяти, требуемой алгоритмом, в зависимости от входных данных.

## 1.2 Асимптотические сравнения

### Определение 1.3: Асимптотическая положительность

Функция  $f(n)$  является асимптотически положительной, если

$$\exists N_0 : \forall n > N_0, f(n) > 0.$$

### Определение 1.4: Асимптотическая неотрицательность

Функция  $f(n)$  является асимптотически неотрицательной, если

$$\exists N_0 : \forall n > N_0, f(n) \geq 0.$$

### Определение 1.5: $O$ -большое

Рассмотрим множество функций:

$$f(n) \in O(g(n)) \iff \exists N_0 > 0, \exists C > 0 : \forall n \geq N_0 \quad 0 \leq f(n) \leq C \cdot g(n)$$

Говорят что:  $f$  асимптотически не больше, чем  $g$ , или  $f$  не больше, чем  $g$  с точностью до константы. Также можно сказать что  $f$  это  $O$ -большое от  $g$ .

### Определение 1.6: $\Omega$ (Омега)

Рассмотрим множество функций:

$$f(n) \in \Omega(g(n)) \iff \exists N_0 > 0, \exists C > 0 : \forall n \geq N_0 \quad f(n) \geq C \cdot g(n) \geq 0$$

Говорят что:  $f$  не меньше, чем  $g$ , или  $g$  — нижняя оценка для  $f$ . Также можно сказать что  $f$  это  $\Omega$  от  $g$ .

### Определение 1.7: $\theta$ (тета)

Рассмотрим множество функций:

$$f(n) \in \Theta(g(n)) \iff \exists N_0 > 0, \exists C_1 > 0, \exists C_2 > 0 : \forall n \geq N_0 \quad C_1 g(n) \leq f(n) \leq C_2 g(n)$$

Говорят что:  $g(n)$  — асимптотически точная оценка  $f(n)$ . Также можно сказать что  $f$  это  $\Theta$  от  $g$ .

**Аналогии с неравенствами:**

Соотношение	Аналогия
$f(n) = O(g(n))$	$a \leq b$
$f(n) = \Theta(g(n))$	$a = b$
$f(n) = \Omega(g(n))$	$a \geq b$

### 1.3 Примеры

#### Пример 1.1: Временная и пространственная сложность бинарного поиска

Временная сложность:  $O(\log n)$

Пространственная сложность:  $O(1)$  (так как дополнительная память никак не зависит от входных данных)

#### Пример 1.2: Временная и пространственная сложность префиксных сумм

Временная сложность:  $O(n)$

Пространственная сложность:  $O(n)$  (если хотим сохранить исходный массив, создаём новый для префиксных сумм)

#### Пример 1.3: Временная и пространственная сложность дерева отрезков

Временная сложность построения:  $O(n \log n)$

Временная сложность обработки запроса:  $O(\log n)$

Пространственная сложность:  $O(n)$

## 2 Бинарный поиск. Бинарный поиск по ответу. Временная сложность

### 2.1 Бинарный поиск

#### Определение 2.1: Бинарный поиск

Бинарный поиск — алгоритм поиска элемента в отсортированном массиве, который делит поисковый интервал пополам, и продолжает поиск в нужной половине.

#### Алгоритм 2.1: Бинарный поиск

**Вход:** отсортированный массив  $arr$ , элемент  $target$ .

**Выход:** индекс элемента или  $-1$ , если не найден.

#### Реализация 2.1: Бинарный поиск

```
int binary_search(vector<int>& arr, int target) {
    int left = 0, right = arr.size() - 1;
    while (left <= right) {
        int mid = left + (right - left) / 2;
        if (arr[mid] == target) return mid;
        if (arr[mid] < target) left = mid + 1;
        else right = mid - 1;
    }
    return -1;
}
```

### 2.2 Бинарный поиск по ответу

#### Определение 2.2: Бинарный поиск по ответу

Бинарный поиск по ответу — алгоритм поиска ответа в диапазоне, который делит поисковый интервал пополам, и продолжает поиск в нужной половине.

#### Алгоритм 2.2: Бинарный поиск по ответу

**Вход:** отсортированный массив  $arr$ , требование  $target$ .

**Выход:** максимальная дельта между элементами, чтобы  $arr$  делился ровно на  $target$  отрезков.

#### Реализация 2.2: Бинарный поиск по ответу

```
int check(const vector<int>& arr, int max_delta) {
    int count = 1;
    int begin_index = 0;
    for (size_t index = 1; index < arr.size(); ++index) {
        if (arr[index] - arr[begin_index] > max_delta) {
            ++count;
            begin_index = index;
        }
    }
    return count;
}

int binary_search(const vector<int>& arr, int target) {
    int left = 0, right = INT_MAX;
    while (left <= right) {
        int mid = left + ((right - left) >> 1);
        if (target <= check(arr, mid)) {
            left = mid;
        } else {
```

```
        right = mid;
    }
    return left;
}
```

## 2.3 Временная сложность

Рекуррентное соотношение:  $T(n) = T(n/2) + \Theta(1)$ .

По мастер-теореме ( $a = 1, b = 2, c = 0$ , случай 2):  $T(n) = \Theta(\log n)$ .

### 3 Вещественнозначный бинарный поиск (по ответу). Временная сложность

#### 3.1 Вещественный бинарный поиск

Применяется для поиска корней уравнений или решения задач с вещественными числами, где требуется найти значение с заданной точностью.

##### Алгоритм 3.1: Вещественный бинарный поиск (поиск корня)

**Задача:** найти  $\sqrt{n}$  с точностью  $\varepsilon$ .

##### Реализация 3.1: Вещественный бинарный поиск (поиск корня)

```
double sqrt_binary_search(double n, double epsilon = 1e-6) {
    double left = 0, right = n + 1;
    while (right - left > epsilon) {
        double mid = (left + right) / 2;
        if (mid * mid < n) left = mid;
        else right = mid;
    }
    return (left + right) / 2;
}
```

#### 3.2 Вещественный бинарный поиск по ответу

Просто совместить идеи бинарного поиска по ответу и вещественного бинарного поиска

#### 3.3 Сложность вещественного бинарного поиска

Начальный интервал:  $[0, n]$  (длина  $n$ ). На каждой итерации интервал уменьшается в 2 раза. Требуемая точность:  $\varepsilon$ .

Количество итераций  $k$ :  $\frac{n}{2^k} \leq \varepsilon \Rightarrow k \geq \log_2\left(\frac{n}{\varepsilon}\right)$ .

Следовательно,  $T(n) = O\left(\log\left(\frac{n}{\varepsilon}\right)\right)$ .

## 4 Префиксные суммы. Обобщение на произвольную обратимую операцию

### 4.1 Префиксные суммы на массиве

#### Определение 4.1: Префиксные суммы

Префиксная сумма (prefix sum) массива  $a[0..n - 1]$  — это массив  $p[0..n]$ , где:

$$p[i] = \sum_{j=0}^{i-1} a[j] = a[0] + a[1] + \dots + a[i-1]$$

#### Реализация 4.1: Построение префиксных сумм

```
vector<int> build_prefix_sum(vector<int>& arr) {
    vector<int> prefix(arr.size() + 1, 0);
    for (int i = 1; i <= arr.size(); i++) {
        prefix[i] = prefix[i-1] + arr[i-1];
    }
    return prefix;
}
```

**Применение:** быстрое вычисление суммы на отрезке  $[l, r]$ :

$$\text{sum}(l, r) = p[r + 1] - p[l]$$

#### Реализация 4.2: Запрос суммы на отрезке

```
int range_sum(vector<int>& prefix, int l, int r) {
    return prefix[r+1] - prefix[l];
}
```

#### Сложность:

- Построение:  $\Theta(n)$
- Запрос:  $\Theta(1)$
- Память:  $\Theta(n)$

### 4.2 Двумерные префиксные суммы

Для матрицы  $a[m][n]$  строится матрица  $p[m + 1][n + 1]$ , где:

$$p[i][j] = \sum_{x=0}^{i-1} \sum_{y=0}^{j-1} a[x][y]$$

#### Реализация 4.3: Построение двумерных префиксных сумм

```
vector<vector<int>> build_prefix_sums_2d(const vector<vector<int>>& a) {
    int n = a.size();
    int m = a[0].size();
    vector<vector<int>> prefix_sum(n + 1, vector<int>(m + 1, 0));
    for (int i = 0; i < n; i++) {
        for (int j = 0; j < m; j++) {
            prefix_sum[i + 1][j + 1] = prefix_sum[i][j + 1] + prefix_sum[i + 1][j]
            - prefix_sum[i][j] + a[i][j];
        }
    }
    return prefix_sum;
}
```

Сумма в прямоугольнике  $[x_1, y_1]$  до  $[x_2, y_2]$ :

$$sum = p[x_2 + 1][y_2 + 1] - p[x_1][y_2 + 1] - p[x_2 + 1][y_1] + p[x_1][y_1]$$

#### Реализация 4.4: Запрос суммы в прямоугольнике

```
int64_t get_sum(std::vector<std::vector<int>>& pref, int x1, int y1,
                 int x2, int y2) {
    return prefix[x2+1][y2+1] - prefix[x1][y2+1] - prefix[x2+1][y1]
        + prefix[x1][y1];
}
```

### 4.3 Обобщение на многомерный случай

Для обобщения на многомерный случай потребуется формула включения/исключения. Применять по аналогии с одномерным и двумерным случаями в построении и поиске ответа.

### 4.4 Обобщение на произвольную обратимую операцию

#### Определение 4.2: Обратимая операция

Обратимой операцией называется операция, которую можно отменить, применив обратную операцию. Например, для  $*$  отменяющая операция —  $/$ , а для  $\text{xor}$  — сам  $\text{xor}$ .

По аналогии с суммой можно использовать любую другую обратимую операцию. Например, разность, умножение, деление,  $\text{xor}$  и т.д.

## 5 Факторизация числа. Функция Эйлера. Сводимость вычисления функции Эйлера к факторизации

### 5.1 Факторизация числа

#### Определение 5.1: Факторизация числа

Разбиение числа на его простые делители ( $8 = 2 * 2 * 2$ )

#### Алгоритм 5.1: Факторизация числа

**Задача:** Дано число  $n$ . Вывести его в виде произведения простых чисел.

**Идея:** Пройдёмся числом  $i$  по числам от 2 до  $\sqrt{n}$ . Если встретили число, тогда есть 2 варианта:

1.  $i$  - простое число. Если число  $n$  не делится на  $i$ , просто пропускаем это число. Иначе записываем в ответ это число  $i$  столько раз, сколько число  $n$  делится на  $i$ , а потом поделим  $n$  на  $i$  это количество раз. После этого  $n$  не будет делиться на  $i$ . То есть получится, что  $n$  больше не делится ни на одно простое число  $\leq i$ .
2.  $i$  - составное число. Так как это число состоит из произведения простых чисел до  $i$ , а число  $n$  в данный момент не делится ни на одно простое число  $i$ , значит  $n$  гарантированно не делится на число  $i$ . То есть число  $n$  не делится ни на одно число  $\leq i$ , будь то простое или составное.

В итоге получили, что число  $n$  или равно 1, или простое число (так как не делится ни на одно число  $\leq \sqrt{n}$ ), которое мы записываем в ответ.

**Время работы:** если число простое, то  $i$  просто пройдётся по числам от 2 до  $\sqrt{n}$ , что в итоге составит сложность  $O(\sqrt{n})$ . Если не простое, то получаем сложность не хуже  $i + T(\frac{n}{2^i})$ , что  $T(n)$ , значит меньше худшего случая, где  $n$  - простое число. (Лучшем случае будет степень двойки, тогда сложность будет равна  $O(\log n)$ )

#### Реализация 5.1: Факторизация числа

```
std::vector<int> factorization(int number) {
    std::vector<int> answer;
    int num = 2;
    while (num * num <= number) {
        while (!(number % num)) {
            answer.push_back(num);
            number /= num;
        }
        ++num;
    }
    return answer;
}
```

### 5.2 Функция Эйлера

#### Определение 5.2: Функция Эйлера

Функция Эйлера  $\varphi(a)$  определяется для всех целых положительных  $a$  и представляет собою количество чисел ряда  $0, 1, \dots, a - 1$ , взаимно простых с  $a$ .

### 5.3 Сводимость вычисления функции Эйлера к факторизации

**Теорема 5.1:** Формула для функции Эйлера

$$\varphi(a) = a \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

где  $p_1, p_2, \dots, p_k$  — различные простые делители числа  $a$ .

**Пример:**  $\varphi(60) = 60 \cdot (1 - 1/2) \cdot (1 - 1/3) \cdot (1 - 1/5) = 60 \cdot 1/2 \cdot 2/3 \cdot 4/5 = 16$ .

**Задача 5.1:** Выведение формулы Эйлера

1. Рассмотрим простой случай:  $n$  - простое число (то есть  $n = p$ ). Очевидно, для любого простого числа количество чисел, взаимно простых с ним и меньших него равно  $p - 1$ .
2. Теперь пусть  $n = p^\alpha$ . Тогда числа, не взаимно простые с  $n$  и меньшие его - все числа, делящиеся на  $p$ . Таких ровно  $\frac{p^\alpha}{p} = p^{\alpha-1}$ . Тогда  $\varphi(n) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p - 1)$
3. Так как функция Эйлера мультипликативна (то есть  $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ ), если  $n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$ . Тогда  $\varphi(n) = \varphi(p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1}) \cdot \dots \cdot \varphi(p_k^{\alpha_k}) = n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_k})$

## 6 Классическое решето Эратосфена за $O(n \log \log n)$ (время работы б/д). Линейное решето Эратосфена

### 6.1 Решето Эратосфена, время работы

#### Алгоритм 6.1: Решето Эратосфена

Для составления таблицы простых чисел, не превосходящих данного целого  $N$ :

1. Выписываем числа  $1, 2, \dots, N$ .
2. Первое, большее 1 число этого ряда есть 2. Оно делится только на 1 и само на себя и, следовательно, оно простое.
3. Вычеркиваем все кратные двум до  $N$ .
4. Теперь первое не вычеркнутое число есть 3. Оно не делится на 2. Оно простое, вычеркиваем все кратные 3.
5. И т.д.

#### Реализация 6.1: Решето Эратосфена

```
std::vector<int> Erat(int num) {
    std::vector<int> erat(num + 1, 0);
    for (int index = 2; index * index <= num; ++index) {
        if (!erat[index]) {
            for (int index1 = index * index; index1 <= num; index1 += index) {
                erat[index1] = 1;
            }
        }
    }
    return erat;
}
```

#### Корректность:

Когда указанным способом будут вычеркнуты все числа кратные простым, меньших простого  $p$ , то все невычеркнутые, меньшие  $p^2$ , будут простыми. Действительно, всякое составное  $a$ , меньшее  $p^2$ , нами уже вычеркнуто как кратное его наименьшего простого делителя, который  $\leq \sqrt{a} < p$ .

#### Полезное примечание:

- При вычеркивании кратных простого  $p$ , это вычеркивание следует начинать с  $p^2$ .
- Составление таблицы простых чисел, не превосходящих  $N$ , будет закончено, когда вычеркнуты все составные кратные простым, не превосходящим  $\sqrt{N}$ .

**Время работы решета Эратосфена:**  $O(n \log \log n)$  (без доказательства).

### 6.2 Линейное решето Эратосфена

#### Реализация 6.2: Решето Эратосфена

```
std::vector<int> Erat(int num) {
    std::vector<int> erat(num + 1, 0);
    std::vector<int> primes;
    for (size_t index = 2; index <= num; ++index) {
        if (erat[index] == 0) {
            primes.push_back(index);
            erat[index] = index;
        }
        for (size_t jndex = 0; jndex < primes.size() && primes[jndex] <
             erat[jndex] && index * primes[jndex] <= num; ++jndex) {
            erat[index * primes[jndex]] = primes[jndex];
        }
    }
}
```

```
    return erat;
}
```

**Идея:**

Каждое составное число должно быть вычеркнуто 1 раз. Для этого пройдёмся по массиву и каждому числу запишем его наименьший делитель (см. реализацию)

**Корректность:**

Это довольно сложная тема, в которой я до конца не разобрался. Буду рад, если разъясните в личке, но на экзамене скорее всего такого не спросят. Если спросят, скорее всего вам попался Костя, поэтому соболезную)

**Время работы:**

$O(n)$  ( $6/\Delta$ )

## 7 Арифметика в $\mathbb{Z}_m$ . Малая теорема Ферма и теорема Эйлера (б/д). Критерий существования обратного по модулю. Поиск обратного по модулю.

### 7.1 Модульная арифметика

#### Определение 7.1: Сравнимость по модулю

Два целых  $a$  и  $b$  называются равноостаточными по модулю  $m$  или сравнимыми по модулю  $m$ , если они дают одинаковый остаток при делении на  $m$ . Сравнимость чисел  $a$  и  $b$  по модулю  $m$  записывается так:

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

#### Реализация 7.1: Модульная арифметика

```
const int64_t MOD = 1e9 + 7;

int64_t BinPow(int64_t a, int64_t n) {
    if (n == 1) {
        return a % MOD;
    }
    if (n % 2) {
        return (a * BinPow(a, n - 1)) % MOD;
    }
    int64_t ans = BinPow(a, n / 2);
    return ans * ans % MOD;
}

int64_t InverseModulo(int64_t a) {
    return BinPow(a, MOD - 2);
}

int64_t PlusMod(int64_t a, int64_t b) {
    return (a + b) % MOD;
}

int64_t MinusMod(int64_t a, int64_t b) {
    return (a - b + MOD) % MOD;
}

int64_t MultiplyMod(int64_t a, int64_t b) {
    return (a * b) % MOD;
}

int64_t DivideMod(int64_t a, int64_t b) {
    return (a * InverseModulo(b)) % MOD;
}
```

#### Алгоритм 7.1: Быстрое возведение в степень

**Задача:** Нужно возвести число  $a$  в степень  $n$  по простому модулю  $m$

**Реализация:** см. выше

**Идея:** если у нас  $n$  чётная, то  $a^n$  можно записать как  $(a^{n/2})^2$ , вычислить рекурсивно  $a^{n/2}$  и полученный ответ возвести в квадрат за  $O(1)$ . В итоге мы каждый раз (в худшем случае через раз) делим степень на 2 и рекурсивно получаем ответ, поэтому

**Временная сложность:**  $O(\log n)$

## 7.2 Малая теорема Ферма и теорема Эйлера (б/д)

### Теорема 7.1: Теорема Эйлера

Если  $\gcd(a, m) = 1$ , то

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

### Теорема 7.2: Малая теорема Ферма

Частный случай теоремы Эйлера для простого  $p$ : если  $\gcd(a, p) = 1$ , то

$$a^{p-1} \equiv 1 \pmod{p}$$

## 7.3 Критерий существования обратного по модулю

### Теорема 7.3: Критерий существования обратного по модулю

Обратное число  $x$  числу  $a$  по модулю  $m$  существует тогда и только тогда, когда  $a$  и  $m$  взаимо просты.

**Необходимость:** Пусть  $\text{НОД}(a, m) = d$ . Тогда  $ax \equiv 1 \pmod{m} \Leftrightarrow ax - mk = 1$ . Т.к. и  $a$ , и  $m$  делится на  $d$ , всё выражение  $ax - mk$  делится на  $d$ , значит и 1 делится на  $d$ , но единственный делитель 1 — само число 1. Значит  $d = 1$

**Достаточность:**  $\text{НОД}(a, m) = 1 \Rightarrow \exists u, v : au + mv = 1$ . Рассмотрим это уравнение по модулю  $m$ . Так как  $mv \equiv 0 \pmod{m}$ ,  $au \equiv 1 \pmod{m}$ . Ч.Т.Д.

## 7.4 Поиск обратного по модулю

**Идея:** Рассмотрим частный случай простого модуля  $p$ . По малой теореме Ферма:  $a^{p-1} \equiv 1 \pmod{p}$ , следовательно,  $a^{p-2} \equiv a^{-1} \pmod{p}$ . Тогда, используя быстрое возведение в степень, найдём  $a^{p-2}$ , что и будет являться обратным по простому модулю  $p$  для числа  $a$ . Сложность алгоритма для простого модуля:  $O(\log n)$

Теперь рассмотрим общий случай не простого модуля  $m$ . По теореме Эйлера:  $a^{\varphi(m)} \equiv 1 \pmod{m}$ , следовательно,  $a^{\varphi(m)-1} \equiv a^{-1} \pmod{m}$ . Тогда, найдя  $\varphi(m)$  за  $\sqrt{m}$  через факторизацию числа, и используя быстрое возведение в степень, получим обратное по модулю  $m$ . Сложность такого алгоритма:  $O(\sqrt{m} + \log n)$

## 8 Критерий существования обратного по модулю. Поиск обратного по модулю. Алгоритм Евклида (классический, б/д)

### 8.1 Критерий существования обратного по модулю

См. выше

### 8.2 Поиск обратного по модулю

См. выше

### 8.3 Алгоритм Евклида (классический, б/д)

#### Теорема 8.1: Основная теорема алгоритма Евклида

Если  $a = bq + r$ , то  $(a, b) = (b, r)$ .

#### Алгоритм 8.1: Алгоритм Евклида

Пусть  $a$  и  $b$  — положительные целые, и  $a > b$ , тогда по теореме о делении с остатком получим систему равенств:

$$\begin{aligned} a &= bq_1 + r_2, \quad 0 < r_2 < b \\ b &= r_2q_2 + r_3, \quad 0 < r_3 < r_2 \\ r_2 &= r_3q_3 + r_4, \quad 0 < r_4 < r_3 \\ &\vdots \end{aligned}$$

Этот ряд можно продолжать пока не получим 0. Заметим, что:

$$(a, b) = (b, r_2) = (r_2, r_3) = \dots = (r_{n-1}, r_n) = r_n$$

#### Алгоритм 8.2: Реализация алгоритма Евклида

#### Реализация 8.1: Алгоритм Евклида

```
int euclid(int a, int b) {
    while (a && b) (a > b ? a %= b : b %= a);
    return a + b;
}
```

**Сложность алгоритма Евклида:**  $O(\log(\min(a, b)))$ .

## 9 Амортизированный анализ. Метод монеток. Метод потенциалов. Применение на примере push\_back в динамическом массиве

### 9.1 Амортизационный анализ

#### Определение 9.1: Амортизационный анализ

Пусть наша программа состоит из элементарных кусков (операций),  $i$ -й из которых работает  $t_i$ .

- Реальное время –  $t_i$
- Среднее время –  $t_{\text{avg}} = \frac{\sum_i t_i}{n}$
- Амортизированное время одной операции –  $a_i = t_i + \Delta\varphi_i$

### 9.2 Метод монет

#### 9.2.1 Принцип

#### Определение 9.2

В методе в ходе группового анализа, разные операции оцениваются по-разному, в зависимости от их фактической стоимости. Величина, которая начисляется на операцию, называется амортизированной стоимостью (amortized cost). Если амортизированная стоимость операции превышает ее фактическую стоимость, то соответствующая разность присваивается определенным объектам структуры данных как кредит (credit). Кредит можно использовать впоследствии для компенсирующих выплат на операции, амортизированная стоимость которых меньше их фактической стоимости.

**Важно:** К выбору стоимости стоит подходить осторожно. Должно выполняться соотношение:

$$\sum_i a_i \geq \sum_i t_i$$

То есть полный кредит в любой момент времени должен быть неотрицательным.

#### 9.2.2 Пример

#### Задача 9.1: push\_back

**Задача:** доказать, что push\_back в динамическом массиве работает за  $O^*(1)$

**Решение:** применим метод монет:

Если в данный момент есть место для вставки элемента, сделаем это и добавим в банк 2 монеты (за выделение места под 2 элемента в будущем). Когда у нас закончится место, заберём деньги из банка и пустем их на выделение места под новые элемента. Это нам ничего не зудет стоить. Поэтому амортизированно у нас push\_back будет работать за  $O^*(1)$ .

### 9.3 Метод потенциалов

#### 9.3.1 Принцип

#### Определение 9.3: Метод потенциалов

Функция потенциала  $\varphi$  — отображает структуру данных  $D_i$  на действительное число  $\varphi(D_i)$ , которое является потенциалом, связанным со структурой данных. Амортизированная стоимость  $i$ -ой операции:

$$a_i = t_i + \varphi(D_i) - \varphi(D_{i-1})$$

**Соотношение:**

$$\sum_i a_i = \sum_i (t_i + \varphi(D_i) - \varphi(D_{i-1})) = \sum_i t_i + \varphi(D_n) - \varphi(D_0)$$

Если потенциал можно определить так, что  $\varphi(D_n) - \varphi(D_0) \geq 0$ , то суммарная амортизированная стоимость даст верхнюю границу полной фактической стоимости.

**Соотношение:** Если потребовать  $\varphi(D_i) \geq \varphi(D_0), \forall i$ , то мы как и в методе бухучета получим предоплату операций.

### 9.3.2 Пример

**Задача 9.2: push\_back**

**Задача:** доказать, что `push_back` в динамическом массиве работает за  $O^*(1)$

**Решение:** применим метод потенциалов:

Пусть  $\varphi(D) = 2 \cdot \text{size} - \text{capacity}$

Тогда:

1. Без переаллокации памяти:  $a_i = 1 + 2 \cdot (\text{size} + 1) - \text{capacity} - 2 \cdot \text{size} + \text{capacity} = 3$
2. С переаллокированием памяти:  $a_i = 1 + 2 \cdot (\text{size} + 1) - \text{capacity} \cdot 2 - 2 \cdot \text{size} + \text{capacity} \cdot 2 = 3$

## 10 Линейные контейнеры. Односвязный и двусвязный списки. Стек, очередь, дек (через списки и через кольцевой буффер)

### 10.1 Односвязный и двусвязный списки

#### Определение 10.1: Односвязный список

Односвязный список — последовательный набор из узлов с данными, где каждый узел знает, где лежит следующий за ним.

#### Реализация 10.1: Односвязный список

```
struct Node {
    int val;
    Node* next;

    Node(int _val) : val(_val), next(nullptr) {}

};

struct list {
    Node* first;
    Node* last;

    list() : first(nullptr), last(nullptr) {}

    bool is_empty() {
        return first == nullptr;
    }

    void push_back(string _val) {
        Node* p = new Node(_val);
        if (is_empty()) {
            first = p;
            last = p;
            return;
        }
        last->next = p;
        last = p;
    }

    void print() {
        if (is_empty()) return;
        Node* p = first;
        while (p) {
            cout << p->val << " ";
            p = p->next;
        }
        cout << endl;
    }
}
```

#### Определение 10.2: Двусвязный список

Двусвязный список — последовательный набор из узлов с данными, где каждый узел знает, где лежат следующий и предыдущий узлы.

#### Реализация 10.2: Двусвязный список

```
struct Node {
    int val;
    Node* next;
    Node* before;

    Node(int _val) : val(_val), next(nullptr), before(nullptr) {}

};
```

```

struct list {
    Node* first;
    Node* last;

    list() : first(nullptr), last(nullptr) {}

    bool is_empty() {
        return first == nullptr;
    }

    void push_back(string _val) {
        Node* p = new Node(_val);
        if (is_empty()) {
            first = p;
            last = p;
            return;
        }
        last->next = p;
        p->before = last;
        last = p;
    }

    void print() {
        if (is_empty()) return;
        Node* p = first;
        while (p) {
            cout << p->val << " ";
            p = p->next;
        }
        cout << endl;
    }
}

```

## 10.2 Стек, очередь, дек (через списки и через кольцевой буффер)

### Определение 10.3: Стек (stack)

Стек — АТД, который хранит элементы и предоставляет к ним доступ в рамках парадигмы LIFO (Last in, First Out).

### Определение 10.4: Очередь (queue)

Очередь — АТД, который хранит элементы и предоставляет к ним доступ в рамках парадигмы FIFO (First in, First Out).

### Определение 10.5: Дек (dequeue)

Дек — АТД, который представляет из себя двустороннюю очередь, то есть можно вставлять/удалять в начало/конец.

### Задача 10.1: Дек через списки

**Идея:** Дек можно реализовать с помощью двусвязного списка с операциями добавления в начало/конец и удаления из начала/конца. Однако при такой реализации обращение к элементу дека будет работать за  $O(n)$ , что подходит под требования, написанные в определении, однако это нас не устраивает, поэтому дек можно реализовать с помощью циклического буфера.

### Задача 10.2: Дек через циклический буффер

**Идея:** Будем заполнять циклический буффер, пока есть место, если место закончилось и мы хотим добавить элемент, расширим capacity в два раза (по аналогии с динамическим массивом), и продолжим заполнение. Для лучшего понимания см. реализацию

**Реализация 10.3: Дек на циклическом буффере**

```
struct RingBuffer{
    void reserve(int new_cap) {
        if (new_cap <= capacity) {
            return;
        }
        int* tmp = new int[new_cap];
        for (int index = 0; index < size; ++index) {
            tmp[index] = data[(begin + index) % capacity];
        }
        delete[] data;
        begin = 0;
        capacity = new_cap;
        data = tmp;
    }

    void push_back(int elem) {
        if (size == capacity) {
            reserve(capacity * 2);
        }
        data[(begin + size) % capacity] = elem;
        ++size;
    }

    void push_front(int elem) {
        if (size == capacity) {
            reserve(capacity * 2);
        }
        begin = (begin + capacity - 1) % capacity;
        data[begin] = elem;
        ++size;
    }

    void pop_back() {
        if (size == 0) {
            return;
        }
        --size;
    }

    void pop_front() {
        if (size == 0) {
            return;
        }
        --size;
        begin = (begin + 1) % capacity;
    }

    int size = 0;
    int begin = 0;
    int capacity = 1;
    int* data = new int[1];
};
```

## 11 Линейные контейнеры. Очередь с поддержкой произвольной ассоциативной операции

### 11.1 Стек с поддержкой минимума

Давайте добавим к интерфейсу стека еще возможность возвращать минимум в нем. Будем хранить в узле стека не только сам элемент, но еще и минимум в стеке. При добавлении нового элемента в стек  $S$  для получения стека  $S'$  будем в голову  $S'$  добавлять минимум как минимум из значения элемента и значения минимума в голове  $S'$ .

#### Алгоритм 11.1: Идея реализации

Будем просто поддерживать стек, в котором первым элементом хранить сам элемент, а вторым - текущий минимум. При добавлении элемента новым минимумом будет или он или предыдущий элемент. Так как у нас есть доступ только к верхнему элементу, остальные минимумы пересчитывать не надо

#### Реализация 11.1: Минимум на стеке

```
#include <stack>

struct MinStack {
public:
    void Push(int element) {
        int min_element = (data_.empty() ? element :
                           std::min(data_.top().second, element));
        data_.push({element, oper_element});
    }
    void Pop() {
        if (!data_.empty()) {
            data_.pop();
        }
    }
    int Top() {
        if (data_.empty()) {
            return -1;
        }
        return data_.top().first;
    }
    int Get() {
        if (data_.empty()) {
            return -1;
        }
        return data_.top().second;
    }
    bool Empty() {
        return data_.empty();
    }
private:
    std::stack<std::pair<int, int>> data_;
}
```

### 11.2 Очередь на двух стеках:

Задача. Дан стек в виде черного ящика. Надо соорудить очередь. Одного стека не хватит, воспользуемся двумя. Сделаем один стек на вход `stack_in` и второй на выход `stack_out`. В первый будем добавлять, а из второго — извлекать. Если при извлечении `stack_out` пуст, то перекидываем все элементы из `stack_in` в `stack_out`.

### 11.3 Очередь с минимумом:

Задача. Сделать очередь с поддержкой операции получения минимума в ней. Заведем очередь на двух стеках, поддерживающих минимум. Запрос минимума сводится к минимуму из минимумов в двух стеках.

**Алгоритм 11.2: Идея реализации**

Сделаем стек на минимуме, но когда удаляем элемент, будем удалять тот, что лежит в обратном стеке. Если он пустой, по "перельём" все элементы из основного стека в обратный. В итоге они будут иметь обратный порядок и ударяя верхний элемент в обратном стеке мы фактически будем удалять нижний элемент в обычном стеке.

**Реализация 11.2: Минимум на очереди**

```
#include<stack>
struct MinQueue {
public:
    void Push(int element) {
        in_data_.Push(element);
    }
    void Pop() {
        if (out_data_.Empty()) {
            while (!in_data_.Empty()) {
                out_data_.Push(in_data_.Top());
                in_data_.Pop();
            }
        }
        if (out_data_.Empty()) {
            return;
        }
        out_data_.Pop();
    }
    int GetMin() {
        if (out_data_.Empty() && in_data_.Empty()) {
            return 0;
        }
        if (out_data_.Empty()) {
            return in_data_.GetMin();
        }
        if (in_data_.Empty()) {
            return out_data_.GetMin();
        }
        return std::min(in_data_.GetMin(), out_data_.GetMin());
    }
    bool Empty() {
        return in_data_.Empty() && out_data_.Empty();
    }
private:
    MinStack out_data_;
    MinStack in_data_;
}
```

**11.4 Обобщение до произвольной ассоциативной операции**

По аналогии с минимумом можно использовать любую ассоциативную операцию, будут небольшие различия в реализации (например, под такую реализацию можно легко подставить плюс в качестве ассоциативной операции, однако для минуса реализация будет немного отличаться)

## 12 Сортировки. Теорема о нижней границе времени сортировки. Стабильные сортировки

### 12.1 Сортировки

#### Постановка задачи:

Имеется последовательность из  $n$  элементов  $x_1, \dots, x_n$ . Необходимо упорядочить элементы по неубыванию (невозрастанию), для удобства далее будем везде сортировать по неубыванию.

Значит нужно найти перестановку элементов:  $p_1, p_2, p_3, \dots, p_n$ , т. ч.  $x_{p_1} \leq x_{p_2} \leq \dots \leq x_{p_n}$ .

### 12.2 Теорема о нижней границе времени сортировки

#### Определение 12.1: Сортировка, основанная на сравнениях

Сортировку называют основанной на сравнениях, если она работает в следующем предположении: объекты можно только сравнивать.

#### Теорема 12.1: Нижняя оценка сортировки сравнениями

Сортировка, основанная на сравнениях, работает за  $\Omega(N \log N)$ .

#### Доказательство:

Необходимо найти единственную корректную перестановку среди их множества — всего есть  $O(n!)$ .

Всё что мы можем сделать это сравнить два элемента и понять, нужно ли их переставить. Число перестановок, которые остаются к исследованию:  $\frac{n!}{2}$ .

Тогда  $T(n) \geq \log(n!) = \Omega(n \log n)$ .

#### Теорема 12.2: лемма о факториале

$$\log N! = \Theta(N \log N)$$

#### Доказательство:

По формуле Стирлинга:

$$\log N! \sim \log \sqrt{2\pi n} \left(\frac{n}{e}\right)^n = \frac{1}{2} \log(2\pi n) + n \log n - n \log e = \Theta(N \log N)$$

### 12.3 Стабильные сортировки

#### Определение 12.2: Устойчивость (стабильность) сортировки

Устойчивость (стабильность) сортировки говорит о том, что элементы, одинаковые для сравнения, не поменяют своего расположения относительно друг друга после сортировки.

## 13 Сортировка слиянием. Посчёт количества инверсий

### 13.1 Сортировка слиянием

**Идея «Разделяй и властвуй»:**

1. Разбить массив на две примерно равные половины.
2. Решить все подзадачи, применив рекурсивно шаги 1 и 3, пока не дойдем до базы, в которой все тривиально (разбиваем массивы и дальше пополам, пока не дойдем до массива из одного элемента).
3. Объединить решения подзадач (слить два отсортированных массива в один большой).

#### Слияние двух отсортированных массивов:

Если у нас есть два отсортированных массива — можно их слить в третий, который будет тоже отсортирован за  $O(n+m)$ , где  $n, m$  — размеры массивов. Достигается это методом двух указателей.

#### Анализ сортировки слиянием:

Время работы составит  $n \log(n)$ , согласно мастер-теореме о рекурсии:  $T(n) = 2T(n/2) + n \Rightarrow T(n) = \Theta(n \log n)$ .

Потребляемая память составит  $O(n)$ , поскольку необходимо завести массив для слияний. Также алгоритму нужно  $O(\log n)$  стековой памяти для хранения параметров рекурсивных вызовов.

К счастью, алгоритм можно реализовать итеративно и без рекурсии, начав решать задачу снизу-вверх: сначала сливаем соседние массивы размеров 1, затем размеров 2, затем 4, и так далее.

#### Реализация 13.1: Сортировка Слиянием

```
vector<int> Merge(std::vector<int> lhs, std::vector<int> rhs) {
    std::vector<int> answer(lhs.size() + rhs.size());
    size_t lhs_index = 0;
    size_t rhs_index = 0;
    while (lhs_index != lhs.size() || rhs_index != rhs.size()) {
        if (lhs_index == lhs.size()) {
            answer[lhs_index + rhs_index] = rhs[rhs_index++];
        } else if (rhs_index == rhs.size()) {
            answer[lhs_index + rhs_index] = lhs[lhs_index++];
        } else {
            if (lhs[lhs_index] <= rhs[rhs_index]) {
                answer[lhs_index + rhs_index] = lhs[lhs_index++];
            } else {
                answer[lhs_index + rhs_index] = rhs[rhs_index++];
            }
        }
    }
    return answer;
}
// vec - [0, n)
std::vector<int> MergeSort(const std::vector<int>& vec, size_t left_index,
size_t right_index) {
    if (right_index - left_index == 1) {
        return {vec[left_index]};
    }
    size_t min_index = (right_index + left_index) / 2;
    auto sorted_segment_1 = MergeSort(vec, left_index, mid_index);
    auto sorted_segment_2 = MergeSort(vec, mid_index, right_index);
    return Merge(sorted_segment_1, sorted_segment_2);
}
```

### 13.2 Подсчёт количества инверсий

**Идея:** при сортировке слиянием будем проверять на новые инверсии: если элемент с индексом  $j$  из правого массива оказался меньше элемента из левого с индексом  $i$  (в ходе их сравнения), то все элементы, начиная с элемента  $i$  образуют инверсии с элементом  $j$  из правого массива. Значит к ответу нам надо прибавить  $lhs.size() - i$  (количество элементов после  $i$ , включая сам  $i$ ).

### Реализация 13.2: Сортировка слиянием с подсчётом инверсий

```

int Merge(std::vector<int>& vec, int left_st, int left_end, int right_st, int
right_end) {
    int answer = 0;
    int l_index = left_st;
    int r_index = right_st;
    std::vector<int> ans;
    ans.reserve(left_end - left_st + right_end - right_st);
    while (l_index != left_end || r_index != right_end) {
        if (l_index == left_end) {
            ans.push_back(vec[r_index]);
            ++r_index;
        } else if (r_index == right_end) {
            ans.push_back(vec[l_index]);
            ++l_index;
        } else {
            if (vec[l_index] <= vec[r_index]) {
                ans.push_back(vec[l_index]);
                ++l_index;
            } else {
                answer += (left_end - l_index);
                ans.push_back(vec[r_index]);
                ++r_index;
            }
        }
    }
    for (int index = left_st; index < left_end; ++index) {
        vec[index] = ans[index - left_st];
    }
    for (int index = right_st; index < right_end; ++index) {
        vec[index] = ans[index + left_end - left_st - right_st];
    }
    return answer;
}

int MergeSort(std::vector<int>& vec, int left, int right) {
    if (right - left == 1) {
        return 0;
    }
    int mid = left + (right - left) / 2;
    int ans1 = MergeSort(vec, left, mid);
    int ans2 = MergeSort(vec, mid, right);
    return ans1 + ans2 + Merge(vec, left, mid, mid, right);
}

```

P.S. Здесь используется не стандартное слияние двух отсортированных массивов, а слияние двух отсортированных отрезков одного массива.

## 14 Бинарная пирамида. Определение. Поддержка свойства пирамиды. Основные операции. Пирамидальная сортировка

### 14.1 Определение

#### Определение 14.1: Двоичная куча (пирамида)

Двоичная куча (пирамида) — подвешенное бинарное дерево, обладающее следующими свойствами:

- Значение элемента в каждой вершине не меньше, чем значения в потомках.
- На  $i$ -ом (нумерация ведется с нуля) ярусе дерева, кроме быть может последнего —  $2^i$  вершин
- Последний слой заполнен слева направо

**Замечание:** При желании можно вместо бинарной пирамиды использовать  $k$ -ичную пирамиду (например тернарную). Это уменьшает число ярусов дерева, необходимых для хранения элементов. На основе бинарной пирамиды можно реализовать очередь с приоритетом.

#### Лемма 14.1: Высота бинарной кучи

Число ярусов (высота) бинарной кучи из  $n$  элементов можно оценить, как  $O(\log n)$ .

**Доказательство:** Рассмотрим все ярусы кучи, без последнего. Тогда у нас имеется полная бинарная куча в которой  $k < n$  элементов и ее высота на 1 меньше. У такой кучи каждый следующий ярус содержит в два раза больше элементов. Пусть высота этой кучи равна  $h$ . Тогда:

$$k = \sum_{i=0}^{h-1} 2^i = 2^h - 1$$

Из этого следует, что  $h \leq \log_2 k$ . Поскольку исходная куча содержит на 1 ярус больше, ее высоту можно оценить как  $O(\log n)$ .

#### Хранение в памяти:

Хранить кучу удобно в массиве (используем 0-индексацию). Пусть мы рассматриваем элемент с индексом  $i$ :

- Индекс левого ребенка:  $2i + 1$
- Индекс правого ребенка:  $2i + 2$
- Индекс родителя:  $\lfloor \frac{i-1}{2} \rfloor$
- Элементы, которые являются листами, имеют индексы  $\lceil \frac{n}{2} \rceil \dots n - 1$

### 14.2 Основные операции

#### Операция Sift Up (Просеивание вверх):

Сравним элемент с родительским элементом, если он меньше — поменяем их местами. Продолжим выполнение операции до тех пор, пока родитель не окажется больше или равным значению нашего элемента, либо пока элемент не станет корнем.

#### Операция Sift Down (Просеивание вниз):

Сравним элемент с дочерними элементами, если один из них больше, чем этот элемент, поменяем местами с большим из дочерних элементов. Продолжим выполнение операции до тех пор, пока элемент не окажется больше всех детей или не окажется листом.

#### Основные операции:

1. **Вставка:** Имеется куча (возможно, пустая), мы хотим добавить в нее элемент. Свойства кучи позволяют только добавить его на последний ярус. Такое добавление может нарушить свойства кучи: добавленный элемент может оказаться больше родителя. Исправить проблему возможно, если выполнить операцию SiftUp. Операция будет работать за  $O(\log n)$ .

2. **Извлечение максимума:** Имеется непустая куча, хотим извлечь максимальный элемент. Исходя из свойств кучи максимум всегда находится в корне. Также согласно свойствам кучи (все ярусы кроме последнего должны быть заполнены), на место извлекаемого элемента необходимо что-то поставить. Для этого подойдет последний элемент последнего яруса, но он может оказаться меньше какого-либо из детей корня. Исправить проблему возможно, если выполнить операцию sift down. Операция будет работать за  $O(\log n)$ .
3. **Increase/Decrease key:** Имея доступ к произвольному ключу можно поменять его значение. Операция будет работать за  $O(\log n)$ .

#### Построение кучи:

Можно построить за  $O(n \log n)$ , просто сделав  $n$  операций вставки. Можно сделать умнее (за  $O(n)$ ). Давайте с поочередно от элемента с индексом  $\frac{n}{2}$  до начала массива вызывать операцию SiftDown. Это будет работать, так как кучи из 1 вершины корректны, а далее мы восстанавливаем кучи из  $k + 1$  элемента и т. д.

#### Теорема 14.1: Построение кучи за $O(n)$

Построение бинарной кучи из  $n$  элементов (методом, описанным выше) работает за  $O(n)$ .

#### Реализация 14.1: Реализация бинарной кучи

```

struct Heap {
    public:
        Heap (const std::vector<int>& arr) : data_(arr) {
            for (size_t index = arr.size(); index + 1 > 0; ++index) {
                SiftDown(index);
            }
        }
        void Insert(const int& number) {
            data_.push_back(number);
            SiftUp(number);
        }
        int EraseMax() {
            std::swap(data_[0], data_.back());
            int answer = data_.back();
            data_.pop_back();
            SiftDown(0);
            return answer;
        }
    private:
        void SiftDown(size_t index) {
            if (((index + 1) << 1) >= data_.size()) {
                return;
            }
            size_t lchild = (index << 1) + 1;
            size_t rchild = (index << 1) + 2;
            if (data_[index] < data_[lchild]) {
                if (data_[index] < data_[rchild]) {
                    std::swap(data_[index], data_[rchild]);
                    SiftDown(rchild);
                } else {
                    std::swap(data_[index], data_[lchild]);
                    SiftDown(lchild);
                }
            } else {
                std::swap(data_[index], data_[lchild]);
                SiftDown(lchild);
            }
        } else if (data_[index] < data_[rchild]) {
            std::swap(data_[index], data_[rchild]);
            SiftDown(rchild);
        }
    }
    void SiftUp(size_t index) {
        if (index == 0) {
            return;
        }
        if (data_[index] > data_[((index - 1) >> 1)]) {

```

```

        std::swap(data_[index], data_[((index - 1) >> 1)]);
        SiftUp(((index - 1) >> 1));
    }
    std::vector<int> data_;
};
```

### 14.3 Пирамидальная сортировка

**Алгоритм:**

- Хотим отсортировать массив  $A$  по неубыванию.
- Построим бинарную кучу (на максимум) на основе массива  $A$  (в самом массиве, т. е. *inplace*).
- Будем извлекать по очереди элементы пирамиды и ставить их в конец массива (это возможно, поскольку после извлечения из пирамиды в конце массива образуется неиспользованная ячейка).
- В итоге получим отсортированный массив.

**Анализ:**

- Время работы пирамидальной сортировки составляет  $O(n \log n)$
- Потребление доп. памяти пирамидальной сортировки составляет  $O(1)$  (если не использовать рекурсию для реализации кучи)
- Сортировка не является устойчивой.

Первое верно, так как извлечение из кучи составляет  $O(\log n)$ . Второе — поскольку все операции можно без создания дополнительных массивов. Третье, поскольку в пирамиде равные элементы могут уйти в разные поддеревья пирамиды.

**Примечание:** Пирамида основана только на сравнениях  $\Rightarrow$  сортировка тоже основана на сравнениях. Заметим, что она работает за  $O(n \log n)$  даже в худшем случае.

#### Реализация 14.2: Heapsort

```

void heapify(int arr[], int n, int i){
    int largest = i;
    int l = 2 * i + 1;
    int r = 2 * i + 2;
    if (l < n && arr[l] > arr[largest])
        largest = l;
    if (r < n && arr[r] > arr[largest])
        largest = r;
    if (largest != i) {
        swap(arr[i], arr[largest]);
        heapify(arr, n, largest);
    }
}

void heapSort(int arr[], int n) {
    for (int i = n / 2 - 1; i >= 0; i--)
        heapify(arr, n, i);
    for (int i = n - 1; i >= 0; i--) {
        swap(arr[0], arr[i]);
        heapify(arr, i, 0);
    }
}
```

## 15 Быстрая сортировка. Процедура Partition $O(1)$ доппамяти. Оценка времени со случайным pivot (б/д)

### 15.1 Быстрая сортировка

Алгоритм быстрой сортировки:

1. Как-нибудь выберем опорный элемент pivot (важно: значение должно присутствовать в массиве, например можно брать самый правый/самый левый/центральный).
2. Разобьем массив на две части, в одной все элементы больше или равны pivot, в другой меньше.
3. Поставим pivot на границе раздела (во избежание бесконечной рекурсии).
4. Рекурсивно решим две образованные подзадачи (шаги 1-3).

### 15.2 Разбиения

Разбиение Ломуто:

1. Заведем два указателя  $l, r$ , изначально оба показывают на начало массива.
2. Пойдем слева направо,  $l$  – будет показывать границу, до которой все элементы меньше опорного.
3. Таким образом для разбиения хватит одного цикла.

#### Реализация 15.1: Разбиение Ломуто

```
int lomuto_partition(int* a, int l, int r) {
    int pivot = a[l + (r - 1) / 2];
    swap(&a[r], &a[l + (r - 1) / 2]);
    int i = l;
    for (int j = l; j <= r; ++j) {
        if (a[j] < pivot) {
            swap(&a[i++], &a[j]);
        }
    }
    swap(&a[i], &a[r]);
    return i;
}
```

Разбиение Хоара:

1. Заведем два указателя  $l, r$ , левый начинает с начала, правый с конца.
2. Устремим их на встречу друг другу.
3.  $r$  пропускает все элементы, которые  $\geq$  pivot,  $l$  – все, которые меньше pivot. Когда оба находят элементы, стоящие не так, меняем местами  $a_l$  и  $a_r$ .
4. Когда  $l, r$  встретятся – мы получим необходимое разбиение.

#### Реализация 15.2: Разбиение Хоара

```
int hoar_partition(int* a, int l, int r) {
    int piv_idx = l + (r - 1) / 2;
    int pivot = a[piv_idx];
    int i = l;
    int j = r;
    while (i <= j) {
        while (a[i] < pivot) { i++; }
        while (a[j] > pivot) { j--; }
        if (i >= j) {
            return j;
        }
        swap(&a[i++], &a[j--]);
    }
}
```

```

    }
    return j;
}

```

**Хоар vs Ломуто:**

На практике разбиение Хоара обычно работает заметно быстрее, чем разбиение Ломуто. Интуитивно это можно объяснить тем, что при разбиении Хоара сначала меняются местами как можно более удаленные друг от друга элементы, благодаря чему в массиве быстрее уменьшается число инверсий. На просторах интернета я нашел оценку числа обменов, которая для Хоара в 3 раза меньше чем для Ломуто.

**Толстое разбиение (задача флага Нидерландов):**

Поскольку числа обладают свойством трихотомии, решение задачи флага Нидерландов можно применить к разбиению элементов на три группы:  $<$  pivot,  $=$  pivot,  $>$  pivot.

1. Заведем два указателя  $l, mid, r$ .
2.  $l = 0, r = n - 1, mid = 0$
3. Будем поддерживать инвариант:  $\text{arr}[r \dots n - 1] > \text{pivot}$ ,  $\text{arr}[0 \dots l] < \text{pivot}$ ,  $\text{arr}[l \dots mid] == \text{pivot}$ .

**15.3 Оценка времени с случайным pivot (б/д)****Лемма 15.1:** Среднее время работы

При случайному выборе pivot:  $\mathbb{E}[X] = O(n \log n)$ .

## 16 Поиск порядковой статистики. Оценка времени с случайным pivot

### Определение 16.1: k-порядковая статистика

k-порядковая статистика — это k-ый по величине элемент.

#### Алгоритм поиска:

1. Выбрать опорный элемент.
2. Провести разбиение как в быстрой сортировке (любым методом, который нравится).
3. Искать ответ только с той стороны, где будет наша статистика.

### Лемма 16.1: Время работы поиска k-ой статистики

Алгоритм в среднем работает при выборе случайного pivot за  $O(n)$  (б/д).

### Реализация 16.1: Поиск k-той порядковой статистики

```

int find_kth(std::vector<int> vec, size_t k) {
    return find_kth(vec, 0, vec.size(), k);
}
int find_kth(std::vector<int>& vec, size_t left_index,
             size_t right_index, size_t k) {
    if (left_index + 1 == right_index) {
        return vec[left_index];
    }
    int pivot = vec[left_index + (right_index - left_index) / 2];
    size_t index = left_index;
    size_t jndex = right_index - 1;
    while (index < jndex) {
        while (index < jndex && vec[index] < pivot) {
            ++index;
        }
        while (jndex > index && vec[jndex] >= pivot) {
            --jndex;
        }
        if (index == jndex) {
            break;
        }
        std::swap(vec[index], vec[jndex]);
    }
    if (index < k) {
        return find_kth(vec, index, right_index, k);
    }
    return find_kth(vec, left_index, index + 1, k);
}

```

## 17 Медиана медиан. Время поиска медианы медиан. Работа алгоритмов быстрой сортировки и порядковой статистики с использованием медианы медиан

### 17.1 Медиана медиан как pivot. Время работы

Алгоритм (Блума-Флойда-Прата-Ривеста-Тарьяна):

1. Разобьем массив на пятерки элементов.
2. В каждой пятерке выберем медиану. Получили массив медиан.
3. Для массива медиан ищем медиану (с помощью алгоритма поиска k-порядковой статистики), и используем ее как опорный элемент.

Обратите внимание, что в алгоритме используется взаимная рекурсия — поиск медианы в массиве медиан, тоже будет использовать медиану медиан.

#### Лемма 17.1: Гарантия разбиения

Медиана медиан гарантированно делит массив в соотношении не хуже чем 3 : 7.

**Доказательство:** Сначала определим нижнюю границу для количества элементов, превышающих по величине опорный элемент  $x$ . В общем случае как минимум половина медиан, найденных на втором шаге, больше или равны медианы медиан  $x$ . Таким образом, как минимум  $\frac{N}{10}$  групп содержат по 3 элемента, превышающих величину  $x$ , за исключением группы, в которой меньше 5 элементов и ещё одной группы, содержащей сам элемент  $x$ . Таким образом получаем, что количество элементов больших  $x$  не менее  $\frac{3n}{10}$ .

#### Лемма 17.2: Линейное время работы

Алгоритм нахождения k-й порядковой статистики с использованием медианы медиан работает за линейное время.

**Доказательство:** У нас есть три составляющих работы алгоритма на каждом шаге:

1. Время на разделение массива на пятерки и их сортировка:  $aN$
2. Время на поиск медианы медиан  $T(\frac{N}{5})$
3. Время на поиск k-й порядковой не превзойдет времени его поиска в большей доле, то есть  $T(\frac{7N}{10})$

Таким образом,  $T(N) \leq T(\frac{N}{5}) + T(\frac{7N}{10}) + aN$ .

Пусть  $T(N) \leq cN$  для некоторой  $c$  и для любого  $n$  до 140. Подставим это соотношение:

$$T(N) \leq T\left(\frac{N}{5}\right) + T\left(\frac{7N}{10}\right) + cN \leq \frac{cN}{5} + \frac{7 \cdot cN}{10} + aN = cN \cdot \frac{9}{10} + aN = cN + \left(-cN \cdot \frac{1}{10} + aN\right)$$

Тогда неравенство  $T(N) \leq cN$  верно, если взять  $c \geq 10a$ . Поскольку такое  $c$  действительно можно выбрать, медиана медиан работает за линейное время.

**Применение:** Если использовать медиану медиан в качестве опорного элемента в быстрой сортировке, время работы сортировки будет  $O(n \log N)$  в худшем случае.

#### Реализация 17.1: Поиск медианы за линию

```
int MedianOfMedians(std::vector<int> vec) {
    return MedianOfMedians(vec, vec.size() / 2);
}
int MedianOfMedians(std::vector<int>& vec, size_t k) {
    if (vec.size() <= 5) {
        std::sort(vec.begin(), vec.end());
        return vec[k];
    }
    vector<int> medians;
```

```
for (size_t index = 0; index < vec.size(); index += 5) {
    size_t last_index = std::min(vec.size(), index + 5);
    sort(vec.begin() + index, vec.begin() + last_index);
    medians.push_back(vec[(last_index + index) / 2]);
}
int median = MedianOfMedians(medians, medians.size() / 2);
vector<int> less_median, greater_median;
for (size_t index = 0; index < vec.size(); ++index) {
    if (vec[index] <= median) {
        less_median.push_back(vec[index]);
    } else {
        greater_median.push_back(vec[index]);
    }
}
if (less_median.size() < k) {
    return MedianOfMedians(greater_median, k - less_median.size());
}
return MedianOfMedians(less_median, k);
```

## 18 Сортировка подсчётом. Стабильный вариант. Алгоритм LSD

### 18.1 Сортировка подсчётом (Counting Sort):

Пусть есть массив положительных чисел, элементы которого ограничены неким числом  $K$ . Почему бы просто не сосчитать какое значение вошло в него сколько раз? Затем выписать элементы по возрастанию нужное число раз!

Подводным камнем такой сортировки является отсутствие стабильности, но отчаиваться рано, ведь можно сделать эту сортировку стабильной.

### 18.2 Стабильный вариант

Заведём массив, в который будем записывать отсортированный массив (изначально заполнен нулями). Теперь на массиве, в котором хранили количество элементов, построим префиксные суммы. Пройдёмся по изначальному массиву с конца в начало и будем ставить элемент на последнее свободное место, выделенное в итоговом массиве. Для лучшего понимания см. реализацию.

#### Реализация 18.1: Стабильная сортировка подсчётом

```
void StableCountintSort(std::vector<char>& vec) { // english language signs
    std::vector<int> count(26, 0);
    std::vector<char> answer(vec.size());
    for (auto &elem: vec) {
        ++count[elem - 'a'];
    }
    for (int index = 1; index < 26; ++index) {
        count[index] += count[index - 1];
    }
    for (int index = vec.size() - 1; index > -1; --index) {
        answer[-count[vec[index] - 'a']] = vec[index];
    }
    vec = answer;
}
```

### 18.3 LSD (Least Significant Digit Sort):

Поймем, что целое число это набор байт. Что будет, если сортировать от последнего разряда к первому? Тут важно заметить, что нам КРАЙНЕ важна стабильность сортировки — без нее перемешаются старые результаты для менее значащих разрядов.

Время сортировки составляет  $O(n + K)$ , где  $K$  — макс. значение цифры в основании системы счисления, по которой число сортируется. Потребляемая доп. память составляет  $O(n + K)$ , поскольку нужен доп массив для совершения перестановки, и для хранения счетчиков.

#### Реализация 18.2: LSD

```
void LSPSort(std::vector<int>& vec) {
    auto vec_copy = vec;
    int max_element = 0;
    for (size_t index = 0; index < vec.size(); ++index) {
        max_element = std::max(max_element, vec[index]);
    }
    int digit_number = 1;
    size_t max_length = to_string(max_element).size();
    for (size_t length = 0; length < max_length; ++length) {
        std::vector<int> count(10);
        for (size_t index = 0; index < vec.size(); ++index) {
            int digit = (vec[index] / digit_number) % 10;
            ++count[digit];
        }
        for (size_t index_count = 1; index_count < count.size();
             ++index_count) {
            count[index_count] += count[index_count - 1];
        }
        for (size_t index = count.size() - 1; index + 1 > 0; ++index) {
            int digit = (vec[index] / digit_number) % 10;
```

```
    vec_copy[count[digit] - 1] = vec[index];
    --count[digit];
}
vec = vec_copy;
digit_number *= 10;
}
```

## 19 Дополнительные знания, не требуемые для сдачи экзамена

### 19.1 Мастер-теорема о рекурсии

**Теорема 19.1:** Мастер-теорема о рекурсии

Имеется рекуррентное соотношение:

$$T(n) = a \cdot T\left(\frac{n}{b}\right) + n^c, \quad \text{где } a \geq 1, b > 1$$

Тогда:

$$T(n) = \begin{cases} \Theta(n^{\log_b a}), & \text{если } a > b^c \\ \Theta(n^c \log n), & \text{если } a = b^c \\ \Theta(n^c), & \text{если } a < b^c \end{cases}$$

**Доказательство (схема):** Раскроем рекурренту:

$$\begin{aligned} T(n) &= n^c + a \cdot T(n/b) \\ &= n^c + a \cdot (n/b)^c + a^2 \cdot (n/b^2)^c + \dots \\ &= n^c \left(1 + \frac{a}{b^c} + \left(\frac{a}{b^c}\right)^2 + \dots\right) \\ &= n^c(1 + q + q^2 + \dots), \quad \text{где } q = \frac{a}{b^c} \end{aligned}$$

Количество членов:  $k = \Theta(\log n)$ .

- Если  $q = 1$  (т.е.  $a = b^c$ ):  $S(q) = k + 1 = \Theta(\log n) \Rightarrow T(n) = \Theta(n^c \log n)$
- Если  $q < 1$  (т.е.  $a < b^c$ ): бесконечно убывающая геометрическая прогрессия,  $T(n) = \Theta(n^c)$
- Если  $q > 1$  (т.е.  $a > b^c$ ):  $S(q) = \Theta(q^k) = \Theta\left(\left(\frac{a}{b^c}\right)^{\log n}\right) = \Theta(n^{\log_b a})$

### 19.2 Доказательство основной теоремы алгоритма Евклида

**Доказательство:**

Пусть  $(a, b) = k$ , тогда и  $a$  и  $bq$  делятся на  $k$ , следовательно,  $r = a - bq$  тоже делится на  $k$ .

С другой стороны, пусть  $(b, r) = k_1$ , тогда  $a = bq + r$  делится на  $k_1$ .

Предположим, что  $k_1 > k$  (или  $k_1 < k$ ), но в силу того что  $k$  (и  $k_1$ ) — НОД, получим противоречие, тогда  $k = k_1$ .