05.02.26

ЗАД. ПРО majority element

ПУСТЬ ДЛИНА ЧЁТНА

MAJ. el. – $\geq \frac{n}{2}$ ВХОЖД.

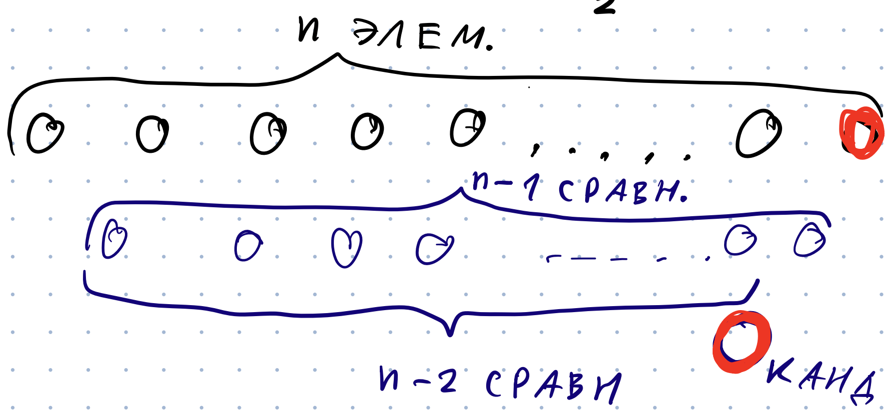
ПРЕДП. ЧТО maj. el. РОВНО $\frac{n}{2}$

$n-1$ СРАВН.

ПЕРЕД ПОСЛЕДН. СРАВН. СДЕЛАНО $n-2$ СРАВН.

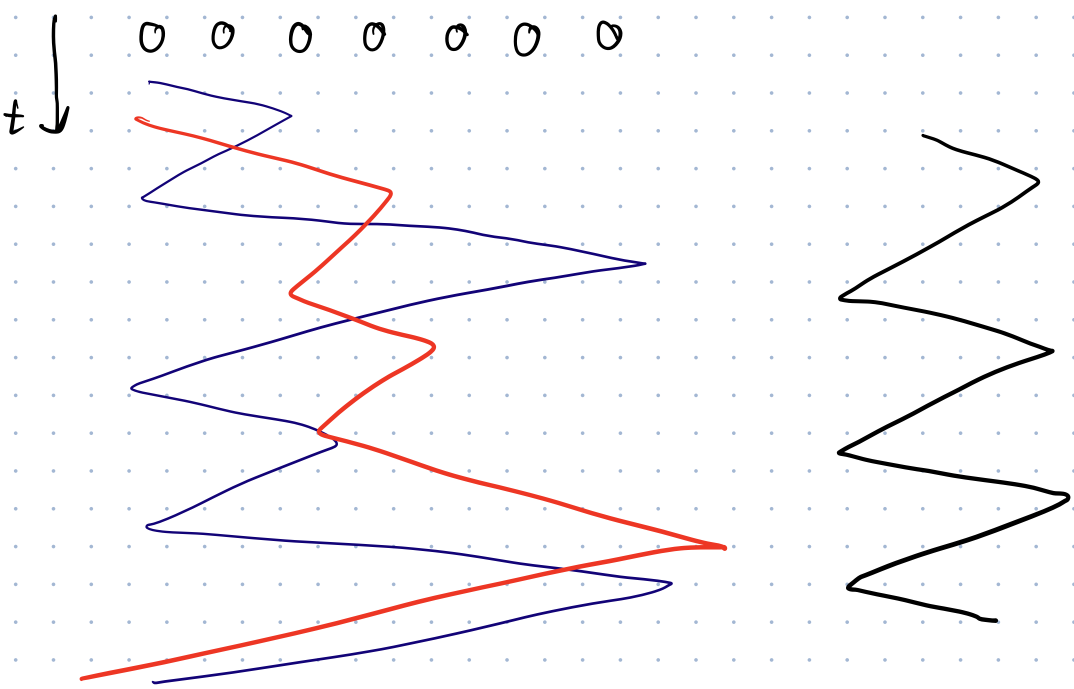
НА ЭТОТ МОМ. МОЖЕТ БЫТЬ ИСКЛЮЧ. max $\frac{n-2}{2}$ ЭКЗ. maj. el.

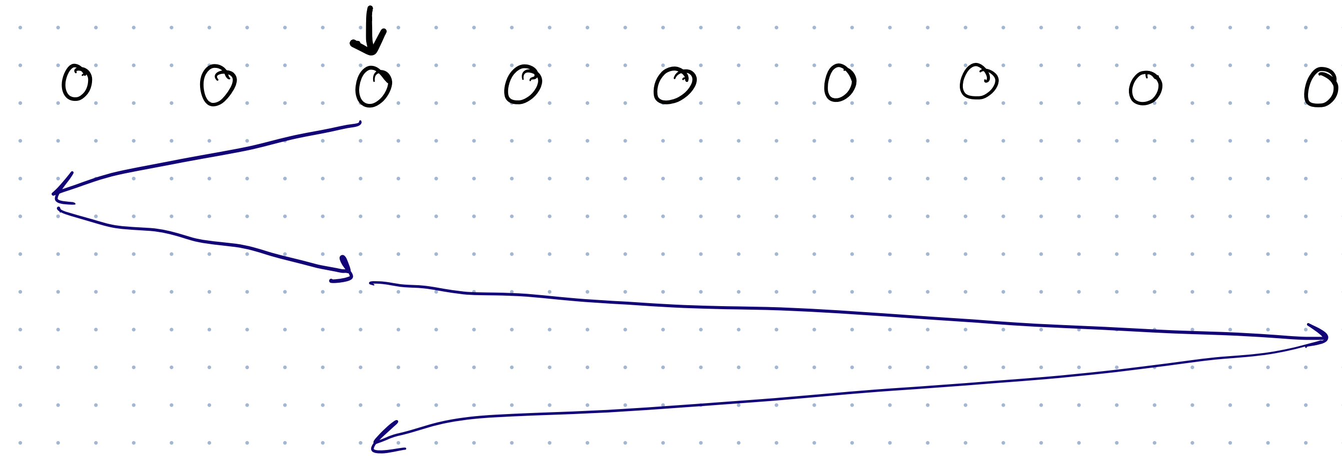
$$\frac{n-2}{2} = \frac{n}{2} - 1$$



	0	1	2	0
КАНД.	0	0	2	2
КОЛ.	1	0	1	0

ЗАДАЧА ПРО ЧАСЫ





ЗАД. ИЗ ДЗ 5

$a^b \mod c$

a, b, c – n-битовые числа

ЧТО МЫ УЖЕ МОЖЕМ:

1) x^y быстро — $O(\log_2 y)$ опер. умн., т.е. $O(n)$
2) $q \cdot p$ для n-бит. чисел — $O(n^{\log_2 3})$
3) $s \% t$ (на осн. divide) — $O(n^2)$

b в бит. виде => посл. оп. умнож.

после кажд. умн. приведение по мод

АЛГ.:

n ит.

1) очер. бит b => 1 или 2 оп. умн.
2) делаем умн. — $O(n^{\log_2 3})$
3) берём ост. — $O(n^2)$

$O(n^3)$

БЫСТРОЕ ПРИВЕДЕНИЕ ПО МОД., БЛИЗКОМУ К 2^k

$a \% 2^k - m$

предп., что $a > 2^k - m$

b – ОТВЕТ (ИЩЕМ ЕГО); $b < 2^k - m$

$$a = (2^k - m)\cdot p + b$$

$$b = a - 2^k p + m\cdot p \quad | \bmod 2^k$$

$$b \equiv a + m\cdot p$$

$\frac{a}{2^k}$ БЛИЗКО К p; $\quad p = \left\lfloor \frac{a}{2^k - m} \right\rfloor$; $\quad p = \frac{a-b}{2^k - m}$

⅃ $p' = \frac{a-b}{2^k}$

∃ exists

∀ all

⅃ let

$$p - p' = \frac{a-b}{2^k - m} - \frac{a-b}{2^k} = \underbrace{(a-b)}_{\text{ДЛИНА} \le 2k} \frac{\cancel{2^k - 2^k} + m}{2^k (2^k - m)}$$