

## Алгоритм Шорса

①

$$x_1 \rightarrow x_2 \rightarrow \dots x_\mu \rightarrow y_1 \rightarrow y_2 \rightarrow \dots y_\lambda \rightarrow x_n \rightarrow x_{n+1} \dots$$

То же биты в цикле повторяются одинаково распределены по модулю  $\lambda$ .

$$t = t + 1 \bmod \lambda$$

$$h = h + 2 \bmod \lambda$$

Тогда падающие биты будут:

$$\Delta = h - t \bmod \lambda$$

А теперь 1 шаг:

$$\Delta' = h + 2 - t - 1 = h - t + 1 = \Delta + 1 \bmod \lambda$$

||

Каждый из групп элементов  $\Rightarrow$  битов - 1 элемент

$$\Delta' = 0 \bmod \lambda$$

||

Они совпадают.

3)

Көмүлдүй бөлгөрүү:

Черепаха күрши -  $t$

Заяц -  $2t$

$m$  - заңынан жиынды.

$$2t = t \pmod{\lambda} \quad \begin{matrix} \text{желан} \\ \text{жакын} \end{matrix}$$

$$2t - t = 0 \pmod{\lambda}$$

$$t = 0 \pmod{\lambda}$$

$$\downarrow \\ t = \lambda \cdot k$$

Заданы черепаха преша тоғызы:

$$\lambda k - m \text{ шаралы}$$

Ал да жоғын бүткін на шарттарда  $\lambda k - m \pmod{\lambda}$

$$x = \lambda k - m \pmod{\lambda}$$

$$x = -m \pmod{\lambda}$$

$$x + m = 0 \pmod{\lambda}$$

Т.к. Себең үз тозын бөлгөрүү мүмкүн, со

ниңдең башка тоғызы.

$\Downarrow$

Егер менде көмүлдүй жерендей башка, то жиындан оны күрсөгөн м

шаралы. А жаңы күрсөгө мөн мүмкүн башка тоғызы башка тоғызы.

2)

1) Ор шаралы жо бөлгөрүү:

$m$  шаралы жерендей

$2m$  жаңы

$B$  шаралы:

не бөлгөрүү 1 шаралы

$$m + \lambda < n \Rightarrow O(n)$$

2) Топтук шаралы жиында:

$$\mu < n \Rightarrow O(n)$$

Умозда:

$$O(h) + O(n) = O(n)$$