Решето Эратосфена

1..n - проверить на простоту

```
is_prime = [True]*(n+1); is_prime[0] = is_prime[1] = False
for i = 2..n:
    if is_prime[i]:
        for (j = 2i; j ≤ n; j += i):
            is_prime[j] = false
```

0 1 2 3 4 5 6 7 8
F F T T F T F T F

1). $Time = O(n \log n)$

$Time \le \sum_{i=2}^{n} \frac{n}{i} = n\left(\frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots + \frac{1}{n}\right) = O(n \log n)$

2). $Time = O(n \log\log n)$

Rem. Э решето за $O(n)$.

Китайская теорема об остатках

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

$\forall i \neq j \quad \gcd(m_i, m_j) = 1$

$x = ?$

$M = m_1 \cdot m_2 \cdot \dots \cdot m_n$

Th. (КТО) $\exists!\ a \in [0, M)$:

$\forall i \quad a \equiv a_i \pmod{m_i}$.

Все решения: $\{a + kM \mid k \in \mathbb{Z}\}$

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \end{cases} \iff x \equiv 5 \pmod 6$$

$$\begin{cases} x \equiv 1 \pmod{m_1} \\ x \equiv 0 \pmod{m_2} \\ \vdots \\ x \equiv 0 \pmod{m_n} \end{cases} \longrightarrow e_1$$

$a_i := \sum_{i=1}^{n} a_i \cdot e_i \bmod M$

$a \bmod m_j$: $\sum_{i=1}^{n} a_i e_i \bmod m_j$

$i = j \quad a_j e_j \bmod m_j = a_j \cdot 1 = a_j$

$i \neq j \quad a_i \underbrace{e_i}_{\bmod m_j = 0} \bmod m_j = 0$

$\sum_{i=1}^{n} a_i e_i \equiv_{m_j} 0 + 0 + \dots + 0 + a_j + 0 + \dots + 0 = a_j$

$e_i = \left(M_i \cdot inv(M_i, m_i)\right) \bmod M$

$M_i := m_1 \cdot m_2 \cdot \dots \cdot m_{i-1} \cdot m_{i+1} \cdot \dots \cdot m_n = \frac{M}{m_i}$

$M_i \cdot \underbrace{inv(M_i, m_i)}_{\equiv_{m_i} 1}$

$\gcd(M_i, m_i) = 1$

$Time = O(n(n + \log m)) = O(n^2)$

$Time = O(n)$

- Использование КТО для длинной арифметики

  \+ * промежуточ. вычисл. – очень большие

  ответ $< L$

$p_1, p_2, \dots, p_k \in \mathbb{P} \quad \prod p_i \ge L$

$p_i \sim 10^9 \qquad k = O(\log L)$

Проведем все вычисления

по модулю $p_1 \to a_1$

по модулю $p_2 \to a_2$

$\vdots$

— " — $p_k \to a_k$

Правильный ответ $\equiv a_1 \pmod{p_1}$, $\equiv a_2 \pmod{p_2}$, $\vdots$ $\Rightarrow a \bmod p_1 \cdots p_k$

это и есть правильный ответ!