Теория чисел

29 ноября 2021 г. 14:48

① Проверка на простоту $O(\sqrt{n})$

```
for (int i=2; i*i<=n; ++i)
    if (n%i==0)
        return false;
return true;
```

```
i=2
while i*i<=n:
    if ---
      - -
    i+=1
```

$\sim O(k \log^3 n)$ с вер. ошибки $\le \frac{1}{4^k}$
(Алгоритм Миллера-Рабина)

② Разложение на пп-ли $12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3^1$ $O(\sqrt{n})$

$O(\sqrt[4]{n})$ и немного быстрее (вероятн.)

```
for (int i=2; i*i<=n; ++i)
    while (n%i==0)
        n/=i, ans.push_back(i)
if(n>1)
    ans.push_back(n);
```

③ Проверка на простоту чисел $1..n$.
Решето Эратосфена

```
is_prime = [True]*n      # 0,1 - ?
for i in range(n):
    if is_prime[i]:
        for j in range(2*i, n, i):
            is_prime[j] = False
```

2	3	4	5	6	7	8	9	10	..	12
П	П	С		С		С	С	С		
				С		С				С

for (int j=2*i; j<n; j+=i)

$$Time = O\left(n + \sum_{\substack{i \in P \\ i \le n}} \frac{n-i}{i}\right) = O(n \log n)$$

$$\le n \cdot \sum_{i=1}^{n} \frac{1}{i} = O(n \log n)$$

Можно доказать, что Time $= O(n \log \log n)$
∃ решето Эратосф., кот. Time $= O(n)$

Простых чисел $1..n \sim \frac{n}{\ln n}$

④ Наибольший общий делитель НОД (greatest common divisor GCD)

$\gcd(a,b) = \max d : \begin{cases} a \vdots d \\ b \vdots d \end{cases}$

$\gcd(12,8) = 4$
$\gcd(12,9) = 3$

Алгоритм Евклида
$\gcd(a,b) \overset{?}{=} \gcd(b, a \bmod b)$

$a = bk + r \quad 0 \le r < b$
$r = a \bmod b$

1). $\begin{matrix} a \vdots d \\ b \vdots d \end{matrix} \Rightarrow \begin{matrix} b \vdots d \\ r = \underbrace{a - bk}_{\vdots d} \vdots d \end{matrix}$

2). $\begin{matrix} b \vdots d \\ r \vdots d \end{matrix} \Rightarrow \begin{matrix} a = \underbrace{bk + r}_{\vdots d} \vdots d \\ b \vdots d \end{matrix}$

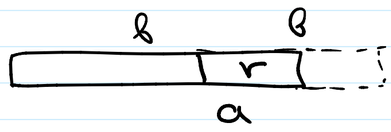
Мн-во общих делителей a и b совп. с мн-вом общих делителей b и $a \bmod b$.
$\Rightarrow$ и наибольший общ. дел. совпадает.

```
def gcd(a,b):
    if b==0:
        return a
    return gcd(b, a%b)
```

($a \bmod b < b$)

Время работы:
1). $a < b \Rightarrow \gcd(b,a)$, $b > a$ и во всех след. вызовах первый арг. > второй

2). $a > b$
- $a \ge 2b$
  $(a,b) \to (b,r) \quad r < b \le \frac{a}{2}$
- $2b > a > b$
  $(a,b) \to (b,r) \quad r = a - b \overset{?}{<} \frac{a}{2}$
  $b \overset{?}{>} a/2$
  $2b \overset{?}{>} a$



На каждом шаге большее число уменьшается хотя бы в 2 раза.
$Time = O(\log a + \log b) = O(\log(ab))$