Теория чисел

Решето Эратосфена

$n \rightarrow$ найти все простые числа $\le n$

`vector<bool> p(n+1, 1);` | $\frac{n}{8}$ байт

```
p[0] = p[1] = 0
for i = 2 .. √n
    if p[i] == 1:
        for j = 2i .. n step = i
            p[j] = 0
```

$\forall n \in \mathbb{P}\ \exists p \in \mathbb{P} : p^2 \le n$

$2i$, $i+2$

$2^{\frac{1}{k}\ln k} \le p_k \le 2k\ln k$

$$T = \Theta(n) + \sum_{k=1}^{n/\ln n} \frac{n}{p_k} = \Theta(n) +$$

$$+ \Theta\left(\sum_{k=\Theta(1)}^{n/\ln n} \frac{n}{k\ln k}\right) = \Theta(n) + \Theta\left(n \int_{\Theta(1)}^{n/\ln n} \frac{dx}{x\ln x}\right) =$$

$M \approx n/\ln n$

$\pi(n)$ = # простых от 1 до n

$$\pi(n) \sim \frac{n}{\ln n} \quad n \to \infty$$

$$\rightarrow \boxed{p_k \sim k \ln k} \quad k \to \infty$$

$$= \Theta(n) + \Theta\left(n \left(\log\log x\right)^{\left\lceil \frac{n/\ln n}{O(1)} \right\rceil}\right) =$$

$$= \Theta(n) + \underline{\Theta(n \log\log n)}$$

$d[x]$ = номер минимального простого, на кот. делится x

$\forall x = 1 \ldots n$

	1	2	3	4
p:	2,	3,	5,	7

	1	2	3	4	5	6	7	8	9
d	-	1	2	1	3	1	4	1	2

$$x = p_i \cdot y \qquad p_i \in P - \min$$

$$\sum_{y=2}^{\lfloor n/p_i \rfloor} [d[y] \geq i]$$

(d[y])=

vector<int> primes, d(n+1, -1);

for (y=2; y<=n; ++y)

if d[y] == -1:

d[y]=primes.size()

primes.push(y)

for (i=0; i<primes.size() &&

i<=d[y] &&

primes[i]*y<=n ; ++i)

x=primes[i]*y;

d[x]=i

∀ x будет быть ≤ одно.

d[x]=i

---

p ∈ ℙ m ∈ ℤ

$\mathbb{Z}_p = \{0, 1, \dots, p-1\}$ $\quad$ $\mathbb{Z}_m = \{0, \dots, m-1\}$

$\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$ $\quad$ $\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m : (a, m) = 1\}$

$|\mathbb{Z}_p^*| = p-1$ $\quad$ $|\mathbb{Z}_m^*| = \varphi(m)$

"

$m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

$\varphi(m) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdots p_k^{\alpha_k - 1} \cdot (p_1 - 1) \cdots (p_k - 1)$

$a \cdot x \equiv 1 \pmod{m}$ $\quad$ $x =: a^{-1}$

$\frac{b}{a}$ $\quad$ $\exists ! c : c \cdot a = b$

$c = b \cdot a^{-1}$

① $m = p \in \mathbb{P}$

$\forall g : (g, p) = 1$

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

$a \cdot a^{p-2} \equiv 1 \pmod{p}$

$a^{-1} = a^{p-2}$ $\quad$ $a \nmid p$

```
pow(x, n, m):
    if n == 0
        return 1 % m
    else{ y = pow(x, n/2, m)
        if n % 2 == 0
            return (y*y) % m
        else
            return (y*y) % m * x
                % m
```

p - модуль → обращаем за O(log p)

---

m - модуль

$a^{-1} = y^{\varphi(m)-1}$

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

$(y, m) = 1$

$O(FACTOR(m) + \log(m))$

Расшир. алгоритм Евклида

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

$\exists\, x, y \in \mathbb{Z}: \quad a \cdot x + b \cdot y = \gcd(a,b)$

```
ext_gcd(a,b): // (x,y)
    if b==0:
        return (1,0);
    else
        (x,y) = ext_gcd(b, a%b)
        return
        (y, x - y*(a/b))
```

$x \cdot b + y \cdot (a \% b) = g$

$a = b \cdot k + r$

$x \cdot b + y \cdot r = g$

$x \cdot b + y(a - bk) = g$

$y \cdot a + (x - yk) \cdot b = g$

$ax \equiv b$

m

$a \cdot x + m \cdot k = 1$

$(a, m) = 1$

$a^{-1} = (ext\_gcd(a, m)).x$

$ax + by = c$ $\quad a, x, b, y, c \in \mathbb{Z}$

$x, y - ?$

$ax \equiv c \pmod{8}$

$2 \cdot x \equiv 4 \pmod{8}$ $\quad x = 2$

+ Обращение по модулю
. Первообразный корень

$\mathbb{Z}_m^* = \{g^0, g^1, g^2, g^3, \ldots, g^{\varphi(m)-1}\}$

5: 2^0 2^1 2^2 2^3 2^4 $\quad ord(2) = 4$

1 2 4 3 1

$4^0 = 1 \quad 4^1 = 4 \quad 4^2 = 1 \quad \mathrm{ord}(4) = 2$

П/о корень $\exists$ по след. модулям:

$$\boxed{2, 4, p^\alpha, 2p^\alpha}$$

$\forall p \in \mathbb{P}$, $p \neq 2$, $\alpha \in \mathbb{N}$

— $g \to$ п/о корень или нет?

$g^x \underset{p}{\equiv} 1 \quad x\text{-min}$ — порядок g

$\mathrm{ord}\, g$

$$\boxed{g - \text{п/о} \iff \mathrm{ord}(g) = p - 1}$$

$\forall x \not\vdots p \quad x^{p-1} \underset{p}{\equiv} 1$

$$\boxed{x^t \underset{p}{\equiv} 1 \Rightarrow t : \mathrm{ord}_p(x)}$$

$p - 1 : \mathrm{ord}(x)$

$$\begin{cases} \mathrm{ord} = p - 1 \\ \mathrm{ord} < p - 1 \end{cases} \quad \underline{p - 1 : \mathrm{ord}}$$

$p - 1$

$$g^{\frac{p-1}{q}} \equiv_p 1 \qquad q \in P$$

$p-1 \,\vdots\, q$

$$\text{ord} = \frac{p-1}{q_1 q_2 q_3 \ldots q_t}$$

$\log p$ — различных простых в $p-1$

$\log p$ — возв. в степень $\frac{p-1}{q}$

$\text{FACTOR}(p-1) + \log^2 p$ — проверили, явл. g п/о корнем

$\sqrt[4]{p-1}$

p не помещ. в маш. слово

$\Rightarrow \log p \log\log p$

$\log^3 p$ — пров., явл. g п/о для длин. чисел

поиск п/о

— детерм: $1 .. p$

проверяем п/о на

([illegible])

(= log p при оо. (на-Рим)

— вероятн.

g – случ. → проверяем

Pr успеха $= \Omega\left(\frac{1}{\log\log p}\right)$

$\log\log p$ шагов

$\{g^0, g^1, \ldots g^{p-2}\} = \mathbb{Z}_p^{\times}$

g^i – п/о корнем ?

$g^i \cdot g^j = g^{i+j} \equiv_p g^{(i+j) \bmod p-1}$

$(i, p-1) = 1$

п/о корней $= \varphi(p-1)$

Pr успеха $= \frac{\varphi(p-1)}{p-1} =$

$p-1 = q_1^{\alpha_1} \cdots q_k^{\alpha_k}$ $\quad k \le \ln(p-1)$

$$= \frac{q_1^{\alpha_1+1} \cdot \ldots \cdot q_k^{\alpha_k+1}}{q_1 \cdot \ldots \cdot q_k} \cdot \frac{(q_1-1)\cdot\ldots\cdot(q_k-1)}{q_1 \cdot \ldots \cdot q_k} =$$

$$= \prod_{q_i \mid p-1} \frac{q_i - 1}{q_i} = \prod \left(1 - \frac{1}{q_i}\right) \geq \ldots$$

$$\ln(P_t) = \sum \ln\left(1 - \frac{1}{q_i}\right) \geq$$

$$\geq \sum \left(-\frac{1}{q_i}\right) =$$

$$= \Omega\left(-\sum_{i=1}^{k} \frac{1}{i \ln i}\right) =$$

$$= \Omega(-\log\log k)$$

$$\ln(1-x) \geq -2x$$

$$0 \leq x \leq \frac{1}{2}$$

$$P_t \sim i \ln i$$

$$q_i \geq p_i$$

$$P_r \geq \sum \left(\frac{1}{\log k}\right) \geq \sum \left(\frac{1}{\log\log p}\right)$$

Дискретное логарифмирование

$$a^x = b \qquad x = \log_a b$$

$$a^x \equiv_m b \qquad x = ?$$

$$x = y \cdot \sqrt{m} + z \qquad z < \sqrt{m}$$

$$a^0,\ a^{\sqrt{m}},\ a^{2\sqrt{m}},\ \ldots,\ a^{m-\sqrt{m}}$$

$$a^x = b \qquad b,\ b \cdot a^{-1},\ b \cdot a^{-2},\ \ldots$$

$$a^{y \cdot \sqrt{m}}$$

```
for i=0..√m
    HT[a^(i√m)] = i
for j=0..√m
    if HT[b] ≠ None:
        return HT[b]*√m + j
b* = a^-1
```

$\sqrt{m}$

Корень k степени по модулю

$$x^k \underset{p}{\equiv} a$$

1). Найдем п/о корень g

2). $g^z \underset{p}{\equiv} a$ – дискр. лог.

$a = g^z$

$(x) := g^{(t)}$ — ищем

$(g^t)^k \underset{p}{\equiv} a \equiv g^z$

$t \cdot k \underset{p-1}{\equiv} z$

ищем — дано

Китайская теорема об остатках

К.Т.О.

$$\begin{cases} x \underset{m_1}{\equiv} a_1 \\ \vdots \\ x \equiv a_k \end{cases} \qquad \forall (m_i, m_j) = 1 \quad i \neq j$$

m_k

$\exists!\ x \in [0, M = m_1 \dots m_k)$

$x \equiv a_i \pmod{m_i} \quad \forall m_i$

$$x = \sum_{i=1}^{k} a_i \cdot R_i$$

$x \equiv 1 \pmod{m_1}$

$x \equiv 0 \pmod{m_i}$

$R_1 \equiv 1 \pmod{m_1}$

$\left(m_2 \cdot m_3 \cdot \dots \cdot m_k\right) \left(m_2 \dots m_k\right)^{-1} \pmod{m_1}$

$\pmod{m_1 \dots m_k}$

M

---

m_i — разложим на простые

$p_i^{\alpha_1} \dots p_k^{\alpha_k}$

1).

$x \equiv a_i \pmod{m_i}$

$x \equiv a_i \pmod{p_i^{\alpha_1}}$

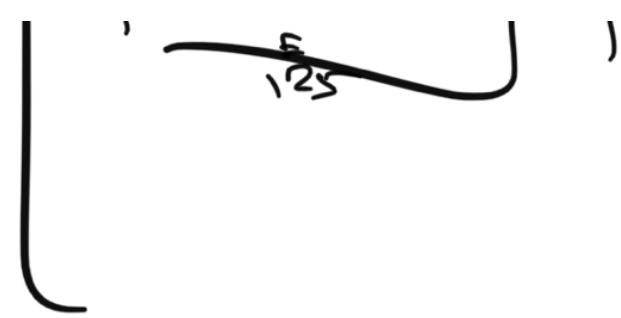
$x \equiv a_i \pmod{p_2^{\alpha_2}}$

$x \equiv a_i \pmod{p_k^{\alpha_k}}$

2).

$p = 2$

$p = 5$



Арифм. выражение
длинные числа

Задача В конце ответ $0 \leq X \leq$ [illegible]

Арифм. выражение
длинные числа

Задача В конце ответ $0 \leq X \leq$ [illegible]