Теория чисел I

Разбор I.

1 3 2 5 , k = 4
↓
3 2 5

a_i - массив из n чисел, k - число

$k = 7 \Rightarrow \begin{cases} 1+6 \\ 2+5 \\ 3+4 \end{cases}$ — выключаем тех кого меньше

$K = 6 \Rightarrow \begin{cases} 1+5 \\ 2+4 \\ 3+3 \end{cases}$ — можем позволить оставить одного.

Теория чисел.

% - Операция в c++ $10 \% 3 = 1$ | $-10 \% 3 = -1$

$10 = \underset{10/3}{3} \cdot 3 + 1$

Кольцо Вычетов.

mod = 10

1 mod 10 = 1 , 2 mod 10 = 2 . . . . . 10 mod 10 = 0

$(11 + 32) \bmod 10 = (1+2) \bmod 10 = 3 \bmod 10$

$(9 + 4) \bmod 10 = 3 \bmod 10.$

$32 \equiv 2 \pmod{10}$, $x \cdot y \bmod 10 = ((x \bmod 10)(y \bmod 10)) \bmod 10$

Деление по простому модулю

(1e9+7, 13, 41, ...)

a - число, p - модуль.простой. Хотим найти $\frac{1}{a} = ?$

Хотим найти b, такое что $ab \equiv 1 \pmod p$

Пример.

$p = 7, a = 3 \Rightarrow b = 5$ $3 \cdot 5 = 15 \equiv 1 \pmod 7$

Малая теорема Ферма.

$a^{p-1} \equiv 1 \pmod p$ или же

$a^p \equiv a \pmod p$ $(2^3 = 8 \equiv 2 \pmod 3)$

n, 2n, 3n, ... (p-1)n — разные остатки

$a^{p-1} \equiv 1 \pmod p \Rightarrow \underset{a}{\overset{}{a}} \cdot \underset{b}{a^{p-2}} \equiv 1 \pmod p \Rightarrow \boxed{a^{-1} = a^{p-2}}$

Док-во:

Бинарное возведение в степень

a^n считаем $a^{n/2}$ и возводим в квадрат

a^{10} — считаем a^5 — считаем a^2

$a^{10} = ((a^2)^2 \cdot a)^2$

Диофантово уравнение.

НОД двух чисел (НОД(30, 12) = 6

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

    else:
        return gcd(b, a%b)
```

30 12
12 6
6 0
⇓
НОД 6

$ax + by = c$, a, b, c – числа Нужно найти x и y

Всё целое

Пусть $g = НОД(a,b)$ $a = k_1 \cdot g$ $b = k_2 \cdot g$

$k_1 \cdot g \cdot x + k_2 \cdot g \cdot y = c$

$g(k_1 x + k_2 y) = c$ ⇒ С должен делится на g иначе нет решений.

$\boxed{ax + by = g}$ $(ax + by = c = g \cdot k)$ $(k = \frac{c}{g})$

```
int gcd(int a, int b, int& x, int& y)
    if a == 0:
        x=0; y=1
        return b;

    int x1,y1;
    int d = gcd(b%a, a, x1, y1)
    x = y1 - (b/a) x1
    y = x1
    return d;
```

← $0 \cdot x + b \cdot y = b$

$x_1 \cdot (b \% a) + y_1 \cdot a = d$

$x_1 \cdot (b - \lfloor \frac{b}{a} \rfloor \cdot a) + y_1 \cdot a = d$

$a \underbrace{(y_1 - \lfloor \frac{b}{a} \rfloor x_1)} + \underbrace{x_1} \cdot b = d$

Работает при неотриц. a и b

$ax' + by' = g \Rightarrow ax + by = c$

где $x = x' \cdot \frac{c}{g}$, $y = x' \cdot \frac{c}{g}$

и учесть знаки a и b.

x и y решения $ax + by = c$ ...целое

$a(x + \frac{b}{g}) + b(y - \frac{a}{g}) = c$

$ax + \frac{ab}{g} + by - \frac{ab}{g} = c$

Все решения выглядят кок:

$(x + \frac{k \cdot b}{g}, y - \frac{k \cdot a}{g})$ k - любое целое

$a = 30$, $b = -12$ $c = 12$, $g = 6$

$x = 2, y = 4$

$x + \frac{b}{g} = 2 + \frac{-12}{6} = 0$

$y - \frac{a}{g} = 4 - \frac{30}{6} = -1$

$0 \cdot 30 + (-1) \cdot (-12) = 12$

$(5 - 17) \bmod 10 = -12 \bmod 10$
$= -2 \bmod 10 = 8 \bmod 10$

$(5 - 7) \bmod 10 \equiv -2 \equiv 8 \pmod{}$

C++ остаток < 0.

$(\underset{n}{a \%} - \underset{n}{b \%} + n) \% n$

Китайская теорема об остатках

$\begin{cases} x \equiv a \pmod n \\ x \equiv b \pmod m \end{cases}$

n и m взаимнопросты
НОД равен 1

Пример $\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \end{cases}$

x = 5 ↗

x ≡ . . . . . . (mod 6)

$x \equiv b_1 \cdot m + b_2 \cdot n \pmod{n \cdot m}$

b_1 – такое число что $b_1 \cdot m \equiv a \pmod n$ – $\overset{=1}{b_1} \cdot 3 \equiv 1 \pmod 2$

b_2 . . . . $b_2 \cdot n \equiv b \pmod m$ – $\underset{1}{b_2} \cdot 2 \equiv 2 \pmod 3$

$107 \equiv 7 \pmod{10}$

$107 - 10 \cdot 10 = 7$

$x = 1 \cdot m + 1 \cdot n = 2 + 3 = 5$

Как искать?

известно, ищем

$b_1 \cdot m + k n = a$

↗ Это диофантово уравнение, т.к. m и n взаимнопросты – решение всегда есть

Обобщение

$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$ m_i – взаимно просты

$x \equiv b_1 \cdot M_1 + \ldots + b_n \cdot M_n \pmod{m_1 \cdot \ldots \cdot m_n}$

где $M_i = \frac{m_1 \cdot \ldots \cdot m_n}{m_i}$ и найти b_i с помощью диофо.

$b_i \cdot M_i \equiv a_i \pmod{m_i}$

Разложение на простые.

Дано n, разложить на произв. простых.

$42 = 7 \cdot 2 \cdot 3$

Как поиск делителей, только в процессе уменьшаем число.

```
i = 2
    while i^2 <= n :
        while n%i == 0:
            ans.add(i)
            n /= i

        i += 1

ans.add(n)
```

n = 14

ans = {2} , n = 7

ans.add(n) ⇒ ans = {2, 7}