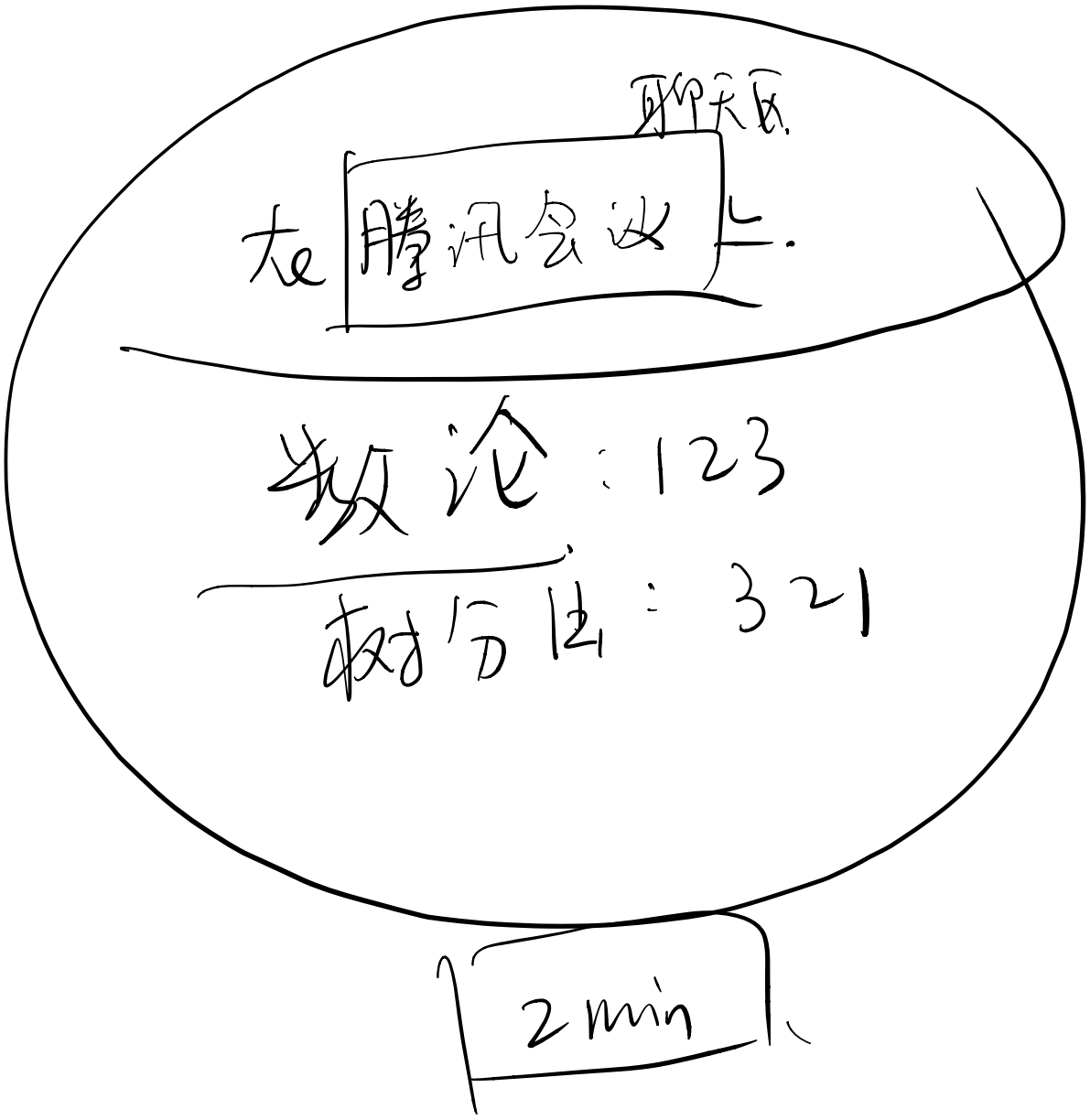


非负数. $gcd(a,b)=(a,b)$

① $a|b$ $(b\neq 0)\Rightarrow a\leq b$.

$d=(a,b)$ $=$ $d'=(a,a+b)$

$\Rightarrow d|a,\ d|b$

$\Rightarrow d|a,\ d|(a+b)$

$\Rightarrow d|(a,a+b)\Rightarrow d|d'\Rightarrow d\leq d'$

$d' = (a, a+b)$

$\Rightarrow d' \mid a, \; d' \mid (a+b)$

$\Rightarrow d' \mid a, \; d' \mid b$

$\Rightarrow d' \mid (a,b) = d \qquad d' \le d \qquad \therefore d' = d$

$(a,b) = (a, a \pm b) \qquad a = kb + r, \; 0 \le r < b$

$(a,b) = (b, a-b) = (b, a-2b) = \cdots$

$= (b, a-kb) = (b, r)$

$= (b, a \% b)$

$(a,b) = (b,a) \qquad b > (a \% b)$

不妨设 $a \ge b$

$\gcd(a,b) = \gcd(a \% b, b) = \gcd(b, a \% b)$

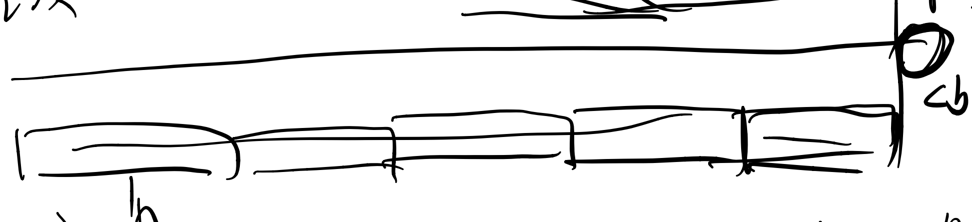
$< b$

$a \ge b. \qquad a \% b \le \lfloor \frac{a}{2} \rfloor = \gcd(a \% b, b \% (a \% b))$

$< \frac{a}{2} \qquad < \frac{b}{2}$

每轮2次

$r = a \% b$



$\frac{a, b}{2}$

$O(\log a + \log b)$

$a = kb + r \quad k \ge 1$

$2r < r + b \quad a \ge b$

$\gcd(a, 0) = a \qquad r < \frac{b+r}{2} \le \frac{kb+r}{2} = \frac{a}{2}$

exgcd

$a = kb + r$ $k \geq 1$ $0 \leq r < b$

$ax +$

$a \equiv b \pmod m$

↳ $a - b = km$.

① $(a, b, m) \equiv ((a,b), m)$

$a = a'd$. $b = b'd$, $m = m'd$

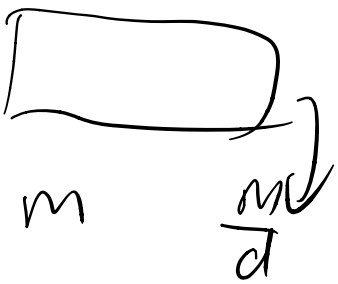
$a' - b' = km'$

$d \mid m$

$a' \equiv b' \pmod{m'}$

$\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$

$d \mid (a, b, m)$



mod 2

1 3

同余方程 $m \neq 0$.

$$ax \equiv b \pmod m$$

$a \neq b$ ✓

$$ax - b = -ym$$

$$ax + my = b$$

$d = (a, m)$

$d \mid a \rightarrow d \mid ax \rightarrow d \mid (ax + my) \Rightarrow d \mid b$

$d \mid my$

① $d \mid b$

$\frac{a}{d} = a'$. $\frac{m}{d} = m'$. $\frac{b}{d} = b'$

② $a'x + m'y = b'$ $(a', m') = 1 \Leftrightarrow a' \perp m'$

证.

③. $ax+by=1$ $\quad (a,b)=1$

exgcd: $a \geq b$

$ax+by=1$

$\Downarrow$ $-bx$ $+bx$

$(a-b)x+b(x+y)=1$

$\Downarrow$ $-bx$ $+bx$

$(a-2b)x+b(2x+y)=1$

$\Downarrow$

$\vdots$

$\Downarrow \forall k \geq 0$ $\quad k=t$

$(a-kb)x+b(kx+y)=1$ $\quad ax+by=1$

$a=tb+r,\ a \leq r < b$ $\quad r < \frac{a}{2} \Rightarrow a \geq b$ $\quad t=\left[\frac{a}{b}\right]$

$(a-tb)x+b(tx+y)=1$

$\Downarrow$

$rx+b\left(\left[\frac{a}{b}\right]x+y\right)=1$

$bx'+ry'=1$

$\Downarrow$

$r=a\%b$

$x'=\left[\frac{a}{b}\right]x+y$

$y'=x$

求这组整数解 (x', y')

$x = y' \quad y = x' - \lfloor \frac{a}{b} \rfloor x$

$10x + 3y = 1 \rightarrow (1, -3)$

$1x + 3(3x + y) = 1$

$x' = 3x + y$

$y' = x$

$3x' + y' = 1$

$x' = 0 \quad y' = 1$

$x = 1 \quad y = x' - 3x = -3.$

$ax + by = 0$

$\Downarrow$

$bx' + (a \% b) y' = 0$

$\Downarrow$

$(a \% b) x'' + (b \% (a \% b)) y'' = 0$

$b = 0$

$x = 1$

$x = 1, \ y = 0.$

$gcd(a, b) \rightarrow^{gcd} (a \% b, b)$

gcd

$\rightarrow \cdots \rightarrow gcd(1, 0)$

$3x' + 1y' = 1$

$2x' + x' + y'$

$x' + 2x' + y'$

$0x' + 1(3x' + y') = 1$

$x'' = 3x' + y'$

$y'' = x'$

$1x'' + 0y'' = 1$

$x'' = 1 \quad y'' = 0$

$x' = 0 \quad y' = x'' - 3x' = 1$

$(0,1)$

(特解) $x = 1$ ✗

结论：$ax + by = c$ 充要条件 (有解)

$\Leftrightarrow (a,b) \mid c$

$\Rightarrow$

$\Leftarrow$: $a'x + b'y = c'$

$a' = \frac{a}{(a,b)}$, $(a',b') = 1$

$x = c'x_0 \cdot y = c'y_0$

$a'x + b'y = 1$

$a'(c'x_0) + b'(c'y_0) = c'$

$a'x_0 + b'y_0 = 1$

① $ax+by=c$. 求解

⇓

② $ax+by=c$, $(a,b)=1$

⇓

③ $ax+by=1$. $(a,b)=1$

以下有解

⇓

④ $ax+by=c$ 有解 $\Leftrightarrow (a,b)\mid c$

⑤: 求 $ax+by=(a,b)$ 的一个特解

求解：

一个特解 $(a,b)=1$ (x_0,y_0) 特解

$$\boxed{ax_0+by_0=1}$$

$$a(x_0+kb)+b(y_0+ka)=1$$

$$\begin{cases} x=x_0-kb \\ y=y_0+ka \end{cases} \quad k\in\mathbb{Z}.$$

是解（全体）

为何是全体解？ (x_1,y_1)

$$ax_0+by_0=1$$

$$ax_1+by_1=1$$

$$a(x_0-x_1)=b(y_1-y_0)$$

$a \mid a(x_0 - x_1) \mid b(y_1 - y_0)$

$a \mid b(y_1 - y_0)$

$(a,b) = 1$

$a \mid (y_1 - y_0)$

$y_0 = 2^2 \times 3 \times 5$

$6 \mid x \times 18$

$n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$

$p_1 \sim p_k$ 质数. $a_i > 0$

$a = p_1^{a_1} \cdots p_k^{a_k}$

$b = p_1^{b} \cdots p_k^{b_k}$, $a_i, b_i \geq 0$

$(a,b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_k^{\min(a_k, b_k)}$

$y_1 \equiv y_0 \pmod a$

$y_1 = ka + y_0$

$ax+by=(a,b)$ 的一解 (x_0, y_0)

$ax_0+by_0=(a,b)$

$a(x_0-?_0)+b(y_0+?_1)=(a,b)$

$\frac{a,b}{(a,b)}$ $=a?_0=b?_1$

$\min ?_0=$

$a?_0$ 是 b 的倍数

$b \mid a?_0$

$?_1=\frac{a?_0}{b}$

$d=(a,b)$ $(a',b')=1$

$b' \mid ?_0$

$b' \mid ?_0$.

$?_0$ 是 $\frac{b}{(a,b)}$

$$a\left(x_0-\frac{kb}{(a,b)}\right)+b\left(y_0+\frac{ka}{(a,b)}\right)=(a,b)$$

$$\begin{cases} x=x_0-k\frac{b}{(a,b)} \\ y=y_0+k\frac{a}{(a,b)} \end{cases}$$

是解? 全体解

$ax_1+by_1=k(a,b)$

$a'(x_1-x_0)=b'(y_0-y_1)$

$a' \mid b'(y_0-y_1)$

$a' \mid (y_0-y_1)$

$y_0-y_1=k\frac{a}{(a,b)}$

$c = t(a,b)$ k

$ax+by=c$ $(a,b)|c$ $ax+by=k(a,b)$

$ax+by = t(a,b)$

$ax+b = c$ x_0, y_0

$x = x_0 - k\frac{b}{(a,b)}$

$y = y_0 + k\frac{a}{(a,b)}$

$ax+by = (a,b) = d$

x_0, y_0 $((a,b)x_0, (a,b)y_0)$

$a'x_0 + b'y_0 = 1$

$a'(dx_0) + b(dy_0) = d$

$ax_0 + by_0 = (a,b)$

$ax+by = (a,b)$ (x_0, y_0) $c = t(a,b)$

$a(tx_0) + b(ty_0) = c$

(tx_0, ty_0)

(a,b)

① $ax+by=1$ (x_0, y_0) : exgcd

⇓

② $ax+by=(a,b)$ (x_0', y_0')

⇓

③ $ax+by=c$. $(a,b) \mid c$ (x_0, y_0)

⇓ 结合：之前

④ 做成 ✓ 全体解

$ax+by=c$ $(a,b) \mid c$

$a'x+b'y=\frac{c}{(a,b)}$

$a'x+b'y=1$

最： $ax \equiv b \pmod m$

$ax+my=b$ $x \equiv x_0 \pmod{\frac{m}{(a,m)}}$

有解 $\Longleftrightarrow$ $(a,m) \mid b$

⇓

(x_0, y_0)

$x \in \{0, \ldots, m-1\}$

$x = x_0 + k\frac{m}{(a,m)}$, $k \in \mathbb{Z}$.

$x \equiv x_0 \pmod{\frac{m}{(a,m)}}$

$x = x_0,\ x_0 \pm \frac{m}{(a,m)},\ x_0 \pm \frac{2m}{(a,m)},\ x_0 \pm 3\frac{m}{(a,m)} \cdots$

思考：$(x \bmod m)$ 有多少种？

(a,m)

m.

$m' = \frac{m}{(a,m)}$ $\quad m' \mid m$ $\quad m = (a,m)\,m'$

$x_0 - k\frac{m}{(a,m)} \to x = x_0 \bmod m' < m'$

最小 2,0 or 解 x

证明：$x,\ x+m',\ x+2m',\ \cdots,\ x+(a,m)m'$ ($x+m$)

$0 \le x < m$ 时有多少解

$[0, m')$: x

$[m', 2m')$: $x+m'$

⋮

$[(a,m)-1)m', (a,m)m'=m)$: $x+((a,m)-1)m'$

$(a,m) \mid a$.

$ax \equiv b \pmod m$

有 $(a,m) \nmid b$.

$t \equiv a \pmod n$

$t \equiv b \pmod m$

$\Leftrightarrow$ $t = a + nx = b - my$

$nx + my = b - a$.

有解 $\Leftrightarrow (n,m) \mid (b-a)$

有 x ?

x_0 [redacted]

$t = a + nx$

$x = x_0 + k\frac{m}{(n,m)}$

$$t = a + nx_0 + k\frac{nm}{(n,m)} \qquad k \in \mathbb{Z}$$

$$t \equiv a + nx_0 \pmod{\frac{nm}{(n,m)}} \pmod{[n,m]}$$

$$\frac{nm}{(n,m)} = \mathrm{LCM}(n,m) = l$$

最小公倍数

$n \mid n\cdot\frac{m}{(n,m)}$; $\frac{m}{(n,m)} \in \mathbb{Z}$

$n \mid l$
$m \mid l$

$n = dn'$
$m = dm'$

$dn' \mid l \Leftrightarrow n \mid l$
$dm' \mid l \qquad m' \mid l$

$l = dn'm'$

$$l = d\frac{n}{d}\frac{m}{d} = \frac{nm}{(m,n)}$$

$n = p_1^{a_1} \cdots p_k^{a_k}$

$m = p_1^{b_1} \cdots p_k^{b_k}$

$$\gcd(n,m) = \prod_{i=1}^{k} p_i^{\min(a_i,b_i)}$$

$$\operatorname{lcm}(n,m) = \prod_{i=1}^{k} p_i^{\max(a_i,b_i)}$$

$$= nm = \prod_{i=1}^{k} p_i^{a_i+b_i}$$

费马小定理 $p \nmid a$

p 项. $1, 2, \dots, p-1$

$a, 2a, \dots, (p-1)a$.

$p-1$ 项

$p=5$

$a=3$

$3, 6, 9, 12.$

证明. ① $p \nmid ia$. $1 \le i < p$

② $\forall i \neq j$. $ia \not\equiv ja \pmod p$ ✓

①. ~~$(p,i)=1$ $(p,a)=1$ $(p, ai)=1$~~

$\Rightarrow p \nmid ia$

②. 反证. $i \neq j$. $(i > j)$

$ia \equiv ja \pmod p$

$(i-j)a \equiv 0 \pmod p$

$p \mid$

$0 < i-j < p$ $i < p$

$S = \{(ia) \bmod p\}$

$0 \notin S$. S中元素互不相同

① $S \subset \{1, \cdots, p-1\}$ 一个子集

S 至多 $p-1$ 个

$S = \{1, \cdots, p-1\}$

$a, 2a, \cdots, (p-1)a$ 是 $1, \cdots, p-1$ 的某种排列 $\pmod p$

$a \cdot (2a) \cdots ((p-1)a) \equiv 1 \cdot 2 \cdots (p-1) \pmod p$

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

$a^{p-1} \cdot 1 \cdot 2 \cdots (p-1) \equiv 0 \pmod p$ 与p互质

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

费马小定理.

$(a, p) = 1$. p质

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

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

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

$ba \equiv ab \equiv 1 \pmod{p}$

$\exists b \; (= a^{p-2})$

$\Downarrow a^{-1}$

$a^{p-2} \, ax \equiv a^{p-2} b \pmod{p}$

$x \equiv a^{p-2} \cdot a$

$x \equiv b \cdot a^{p-2}$

$a^{p-2} \sim a^{-1}$

$a \equiv 1$

$a = 1, \ldots, p-1$, 均不为 a^{p-2}

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

$\frac{a}{b} \equiv ? \pmod{p}$ $(b, p) = 1$. 均不为

$a \cdot b^{-1} \equiv a \cdot b^{-1} \cdot \underbrace{b^{p-1}}_{\equiv 1} \equiv a \cdot b^{p-2}$

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

$3x \equiv 5 \pmod 7$

$\div 3 \rightarrow \times 3^{7-2}$

$\times 3$ 再 $\div 3$

$3^5 \equiv 5 \pmod 7$

$x \equiv 5 \times 5 \equiv 4 \pmod 7$

快速求逆元

$\bmod p$

$1^{-1}, 2^{-1}, \dots, n^{-1} \pmod p$

$ax \equiv 1 \pmod p$

$i! = fac(i) = i(i-1)\cdots 1$

$fac(i) = fac(i-1) \cdot i \ \%p$

$facinv(n) = (n!)^{-1} = (n!)^{p-2}$ 快速幂

$facinv(i) = (i!)^{-1}$ $fac(n)^{p-2} \ \%p$

$\frac{1}{i!} = \frac{(i+1)}{(i+1)!} = \frac{i+1}{(i+1)\,i!}$

$\downarrow n-1$

$facinv(i) = (i+1)\,facinv(i+1)$

$\frac{1}{i} = \frac{(i-1)!}{i!} = \frac{(i-1)!}{i(i-1)!}$

$\frac{1}{i} = inv(i) = fac(i-1) \cdot facinv(i) \% p$

$\left(\frac{1}{i}\right)$.

初中规划

高一：浙大：500pts+ → 一本

我：肯定冲500pts+.

NOIP：Day1 T1："小凯的疑惑"

会凯疑惑 2h 不会

300pts (295pts)

WC THUWC/PKC 去不了

NOIP：全省150+，2h：高一前5月份学

→ 11月 NOIP：400+

→ [illegible] 一本

高一：

一轮

88名 → 20+名

15个

APIO → 二轮

我在学也要

圆方树

KD-Tree

个位数 /

APIO

二轮

当天 8:00

7:30 ：起

学点？ → 圆方树

Tree (X)

Day1

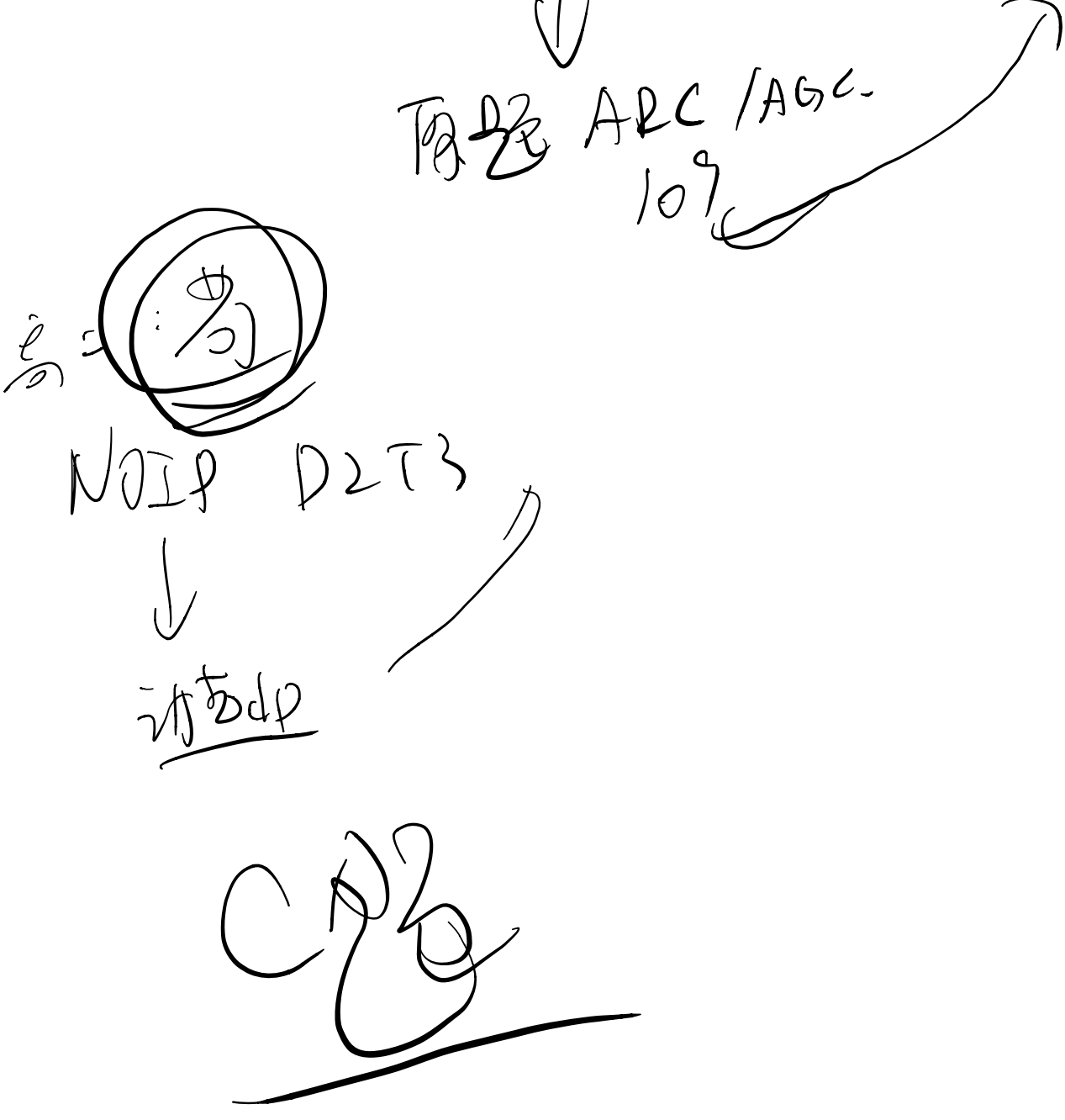
场上：

T1：SB 题

T2：圆：不会

T3：不可做：10/30 pts：10^{12}

$n \le 10^{18}$


预处 ARC /AGC.
109
高:
NOIP D2T3
↓
动态dp
CDQ