提高算法班

乘法逆元、[扩展]欧拉定理、扩展欧几里得算法、[扩展]中国剩余定理

Mas

引理1

引理1

$(a,n)=(b,n)=1$ 的充分必要条件为 $(ab,n)=1$

充分性证明

即证

$$(a,n)=(b,n)=1 \Rightarrow (ab,n)=1$$

由于 $(a,n)=1$, 根据 裴蜀定理 $\exists\, x,y \in \mathbb{Z}$ 使得 $ax + ny = 1$

同理 $\exists\, u,v \in \mathbb{Z}$ 使得 $bu + nv = 1$

两式相乘有

$$(ax + ny)(bu + nv) = 1 \times 1$$

展开得到

$$ab(xu) + n(axv + buy + nyv) = 1$$

引理1

根据裴蜀定理逆定理，显然有 $1 \mid ab \wedge 1 \mid n$ 那么 $(ab,n) = 1$

充分性得证

必要性质证明

即证

$$(ab,n) = 1 \Rightarrow (a,n) = (b,n) = 1$$

若 $(ab,n) = 1$ 互质，但 $(a,n) = d$ 且 $d > 1$

根据最大公约数定义有 $d \mid a$ 且 $d \mid n$

根据整除性质同时也有 $d \mid ab$

即 d 也是 ab 和 n 的公因数，这与 $(ab,n) = 1$ 矛盾

同理可证 $(b,n) = 1$

充分性得证

剩余类、剩余系

剩余类 (residue class)

若 $m \in \mathbb{Z}^+$, 对每个整数 $0 \le r \le m-1$

称集合 $C_r = \{n \mid n \equiv r \bmod m, n \in \mathbb{Z}\}$ 为模 m 的一个剩余类

剩余系 (residue system)

模正整数 m 的余数所组成的集合

完全剩余系 (complete residue system)

整数集 $\mathbb{Z}_m = \{r_1, r_2, \cdots, r_m\}$ 满足:

- 任意不同元素 $r_i \not\equiv r_j \pmod m$
- 任意整数 a , 满足 $r \equiv a \pmod m$

当 $\mathbb{Z}_m = \{0,1,\cdots,m-1\}$ 时称为 **最小非负完全剩余系**

剩余类、剩余系

简化剩余系/缩系 (reduced residue system)

整数集 Φ_m 满足:

- 任意元素 $r \in \Phi_m$ 都有 $(r, m) = 1$
- 任意不同元素 $r_i \not\equiv r_j \pmod{m}$
- $\forall\, (a, m) = 1$ 都存在 $r \in \Phi_m$ 满足 $r \equiv a \pmod{m}$

显然 $\Phi_m \subseteq \mathbb{Z}_m$, $|\Phi_m| = \varphi(m)$

引理2

若 $(x, m) = 1$,$\Phi_m = \{ r_1, r_2, \cdots, r_{\varphi(m)} \}$ 为模 m 的缩系, 则 $S = \{ xr_1, xr_2, \cdots, xr_{\varphi(m)} \}$ 也为模 m 的缩系

证明

对于任意 $x \in S$ 根据 **引理1** 有

$$(r, m) = (x, m) = 1 \Rightarrow (xr, m) = 1$$

引理2

根据缩系定义 $x \in S$ 且 $(x,m)=1$

存在唯一 $r \in \Phi_m$ 满足

$$x \equiv r \pmod m$$

对于两个不同元素 $s_i, s_j \in S$

若 $\exists\, i \neq j, s_i \equiv s_j \pmod m$ 即

$$x \times r_i \equiv x \times r_j \pmod m$$

由于 $(a,m)=1$，根据裴蜀定理 a^{-1} 必然存在

同乘 a^{-1} 可得 $r_i \equiv r_j \pmod m$ ，与假设矛盾

$|\Phi_m| = \varphi(m) = |S|$ 且 S 中元素两两不同余，那么 S 也为模 m 的缩系

命题得证

#3146、互质和

题目描述

给出两个正整数 a, b

若 $\gcd(a,b)=1$,则称 a, b 互质,记为 $a \perp b$

给定正整数 n 请求出

$$\sum_{i=1}^{n} (i \cdot [i \perp n])$$

> 即求出 $1 \sim n$ 范围内所有与 n 互质数之和

输入格式

输入一个正整数 n

输出格式

输出一个整数表示答案

答案可能很大输出 $\bmod 1000000007$ 后的结果

数据规模

对于 20% 的数据 $1 \le n \le 10^5$

对于 40% 的数据 $1 \le n \le 8 \times 10^6$

对于 50% 的数据 $1 \le n \le 2 \times 10^7$

对于全部的数据 $1 \le n \le 10^{15}$

记 Φ_m 为模 m 的 **最小非负简化剩余系**

若 $m > 2$ 有

$$\sum_{i \in \Phi_m} i = \frac{\varphi(m)}{2} m$$

#3146、互质和

令 Φ_m 为模 m 的 **最小非负简化剩余系**

对于 $i \in \Phi_m$ 有

$$(m, i) = (m - i, i) = 1$$

由于 $0 < i < m$, 显然 $0 < m - i < m$ 即 $(m - i) \in \Phi_m$

若 $(m - i) = i$ 有 $(m, i) = i$

- $m > 2 \Rightarrow i > 1$ 此时与简化剩余系性质矛盾
- $m = 2, i = 1$ 此时与 $m > 2$ 条件不符

综上在 Φ_m 中满足条件的 $i, m - i$ 都是成对出现 , 其元素和为

$$\frac{\varphi(m)}{2} m$$

能否以另一种形式证明:

若 $m \in \mathbb{N} \wedge m > 2$ 有 $2 \mid \varphi(m)$

欧拉定理

欧拉定理（**Euler's theorem**）是费马小定理的更一般形式

若 $(a,m)\ =\ 1$ 则有

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

证明

令 Φ_m 为模 m 的最小非负简化剩余系

若 $(a,m)=1$ 根据 **引理2**

$$\prod_{x\in\Phi_m} ax = a^{\varphi(m)} \prod_{x\in\Phi_m} x \equiv \prod_{x\in\Phi_m} x \pmod m$$

$x\in\Phi_m$ 都与 m 互质，根据裴蜀定理 x^{-1} 必然存在

不妨令每个 x 都乘上 x^{-1}

即

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

扩展欧拉定理

对欧拉定理推广

$$a^b \equiv \begin{cases} a^{b \bmod \varphi(m)} & (a,m)=1 \\ a^b & (a,m)\neq 1, b < \varphi(m) \\ a^{(b \bmod \varphi(m))+\varphi(m)} & (a,m)\neq 1, b \geq \varphi(m) \end{cases} \pmod m$$

引理3

若 $a \equiv b \pmod p$ 对于任意整数 k 有

$$ka \equiv kb \pmod{kp}$$

根据同余性质

$p \mid (a-b)$ 即 $a-b = qp$ 其中 $q \in \mathbb{Z}$

两边同乘 k 即

$$ka - kb = q(kp)$$

得证

扩展欧拉定理

证明

- $(a,m)=1$ 时

  根据带余数除法将 b 展开

$$a^b=a^{\left\lfloor\frac{b}{\varphi(m)}\right\rfloor\times\varphi(m)+b \bmod \varphi(m)}=\left(a^{\varphi(m)}\right)^{\left\lfloor\frac{b}{\varphi(m)}\right\rfloor}\times a^{b \bmod \varphi(m)}$$

$$\equiv a^{b \bmod \varphi(m)} \pmod m$$

- $(a,m)\neq 1$ 且 $b<\varphi(m)$ 时

  无需证明

- $(a,m)\neq 1$ 且 $b\geq\varphi(m)$ 时

  取 a 的质因子 p，令 $m=sp^r$ 且 $(s,p)=1$

$$p^{\varphi(s)}\equiv 1 \pmod s$$

扩展欧拉定理

同取 $\varphi(p^r)$ 次方

$$\left(p^{\varphi(s)}\right)^{\varphi(p^r)} = p^{\varphi(s)\times\varphi(p^r)} \equiv 1 \pmod s$$

根据积性函数性质

$$p^{\varphi(s)\times\varphi(p^r)} = p^{\varphi(m)} \equiv 1 \pmod s$$

根据 **引理3** 两边同乘 p^r

$$p^{\varphi(m)+r} \equiv p^r \pmod{sp^r}$$

即

$$p^{\varphi(m)+r} \equiv p^r \pmod m$$

扩展欧拉定理

对于 $b \geq \varphi(m)$ 时，有 $\varphi(m) \geq r$

~~*上述结论求导后较为显然*~~

不求导证明见: https://oj.shiyancang.cn/Public/26.html

即 $b \geq r$

$$p^b = \boldsymbol{p^{b-r}} \times p^r$$

$$\equiv p^{b-r} \times p^{\varphi(m)+r} = p^{b+\varphi(m)} \pmod m$$

同样的有

$$p^{b+\varphi(m)} \equiv p^b \pmod m$$

当 $b - \varphi(m) \geq \varphi(m)$ 时也可写为

$$p^b \equiv p^{b-\varphi(m)} \pmod m$$

即当指数都不小于 $\varphi(m)$ 时，指数存在周期 $\varphi(m)$

扩展欧拉定理

由于 $0 \le b \bmod \varphi(m) < \varphi(m)$

再加上$\varphi(m)$ 那么有 $\left(b \bmod \varphi(m)\right) + \varphi(m) \ge \varphi(m)$

即

$$p^b \equiv p^{(b \bmod \varphi(m))+\varphi(m)} \pmod m \qquad\qquad b \ge \varphi(m)$$

对于任意正整数 k 同样有

$$\left(p^k\right)^b = p^{kb} \equiv p^{kb+\varphi(m)} \equiv p^{kb+k\varphi(m)} = \left(p^k\right)^{b+\varphi(m)} \pmod m$$

同样等价于

$$\left(p^k\right)^b \equiv \left(p^k\right)^{(b \bmod \varphi(m))+\varphi(m)} \pmod m \qquad\qquad b \ge \varphi(m)$$

扩展欧拉定理

将 a 唯一分解为 $p_1^{c_1}p_2^{c_2}\dots p_k^{c_k}$

那么

$$a^b=\left(p_1^{c_1}p_2^{c_2}\dots p_k^{c_k}\right)^b$$

根据同余式可乘性质

$$\left(p_1^{c_1}p_2^{c_2}\dots p_k^{c_k}\right)^b\equiv\left(p_1^{c_1}p_2^{c_2}\dots p_k^{c_k}\right)^{(b \bmod \varphi(m))+\varphi(m)}\pmod m$$

即

$$a^b\equiv a^{(b \bmod \varphi(m))+\varphi(m)}\pmod m$$

命题得证

#2751、扩展欧拉定理

题目描述

给你三个正整数 a, m, b ,你需要求： $a^b \bmod m$

输入格式

一行三个整数 a, m, b

输出格式

一个整数表示答案

输入样例1

```
2 7 4
```

输出样例1

```
2
```

数据范围

对于 100% 的数据, $1 \leq a \leq 10^9, 1 \leq b \leq 10^{2000000}, 1 \leq m \leq 10^8$

威尔逊定理

威尔逊定理（**Wilson's theorem**）给出了判定一个自然数是否为质数的充分必要条件

当且仅当 p 为质数时有

$$(p-1)! \equiv -1 (\mathrm{mod}\, p)$$

证明

必要性

即证明 $(p-1)! \equiv -1 (\mathrm{mod}\, p) \Rightarrow p \in \mathbb{P}$

记 $X = (p-1)! + 1$

若 $p \notin \mathbb{P}$，设 a 为 p 的质因子，根据同余性质有 $p \mid X \Rightarrow a \mid X$

而 $2 \leq a \leq p-1 \Rightarrow a \mid (p-1)!$ 那么 $a \nmid X$，产生矛盾，必要性得证

充分性

即证明 $p \in \mathbb{P} \Rightarrow (p-1)! \equiv -1 (\mathrm{mod}\, p)$

当 $p = 2$ 时通过计算验证成立

威尔逊定理

考虑 $p > 2$ 时

由于 p 为素数，$\forall 1 \le i \le p-1$ 都有 $(i,p)=1$

根据裴蜀定理 i^{-1} 必然存在

考虑何时有 $i = i^{-1}$

$$i^2 \equiv 1 (\bmod p) \Rightarrow p \mid i^2 + 1$$

$$\Rightarrow p \mid (i+1)(i-1)$$

$$\Rightarrow p \mid (i+1) \vee p \mid (i-1)$$

当 $p > 2$ 时不存在 $p \mid (i+1) \wedge p \mid (i-1)$，若存在则说明 $p \mid (i+1)-(i-1) = 2$

仅当 $i+1 = p$ 或 $i-1 = p$ 时成立

即仅当 $i = 1, i = p-1$ 时 $i = i^{-1}$

即对于 $2 \le i \le p-2$ 存在不为自身的乘法逆元

威尔逊定理

由于 $2 \mid (p-3)$，对于 $2 \le i \le p-2$ ，不妨令 i 与 i^{-1} 两两配对有

$$(p-1)! \equiv 1 \times 1^{\frac{p-3}{2}} \times (p-1) \equiv -1 (\bmod\, p)$$

命题得证

Gauss 对威尔逊定理进行了推广

$$\prod_{\substack{i=1 \\ \gcd(i,n)=1}}^{n} i = \begin{cases} -1 \pmod{n}, & \text{if } n = 4 \lor n = p^k \lor n = 2p^k \\ 1 \pmod{n}, & \text{otherwise} \end{cases}$$

其中 p 为奇质数 n, k 为任意正整数

读者可自行尝试证明

#2750、威尔逊定理

题目描述

这还是一道模板题,给你一个正整数 n 求

$$(n-1)! \mod n$$

输入格式

第一行输入一个正整数 T ,表示 T 组数据
接下来 T 行,每行一个正整数 n

输出格式

对于每一组输出一行, $(n-1)! \mod n$ 的结果

数据规模

对与全部的数据 $1 \leq T \leq 10^4, 1 \leq n \leq 2 \times 10^9$

若 n 为 1 结果为 0

根据 **威尔逊定理** , 若 n 为质数结果为 $n-1$

若 n 为合数 , 必然存在 $n = a \times b$ 且有 $1 < a, b < n$

- 若 $a \neq b$

  不妨假设 $1 < a < b < n$

  那么

  $(n-1)! = 1 \times 2 \times \cdots \times \boldsymbol{a} \times \cdots \times \boldsymbol{b} \times \cdots \times (n-1) \equiv 0 \pmod n$

- 若 $a = b$

  - 若 a 不为质数

    令 $a = x \times y$ 且有 $x, y < a$

#2750、威尔逊定理

那么

$$(n-1)! = 1\times 2\times \boldsymbol{x}\times\cdots\times \boldsymbol{y}\cdots\times \boldsymbol{a}\times\cdots\times (n-1)\equiv 0 \pmod n$$

- 若 a 为质数

那么 a 无法分解

考虑 $2a$ 是否在 $1\sim n-1$ 范围内，即

$$2\sqrt{n}\le n-1$$

解得 $n\ge 2\sqrt{2}+3$

即 $n=4$ 时不满足条件此时答案为 2

否则

$$(n-1)! = 1\times 2\times\cdots\times \boldsymbol{a}\times\cdots\times \boldsymbol{2a}\times\cdots\times (n-1)\equiv 0 \pmod n$$

扩展欧几里得

形如

$$ax \equiv c \pmod b$$

的方程被称为线性同余方程（**Congruence Equation**）

方程 $ax + by = c$ 与方程 $ax \equiv c \pmod b$ 等价

根据裴蜀定理、欧几里得算法

$$ax + by = (a, b) \Leftrightarrow (b, a \bmod b) = bx' + (a \bmod b)y'$$

其中 $a \bmod b$ 为 $a - \left\lfloor \frac{a}{b} \right\rfloor b$ 代入上式后可得

$$bx' + (a \bmod b)y' = bx' + \left(a - \left\lfloor \frac{a}{b} \right\rfloor b\right)y'$$

$$= ay' + b(x' - \left\lfloor \frac{a}{b} \right\rfloor y')$$

扩展欧几里得

得出 x,y 和 x',y' 的关系

$$\begin{cases} x = y' \\ y = x' - \left\lfloor \frac{a}{b} \right\rfloor y' \end{cases}$$

当 $b = 0$ 时, a 为 (a,b)

当且仅当 $x' = 1$ 时等式成立

y' 可以为任何值，为方便起见不妨设 $y' = 0$

根据 $x = y', y = x' - \left\lfloor \frac{a}{b} \right\rfloor y'$ 可倒推出 x 和 y 的解

上述倒推过程为 **裴蜀定理** 的另一形式证明

扩展欧几里得

$ax+by=c$ 有无穷组解，扩展欧几里得算法可求出其中一组特解 x_0, y_0

显然 $a(x_0+kb)+b(y_0-ka)=c$，可以得出

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

但该形式并不能覆盖所有解

$$\begin{cases} ax + by = c \\ ax_0 + by_0 = c \end{cases} \Rightarrow ax + by = ax_0 + by_0$$

$$\Rightarrow a(x-x_0) = b(y_0-y) \Rightarrow \frac{a}{(a,b)}(x-x_0) = \frac{b}{(a,b)}(y_0-y)$$

$$\Rightarrow \frac{a}{(a,b)}(x-x_0) \mid \frac{b}{(a,b)}(y_0-y) \wedge \frac{b}{(a,b)}(y_0-y) \mid \frac{a}{(a,b)}(x-x_0)$$

扩展欧几里得

由于 $\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right) = 1$ 那么有

$$\frac{a}{(a,b)} \mid (y_0 - y)$$

即存在 $k \in \mathbb{Z}$ 满足

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

将 $y = y_0 - \frac{a}{(a,b)}k$ 代入 $a(x - x_0) = b(y_0 - y)$

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

扩展欧几里得

因此方程 $ax + by = c$ 的通解如下

$$\begin{cases} x = x_0 + k\dfrac{b}{(a,b)} \\ y = y_0 - k\dfrac{a}{(a,b)} \end{cases} \quad k \in \mathbb{Z}$$

对于某些情况下，要求最小非负整数解

若 $\frac{b}{(a,b)}$ 非负，由于 $x_{\min} = x_0 + k\frac{b}{(a,b)}$ 那么

$$x_{\min} = \left(\frac{b}{(a,b)} + \left(x_0 \bmod \frac{b}{(a,b)}\right)\right) \bmod \frac{b}{(a,b)}$$

#2749、同余方程

题目描述

求关于 x 的同余方程

$$ax \equiv 1 \pmod b$$

的最小正整数解。

输入格式

输入两个正整数 a, b ,用一个空格隔开

输出格式

一个正整数 x_0 ,即最小正整数解

> *输入数据保证一定有解*

数据规模

对于 40% 的数据, $2 \le b \le 1000$
对于 60% 的数据, $2 \le b \le 5 \times 10^6$
对于 100% 的数据, $2 \le a, b \le 2 \times 10^9$

```cpp
#include <bits/stdc++.h>
using namespace std;
int n, b, x, y;
int exgcd(int a, int b, int &x, int &y)
{
    if (!b)
    {
        x = 1, y = 0;
        return a;
    }
    int res = exgcd(b, a % b, y, x);
    y -= a / b * x;
    return res;
}
int main()
{
    cin >> n >> b;
    exgcd(n, b, x, y);
    cout << (b + x % b) % b;
    return 0;
}
```

#791、青蛙的约会

题目描述

两只青蛙在网上相识了,它们聊得很开心,于是觉得很有必要见一面

它们很高兴地发现它们住在同一条纬度线上,于是它们约定各自朝西跳,直到碰面为止

可是它们出发之前忘记了一件很重要的事情,既没有问清楚对方的特征,也没有约定见面的具体位置

不过青蛙们都是很乐观的,它们觉得只要一直朝着某个方向跳下去,总能碰到对方的

但是除非这两只青蛙在同一时间跳到同一点上,不然是永远都不可能碰面的

为了帮助这两只乐观的青蛙,你被要求写一个程序来判断这两只青蛙是否能够碰面,会在什么时候碰面

两只青蛙分别叫做青蛙 A 和青蛙 B

规定纬度线上东经 0 度处为原点,由东往西为正方向,单位长度 1 米

这样我们就得到了一条首尾相接的数轴

设青蛙 A 的出发点坐标是 x ,青蛙 B 的出发点坐标是 y

青蛙 A 一次能跳 m 米,青蛙 B 一次能跳 n 米,两只青蛙跳一次所花费的时间相同

纬度线总长 L 米,求出它们跳了几次以后才会碰面

数据范围

对于 100% 的数据, $0 \leq x, y < 2 \times 10^9, 0 < m, n < 2 \times 10^9, 0 < L < 2.1 \times 10^9, x \neq y$

输入格式

输入只包括一行 5 个整数 x, y, m, n, L

输出格式

输出碰面所需要的跳跃次数

如果永远不可能碰面则输出一行 `Impossible`

#791、青蛙的约会

设两只青蛙一共跳了 t 次相遇，共跳了 k 为圈数

$$x + tm \equiv y + tn \pmod{l} \Leftrightarrow x + tm - y - tn = kl$$

整理得

$$t(m-n) - kl = y - x$$

使用扩展欧几里得算法解线性同余方程

$$t(m-n) - kl = \gcd(m-n, l)$$

的一个特解 t_0

最小非负整数解 $t = \left(t_0 \bmod \frac{l}{\gcd(m-n,l)} + \frac{l}{\gcd(m-n,l)}\right) \bmod \frac{l}{\gcd(m-n,l)}$

若 $(y-x) \nmid \gcd(m-n, l)$ 则无解

否则将 t 扩大 $\frac{y-x}{\gcd(m-n,l)}$ 倍即可

#791、青蛙的约会

仅保证 t 最小非负，是否有可能圈数 $k < 0$？

$$\frac{t(m-n)-\gcd(m-n,l)}{l}=k$$

若 $m-n>0$ 那么 $\gcd(m-n,l) \le m-n$

由于已保证 t 非负，若 $t=0$ 此时 $k=0$

否则 $t>0$ 显然有 $k>0$

若 $m-n=0$

仅当 $x \equiv y \pmod{l}$ 时有解，此时 $t=k=0$

若 $m-n<0$

可将原式转为 $t(n-m)+kl=x-y$ 求解

此时同样有 $k \ge 0$

乘法逆元

给定两个整数 a 和 m , 假设存在整数 x 满足

$$ax \equiv 1 (\mathrm{mod}\ m)$$

那么称 x 为 a 关于 m 的乘法逆元 , 记作 a^{-1} (若逆元存在必然有 $(a,m) = 1$) , 可直接扩展欧几里得算法求解

也可对上式变形

$$ax \equiv 1 \ (\mathrm{mod}\ m) \Rightarrow ax \equiv a^{\varphi(m)} \ (\mathrm{mod}\ m)$$

$$\Rightarrow x \equiv a^{\varphi(m)-1} (\mathrm{mod}\ m)$$

利用快速幂求解

令 $f(x) = x^{-1}$ (保证模意义下逆元存在) $f(x)$ 为 **完全积性函数** , 即有 $f(ab) = f(a) \times f(b)$

$$a \times b \times f(ab) = (ab) \times (ab)^{-1} = a \times a^{-1} \times b \times b^{-1} = a \times f(a) \times b \times f(b)$$

$$\Rightarrow f(ab) = f(a) \times f(b)$$

这意味着当逆元存在时 , 多个数乘积的逆元等于这些数的逆元的乘积

乘法逆元

若要求 $1 \sim n$ 中每个数模 p 的逆元，上述方式不优

显然

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

考虑 $i > 1$ 时的 i^{-1}

记 $k = \left\lfloor \frac{p}{i} \right\rfloor, r = p \bmod i$ 有 $p = ki + r$

不难得出

$$ki + r \equiv 0 \pmod p$$

两边同时乘 $i^{-1} \times r^{-1}$

$$kr^{-1} + i^{-1} \equiv 0 \pmod p$$

即

$$i^{-1} \equiv -kr^{-1} \pmod p$$

乘法逆元

将 $k = \left\lfloor \frac{p}{i} \right\rfloor, r = p \bmod i$ 代入

$$i^{-1} \equiv -\left\lfloor \frac{p}{i} \right\rfloor (p \bmod i)^{-1} \pmod p$$

考虑递推求解

由于 $r = p \bmod i < i$, 可认为 r^{-1} 已知

$$i^{-1} \equiv \begin{cases} 1, & i = 1 \\ -\left\lfloor \frac{p}{i} \right\rfloor (p \bmod i)^{-1}, & 2 \le i \end{cases} \pmod p$$

事实上当 $i \mid p$ 时 i^{-1} 并不存在 , 此时 $r = 0$ 同样 r^{-1} 也不存在

但 $p \in \mathbb{P}$ 可保证 i^{-1} 与 r^{-1} 必然存在

不难证明： $2 \nmid p$ 时 $2^{-1} \equiv \frac{p+1}{2} \pmod p$

#919、乘法逆元

题目描述

给定正整数 n 与 p

求 $1 \sim n$ 中的所有数在模 p 意义下的乘法逆元

输入格式

一行两个正整数 n 与 p

输出格式

n 行

第 i 行一个正整数,表示 i 在模 p 意义下的乘法逆元

数据范围

对于全部的数据 $1 \le n \le 3 \times 10^6, n < p < 20000528$, p 为质数

```
inv[1] = 1;
for (int i = 2; i <= n; i++)
  inv[i] = p - p / i * inv[p % i] % p;
for (int i = 1; i <= n; i++)
  printf("%lld\n", inv[i]);
```

时间复杂度 $O(n)$

是否有可能存在 $i \mid p$?

乘法逆元

有时需要 n 个求 $1 \sim p-1$ 范围内逆元

记第 i 个询问为 a_i 令

$$\mathrm{S}_i = \prod_{j=1}^{i} a_j$$

使用快速幂/扩展欧几里得计算 S_n 的逆元，记为 Sv_n

由于 Sv_n 是 n 个数的积的逆元

所以当把 Sv_n 乘 a_n 时，a_n 与 a_n^{-1} 抵消，得到 $a_1 \sim a_{n-1}$ 的积逆元，记为 Sv_{n-1}

同理可依次计算出所有的 Sv_i

不难发现

$$a_i^{-1} = \mathrm{S}_{i-1} \times \mathrm{Sv}_i$$

时间复杂度 $O(n + \log p)$

#2748、又是乘法逆元

题目描述

给定 n 个正整数,求每个数在模 p 意义下的乘法逆元

> *请使用高效的读入方式*

输入格式

第一行一个整数 n

第二行 n 个整数 a_i

输出格式

一行一个数表示

$$\sum_{i=1}^{n} a_i^{-1} \times 998244353^{n-i} \pmod p$$

数据范围

对于全部的数据, $1 \leq n \leq 10^6, 1 \leq a_i < p, p = 10^9 + 7$

中国剩余定理

引理4

$$\begin{cases} a \equiv b \pmod{\mathrm{m}_1} \\ a \equiv b \pmod{\mathrm{m}_2} \\ \quad\cdots \\ a \equiv b \pmod{\mathrm{m}_n} \end{cases} \Rightarrow \quad a \equiv b \pmod{\mathrm{M}_n}$$

证明

考虑仅有两个数时的情况即

$$\begin{cases} a \equiv b \pmod{\mathrm{m}_1} \\ a \equiv b \pmod{\mathrm{m}_2} \end{cases} \Rightarrow \quad a \equiv b \pmod{[\mathrm{m}_1, \mathrm{m}_2]}$$

根据同余性质 $\begin{cases} a - b = k_1\mathrm{m}_1 \\ a - b = k_2\mathrm{m}_2 \end{cases} \Rightarrow k_1\mathrm{m}_1 = k_2\mathrm{m}_2 \ \ (k_1, k_2 \in \mathbb{Z})$

记 $d = (\mathrm{m}_1, \mathrm{m}_2)$, 则 $\mathrm{m}_1 = pd$, $\mathrm{m}_2 = qd$

可得 $k_1 p = k_2 q \Rightarrow p \mid k_2 q$

显然 $(p, q) = 1$ 根据互质的性质有 $p \mid k_2$

中国剩余定理

设 $k_2 = pu\ (u \in \mathbb{Z})$，代入 $a - b\ =\ k_2\mathrm{m}_2$ 中

$$a - b\ = u\frac{\mathrm{m}_1\mathrm{m}_2}{d} = u[\mathrm{m}_1, \mathrm{m}_2]$$

即 $n =\ 2$ 时成立

假设 $n = k$ 时成立，考虑 $n = k + 1$ 时

$$\begin{cases} a \equiv b \pmod{\mathrm{M}_k} \\ a \equiv b \pmod{\mathrm{m}_{k+1}} \end{cases}$$

由于 $\mathrm{M}_{k+1}\ = [\mathrm{M}_k, \mathrm{m}_{k+1}]$ 即 $a \equiv b \pmod{\mathrm{M}_{k+1}}$

命题得证

根据引理可得出：模最小公倍数范围内，任意不同数对各个模的余数组合不同

中国剩余定理

孙子算经：

有物不知其数,三三数之剩二,五五数之剩三,七七数之剩二问物几何?

上面具体问题的解答口诀由明朝数学家程大位在《算法统宗》中给出:

三人同行七十希，五树梅花廿一支，七子团圆正半月，除百零五便得知

上述问题等价于求解线性同余方程组

$$\begin{cases} X \equiv 2 \pmod 3 \\ X \equiv 3 \pmod 5 \\ X \equiv 2 \pmod 7 \end{cases}$$

考虑构造一个解

$$X = X_1 + X_2 + X_3$$

令 $X_1 = 70x_1$ 且 $X_1 \equiv 2 \pmod 3$，类似的其余部分恰被模数整除

$$X = 35x_1 + 21x_2 + 15x_3$$

中国剩余定理

求解

$$70x_1 \equiv\ 2\ (\mathrm{mod}\ 3)$$

由于 $(70,3) = 1$, 必然存在乘法逆元 , 同乘逆元可求出 x_1

类似的 $(21,5) = (15,7) = 1$

解得

$$\begin{cases} x_1 = 1 \\ x_2 = 3 \\ x_3 = 2 \end{cases}$$

综上通解 $\mathrm{X} = 233$

X 在模 [3,5,7] 下存在唯一解即

$$\mathrm{X} = 233\ \mathrm{mod}\ 105 = 23$$

中国剩余定理

将问题形式化

$$\begin{cases} x \equiv a_1 \pmod{\mathrm{m}_1} \\ x \equiv a_2 \pmod{\mathrm{m}_2} \\ \qquad \vdots \\ x \equiv a_n \pmod{\mathrm{m}_n} \end{cases}$$

其中 a_i, m_i 为给定常数，且当 $i \neq j$ 时 $(\mathrm{m}_i, \mathrm{m}_j) = 1$

中国剩余定理（**Chinese Remainder Theorem**）给出了构造解的方法

令

$$\mathrm{M} = \prod_{i=1}^{n} \mathrm{m}_i \qquad \mathrm{M}_i = \frac{\mathrm{M}}{\mathrm{m}_i} \qquad \mathrm{M}_i\,\mathrm{t}_i \equiv 1 \pmod{\mathrm{m}_i}$$

在模 M 意义下的唯一解 X 为

$$\mathrm{X} \equiv \sum_{i=1}^{n} a_i \mathrm{M}_i \mathrm{t}_i \pmod{\mathrm{M}}$$

中国剩余定理

存在性

显然 $(\mathrm{M}_i, \mathrm{m}_i) = 1$, 根据 **裴蜀定理** 在模 m_i 意义下 t_i 必然存在

$\forall\ 1 \le i \le\ n$ 有 $\mathrm{m}_i \mid \mathrm{M}$

$\forall\ 1 \le j \le\ n$ 且 $j \ne\ i$ 有 $\mathrm{m}_i \mid \mathrm{M}_j = \frac{\mathrm{M}}{\mathrm{m}_j}$ 即 $\mathrm{M}_j \equiv 0 \pmod{\mathrm{m}_i}$

那么有

$$\mathrm{X} \equiv a_i\mathrm{M}_i\mathrm{t}_i + \sum_{\substack{j=1 \\ j\ne i}}^{n} a_j\mathrm{M}_j\mathrm{t}_j \equiv a_i\mathrm{M}_i\mathrm{t}_i \equiv a_i \pmod{\mathrm{m}_i}$$

所以 X 为方程组的一个解

中国剩余定理

唯一性

设 $Y \in \mathbb{Z}$ 为方程组的一个解，即 $\forall\, 1 \le i \le n$ 都有 $Y \equiv a_i \pmod{m_i}$

同样的 X 也为方程组一个解所以有

$$X \equiv Y \equiv a_i \pmod{m_i}$$

根据 **引理4**

$$X \equiv Y \pmod{[m_1, m_2, \cdots m_n]}$$

$$\Rightarrow X \equiv Y \pmod{M}$$

所以解在模 M 意义下的唯一

单射、满射、双射

实验舱 青少年编程 LAB 走近科学 走进名校

单射 (injection)

映射 f: A → B 为单射当且仅当 $a, b \in$ A 有 $f(a) = f(b) \Longrightarrow a = b$

$f : \mathbb{R} \to \mathbb{R}$ 定义 $f(x) = 2x + 1$, f 是单射

$f : \mathbb{R} \to \mathbb{R}$ 定义 $f(x) = x^2$, f 不是单射 (如 $2^2 = (-2)^2$ 即存在多对一)

满射 (surjection)

映射 f: A → B 为满射当且仅当 $b \in$ B 存在 $a \in$ A 满足 $f(a) = b$

$f : \mathbb{R} \to \mathbb{R}$ 定义 $f(x) = 2x + 1$, f 是满射

$f : \mathbb{R} \to \mathbb{R}$ 定义 $f(x) = x^2$, f 不是满射 (在 $x \in \mathbb{R}$ 上不存在 $x^2 = -1$)

而 $f : \mathbb{R} \to \mathbb{R}^*$ 定义 $f(x) = x^2$, f 是满射

双射 (bijection)

映射 f: A → B 为双射当且仅当 $b \in$ B 存在 **唯一** $a \in$ A 满足 $f(a) = b$

单射、满射、双射

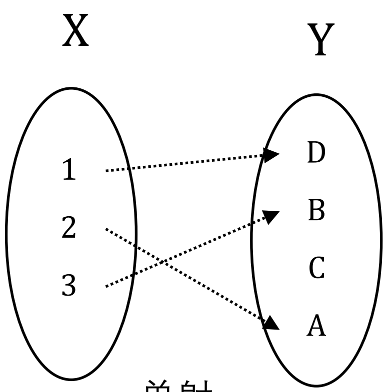
$f:\mathbb{R}\to\mathbb{R}$ 定义 $f(x)=x^3-x$, f 不是双射 (如 $x\in\{-1，0，1\}$ 都有 $f(x)=0$ 即对应关系不唯一)

$f:\mathbb{R}\to\mathbb{R}$ 定义 $f(x)=e^x$, f 不是双射 (不存在 $f(x)=-1$)

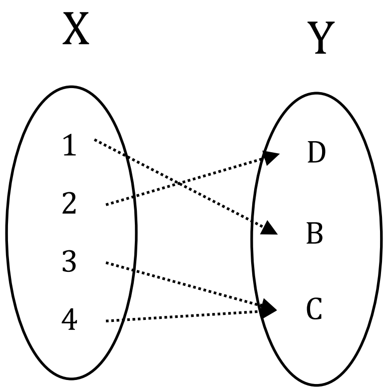
同时满足单射和满射的映射关系 , 即为双射

双射说明了两个有限集合 A 和 B 的元素数目相等

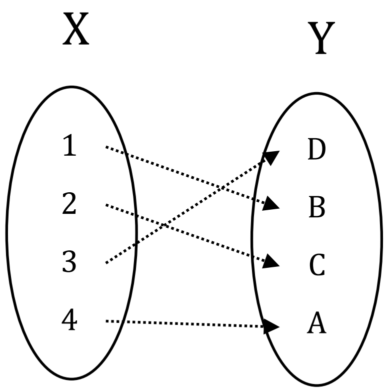
在组合数学中 , 若 $f\colon A\to B$ 满足双射 , 可将 A 的元素计数问题转为 B 的元素计数问题



单射



满射



双射

中国剩余定理 & 欧拉函数

若 $\gcd(n,m)=1$ 有 $\varphi(nm)=\varphi(n)\varphi(m)$

证明

记集合 $\mathrm{S}(n)=\{1\le x\le n\mid \gcd(x,n)=1\}$ 显然 $|S(n)|=\varphi(n)$

记集合 $\mathrm{D}(n,m)=\{\langle x,y\rangle\mid x\in \mathrm{S}(n),y\in \mathrm{S}(m)\}$ 其中 $\gcd(n,m)=1$ 显然 $|\mathrm{D}(n,m)|=|\mathrm{S}(n)|\times|\mathrm{S}(m)|=\varphi(n)\times\varphi(m)$

若能证明 $f:\mathrm{S}(nm)\to \mathrm{D}(n,m)$ 存在一一对应关系(**双射**) 那么原命题即得证

考虑集合 $\mathrm{S}(nm)$ 与集合 $\mathrm{D}(n,m)$ 的关系

对于 $u\in \mathrm{S}(nm)$ 可认为 $(u \bmod n, u \bmod m)\in \mathrm{D}(n,m)$ 根据整除性质 $u\notin\{0,n,m,nm\}$ 否则 $\gcd(u,nm)\ne 1$

根据**引理1** $\gcd(u,n)=\gcd(u,m)=1 \Leftrightarrow \gcd(u,nm)=1$

根据上述性质 $\gcd(u,n)=1=\gcd(u \bmod n,n)$ 又有 $0\le u \bmod n<n$ 即 $u \bmod n\in \mathrm{S}(n)$

同理有 $u \bmod m\in \mathrm{S}(m)$

即 $\mathrm{S}(nm)$ 与集合 $\mathrm{D}(n,m)$ 存在映射关系

中国剩余定理 & 欧拉函数

存在性质 : 若 $\gcd(n,m) = 1$, $n \mid a \wedge m \mid a$ 则有 $nm \mid a$

$n \mid a$ 那么 $a = nk\ (k \in \mathbb{Z})$, 由于 $m \mid a = nk \Rightarrow m \mid k$ 同乘 n 即 $nm \mid nk = a$

$\forall\, u \in \mathrm{S}(nm)$, $v \in \mathrm{S}(nm)$ 若存在 $\langle u \bmod n , u \bmod m\rangle = \langle v \bmod n , v \bmod m\rangle$ 则说明

$$\begin{cases} u \equiv v \pmod n \\ u \equiv v \pmod m \end{cases} \Rightarrow \begin{cases} n \mid u - v \\ m \mid u - v \end{cases} \Rightarrow nm \mid u - v$$

由于 $1 \le u, v \le nm$ 那么 $p = q$, 即 $\mathrm{S}(ab)$ 到 $\mathrm{D}(a,b)$ 存在 **单射关系**

$\forall\, (x,y) \in \mathrm{D}(n,m)$ 若根据 **中国剩余定理** 必然唯一存在 $0 \le u \le nm$ 满足

$$\begin{cases} u \equiv x \pmod n \\ u \equiv y \pmod m \end{cases}$$

同时 $\gcd(x,n) = \gcd(u \bmod n, n) = 1 = \gcd(u , n)$, 即 $u \in \mathrm{S}(nm)$

即 $\mathrm{S}(ab)$ 到 $\mathrm{D}(a,b)$ 存在 **满射关系**

综上 $\mathrm{S}(ab)$ 到 $\mathrm{D}(a,b)$ 存在一一对应关系

命题得证

#793、曹冲养猪

题目描述

自从曹冲搞定了大象以后,曹操就开始琢磨让儿子干些事业,于是派他到中原养猪场养猪

可是曹冲很不高兴,于是在工作中马马虎虎,有一次曹操想知道母猪的数量
于是曹冲想狠狠耍曹操一把

举个例子

假如有 16 头母猪,如果建了 3 个猪圈,剩下 1 头猪就没有地方安家了

如果建造了 5 个猪圈,但是仍然有 1 头猪没有地方去

如果建造了 7 个猪圈,还有 2 头没有地方去

你作为曹总的私人秘书理所当然要将准确的猪数报给曹总,你该怎么办?

输入格式

第一行包含一个整数 n ,表示建立猪圈的次数

接下来 n 行,每行两个整数 a_i, b_i ,表示建立了 a_i 个猪圈,有 b_i 头猪没有去处

你可以假定 a_i, a_j 互质

输出格式

输出仅包含一个正整数
即为曹冲至少养猪的数目

数据范围

对于全部数据, $1 \leq n \leq 10, 1 \leq b_i \leq a_i \leq 1000$

```
long long CRT()
{
    long long res = 0, M = 1;
    for (int i = 1; i <= n; i++)
        M *= b[i];
    for (int i = 1; i <= n; i++)
    {
        long long Mi = M / b[i], ti = inv(Mi, b[i]);
        res = (res + (a[i] * Mi * ti)) % M;
    }
    return res;
}
```

扩展中国剩余定理

当模数不保证互质时，求解线性同余方程组

- 两个方程时

$$\begin{cases} X \equiv a_1 \pmod{m_1} \\ X \equiv a_2 \pmod{m_2} \end{cases}$$

上述问题等价于

$$a_1 + m_1 p = a_2 + m_2 q$$

变形为

$$m_1 p - m_2 q = a_2 - a_1$$

根据裴蜀定理

当且仅当 $(m_1, m_2) \mid (a_2 - a_1)$ 时有解

扩展中国剩余定理

通过扩展欧几里得求出一组特解 p_0, q_0

其通解为

$$\begin{cases} p = p_0 + k\dfrac{\mathrm{m}_2}{(\mathrm{m}_1, \mathrm{m}_2)} \\ q = q_0 - k\dfrac{\mathrm{m}_1}{(\mathrm{m}_1, \mathrm{m}_2)} \end{cases}$$

通过 p_0 也可得出一组 X 的一个特解

$$\mathrm{X}_0 = p_0\mathrm{m}_1 + a_1$$

- 多个方程时

若有 n 个线性同余方程

考虑求出满足首个方程的特解

并将首个与第二个方程合并后再次求解

扩展中国剩余定理

X 通解为

$$X = a_1 + m_1\left(p_0 + k\frac{\mathrm{m}_2}{(\mathrm{m}_1, \mathrm{m}_2)}\right)$$

$$= a_1 + p_0\mathrm{m}_1 + k\frac{\mathrm{m}_1\mathrm{m}_2}{(\mathrm{m}_1, \mathrm{m}_2)}$$

$$= a_1 + p_0\mathrm{m}_1 + k[\mathrm{m}_1, \mathrm{m}_2]$$

其中 $a_1, \mathrm{m}_1, \mathrm{m}_2, p_0$ 均为已知数

所以两个线性同余方程等价于

$$X \equiv a_1 + p_0\mathrm{m}_1 \pmod{[\mathrm{m}_1, \mathrm{m}_2]}$$

将其特解累加

最终解在模 $[\mathrm{m}_1, \mathrm{m}_2, \cdots, \mathrm{m}_n]$ 意义下唯一

#3208、扩展中国剩余定理

题目描述

给定 n 组非负整数 a_i, b_i ,求解关于 x 的方程组的最小非负整数解

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

输入格式

输入第一行包含整数 n

接下来 n 行,每行两个非负整数 m_i, a_i

输出格式

输出一行,为满足条件的最小非负整数 x

数据规模

对于 100% 的数据, $1 \le n \le 10^5, 1 \le b_i, a_i \le 10^{12}$,保证所有 a_i 的最小公倍数不超过 10^{18}

> *请注意程序运行过程中进行乘法运算时结果可能有溢出的风险*
>
> *数据保证有解*

```cpp
LL excrt(const vector<LL> &m, const vector<LL> &a)
{
  LL m0 = m[0], a0 = a[0], x, y;
  for (int i = 1; i < m.size(); i++)
  {
    LL d = exgcd(m0, m[i], x, y), k = m[i] / d;
    LL c = (a[i] - a0 % m[i] + m[i]) % m[i];
    if (c % d)
      return -1;
    x = mul(x, c / d, k);
    a0 = a0 + x * m0;
    m0 = m0 / d * m[i];
  }
  return (a0 % m0 + m0) % m0;
}
```

本题数据范围较大，直接相乘可能将导致溢出

可选择 ~~int128 作为~~数据类型

考虑龟速乘

#3208、扩展中国剩余定理

对于两个方程合并后的结果

$$\mathrm{m}_1 p - \mathrm{m}_2 q = a_2 - a_1$$

$$\Rightarrow \mathrm{m}_1 p \equiv a_2 - a_1 \pmod{\mathrm{m}_2}$$

对于 $a_2 - a_1$ 仅需保留模 m_2 意义下的非负整数

对于两组方程求出的特解 p_0 将其转为最小非负整数解后，再将其放大 $\frac{a_2-a_1}{\gcd(\mathrm{m}_1,\mathrm{m}_2)}$ 倍

根据解系的特征显然有 $\frac{\mathrm{m}_2}{\gcd(\mathrm{m}_1,\mathrm{m}_2)}$ 为周期

对于 p_0 仅需保留模 $\frac{\mathrm{m}_2}{\gcd(\mathrm{m}_1,\mathrm{m}_2)}$ 意义下的非负整数

由于保证了模数的最小公倍数不会溢出，所以其它情况无需考虑溢出

实验舱
青少年编程
走近科学 走进名校

谢谢观看