

{% note info %} 摘要 Title: 223. 阿九大战朱最学 Tag: 中国剩余定理 Memory Limit: 64 MB Time Limit: 1000 ms  
{% endnote %}

Powered by: NEFU AB-IN

Link

@TOC

## 223. 阿九大战朱最学

### • 题意

自从朱最学搞定了 QQ 农场以后，就开始捉摸去 QQ 牧场干些事业，不仅在自己的牧场养牛，还到阿九的牧场放牛！阿九很生气，有一次朱最学想知道阿九牧场奶牛的数量，于是阿九想狠狠耍朱最学一把。举个例子，假如有 16 头奶牛，如果建了 3 个牛棚，剩下 1 头牛就没有地方安家了。如果建造了 5 个牛棚，但是仍然有 1 头牛没有地方去，然后如果建造了 7 个牛棚，还有 2 头没有地方去。你作为阿九的私人秘书理所当然要将准确的奶牛数报给阿九，你该怎么办？假定不同  $a_i$  之间互质。

### • 思路

中国剩余定理板子问题

前提  $m_1, m_2, \dots, m_k$  两两互质

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

结果

$$x = a_1 \cdot M_1 \cdot M_1^{-1} + a_2 \cdot M_2 \cdot M_2^{-1} + \dots + a_k \cdot M_k \cdot M_k^{-1}$$

$$M = m_1 \cdot m_2 \cdot \dots \cdot m_k$$

$$M_i = \frac{M}{m_i}$$

$M_i^{-1}$  表示  $M_i$  模  $m_i$  的逆

由于要模  $m_i$ ，但  $m_i$  不一定是质数，但  $M_i$  肯定与  $m_i$  互质，所以用 exgcd 求逆元  
如  $ax \equiv 1 \pmod{n} \rightarrow ax - ny = 1 \rightarrow ax + ny' = 1$  等式一定有解  
 $x$  就是  $a$  的逆元

### 最小正解为啥是模 $p$

答： $p$  是所有模数的乘积， $(x + p) \equiv x \pmod{a_i}$  后，仍然是一个解，因为  
 $x \equiv x + p \pmod{a_i}, p = \prod_{i=1}^k a_i$

### • 代码

## 中国剩余定理

```

'''
Author: NEFU AB-IN
Date: 2022-03-11 15:59:10
FilePath: \ACM\Acwing\223.py
LastEditTime: 2022-03-11 16:59:46
'''

N = 20
m, a = [0] * N, [0] * N

def exgcd(a, b):
    global x, y
    if b == 0:
        x, y = 1, 0
        return a
    d = exgcd(b, a % b)
    x, y = y, x
    y -= (a // b) * x
    return d

n = int(input())

M = 1 # 模数之积
for i in range(n):
    m[i], a[i] = map(int, input().split()) #模数, 余数
    M *= m[i]

x, y, ans = 0, 0, 0
for i in range(n):
    Mi = M // m[i]
    exgcd(Mi, m[i])
    ans += a[i] * Mi * x #每次加上 M * (M^-1) * a[i]

print((ans + M) % M) # ans + M 仍然是一个解

```

## 中国剩余定理拓展版

```

'''
Author: NEFU AB-IN
Date: 2022-03-11 20:29:00
FilePath: \ACM\Acwing\204.py
LastEditTime: 2022-03-11 21:05:51
'''

```

```
def exgcd(a, b):
    global k1, k2
    if b == 0:
        k1, k2 = 1, 0
        return a
    d = exgcd(b, a % b)
    k1, k2 = k2, k1
    k2 -= (a // b) * k1
    return d

n = int(input())

m1, a1 = map(int, input().split())
flag = 0
for i in range(n - 1):
    m2, a2 = map(int, input().split())
    k1, k2 = 0, 0
    d = exgcd(m1, m2)
    if (a2 - a1) % d:
        flag = 1
        break
    k1 *= (a2 - a1) // d
    # k1' = k1 + k * (m2 // d) , k取任意整数
    t = m2 // d
    k1 = k1 % t # 取最小的k1
    # x = a + km
    a1 = k1 * m1 + a1
    m1 = m1 // d * m2

if flag:
    print(-1)
else:
    print(a1 % m1) #x的最小正整数解
```