1. (20 points) Let a_1, a_2, a_3, a_4 be arbitrary integers. Find ALL integer solutions of the following equation system.

$$\begin{cases} x \equiv a_1 (\text{mod } 11); \\ x \equiv a_2 (\text{mod } 13); \\ x \equiv a_3 (\text{mod } 17); \\ x \equiv a_4 (\text{mod } 19). \end{cases}$$

$x \equiv a_1 (\text{mod } 11)$ ⇒ there exists an integer u such that $x = 11u + a_1$, in a similar way :

$x \equiv a_2 (\text{mod } 13) \Rightarrow x = 13(11u + a_1) + a_2 = 13 \times 11 u + 13a_1 + a_2$

$x \equiv a_3 (\text{mod } 17) \Rightarrow x = 17(13 \times 11u + 13a_1 + a_2) + a_3$

$= 17 \times 13 \times 11 u + 17 \times 13 a_1 + 17 a_2 + a_3$

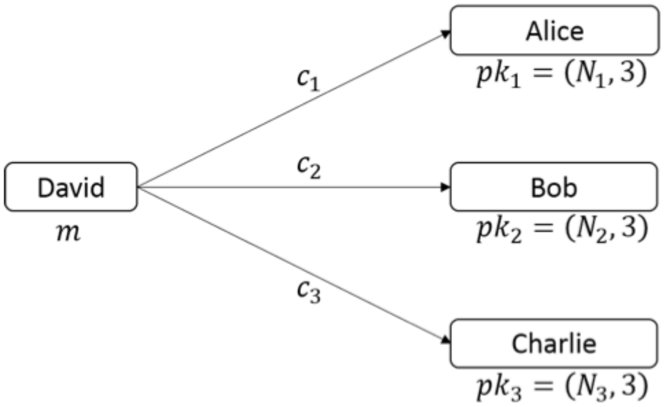
$x \equiv a_4 (\text{mod } 19) \Rightarrow x = 19(17 \times 13 \times 11 u + 17 \times 13 a_1 + 17 a_2 + a_3) + a_4$

$= 19 \times 17 \times 13 \times 11 u + 19 \times 17 \times 13 a_1 + 19 \times 17 a_2 + 19a_3 + a_4$

$= 46189 u + 4199 a_1 + 323 a_2 + 19 a_3 + a_4$

So the solution is $x \equiv 46189 (\text{mod } (4199a_1 + 323a_2 + 19a_3 + a_4))$

2. (20 points) See the following figure. The RSA public keys of Alice, Bob and Charlie are $pk_1 = (N_1, 3), pk_2 = (N_2, 3)$ and $pk_3 = (N_3, 3)$, respectively. David wants to send a private message m to Alice, Bob and Charlie, where m is an integer and $0 < m < N_i$ for $i = 1, 2, 3$. In order to keep m secret from an eavesdropper Eve, David encrypts m as $c_1 = m^3 \bmod N_1$, $c_2 = m^3 \bmod N_2$ and $c_3 = m^3 \bmod N_3$; and then sends c_1 to Alice, c_2 to Bob and c_3 to Charlie.



Suppose that N_1, N_2, N_3 are pairwise relatively prime. Show that with the knowledge of all public keys and all ciphertexts, Eve can decide the value of m.

According to the process of RSA, we have

$c_1 = m^3 \bmod N_1$

$c_2 = m^3 \bmod N_2$

$c_3 = m^3 \bmod N_3$

So we can know that there exist $k_1, k_2, k_3 \in Z$ such that $m^3 = c_1 + k_1 N_1$, $m^3 = c_2 + k_2 N_2$, $m^3 = c_3 + k_3 N_3$.

so from the three equations $c_1 + k_1 N_1 = c_2 + k_2 N_2 = c_3 + k_3 N_3$

we can solve the solution of k_1, k_2, k_3

thus we can know the value of m.

3. (20 points) Let $G = \{x : x \in \mathbb{R}, x > 1\}$. Define $x \star y = xy - x - y + 2$ for all $x, y \in \mathbb{R}$. Show that $(G, \star)$ is an Abelian group.

Closure: $\forall\, x, y \in G$, $x * y = xy - x - y + 2 = (x-1)(y-1) + 1$

since $x, y > 1$, then $(x-1)(y-1)+1 > 1$, so $x * y \in G$

Associative: $\forall\, x, y, z \in G$ $x * (y * z) = x * (yz - y - z + 2)$

$= x(yz - y - z + 2) - x - (yz - y - z + 2) + 2$

$= xyz - xy - xz + 2x - x - yz + y + z - 2 + 2$

$= xyz - xy - xz - yz + x + y + z$

$(x * y) * z = (xy - x - y + 2) * z = (xy - x - y + 2)z - (xy - x - y + 2) - z + 2$

$= xyz - xz - yz + 2z - xy + x + y - 2 - z + 2$

$= xyz - xy - xz - yz + x + y + z$

so $x * (y * z) = (x * y) * z$

Identity: $\exists\, 2 \in G$, $\forall\, a \in G$, $a * 2 = 2a - a - 2 + 2 = a$

$2 * a = 2a - 2 - a + 2 = a$ so $a * 2 = 2 * a = a$

Inverse: $\forall\, a \in G$, $\exists\, 1 \in G$ $a * 1 = a - 1 - a + 2 = 1$

$1 * a = a - 1 - a + 2 = 1$ so $a * 1 = 1 * a = 1$

Commutative: $\forall\, a, b \in G$, $a * b = ab - a - b + 2$

$b * a = ab - b - a + 2$

so $a * b = b * a$

Conclusion: $(G, *)$ is an Abelian group.

4. (20 points) Let $(G, \cdot)$ be a multiplicative (Abelian) group of order m. Show that $o(a)|m$ for any $a \in G$, i.e., the order of any group element must be a divisor of the group's order.

Suppose there is an equivalence relation

$R = \{ <a,b> \mid a,b \in G \text{ and } a^{-1} * b \in H \}$

Equivalence classes are formed by the division of equivalence relation R and group G, Suppose there are k equivalence classes

$\forall a \in G$, $o(a) = o(H)$ H is a subgroup of G.

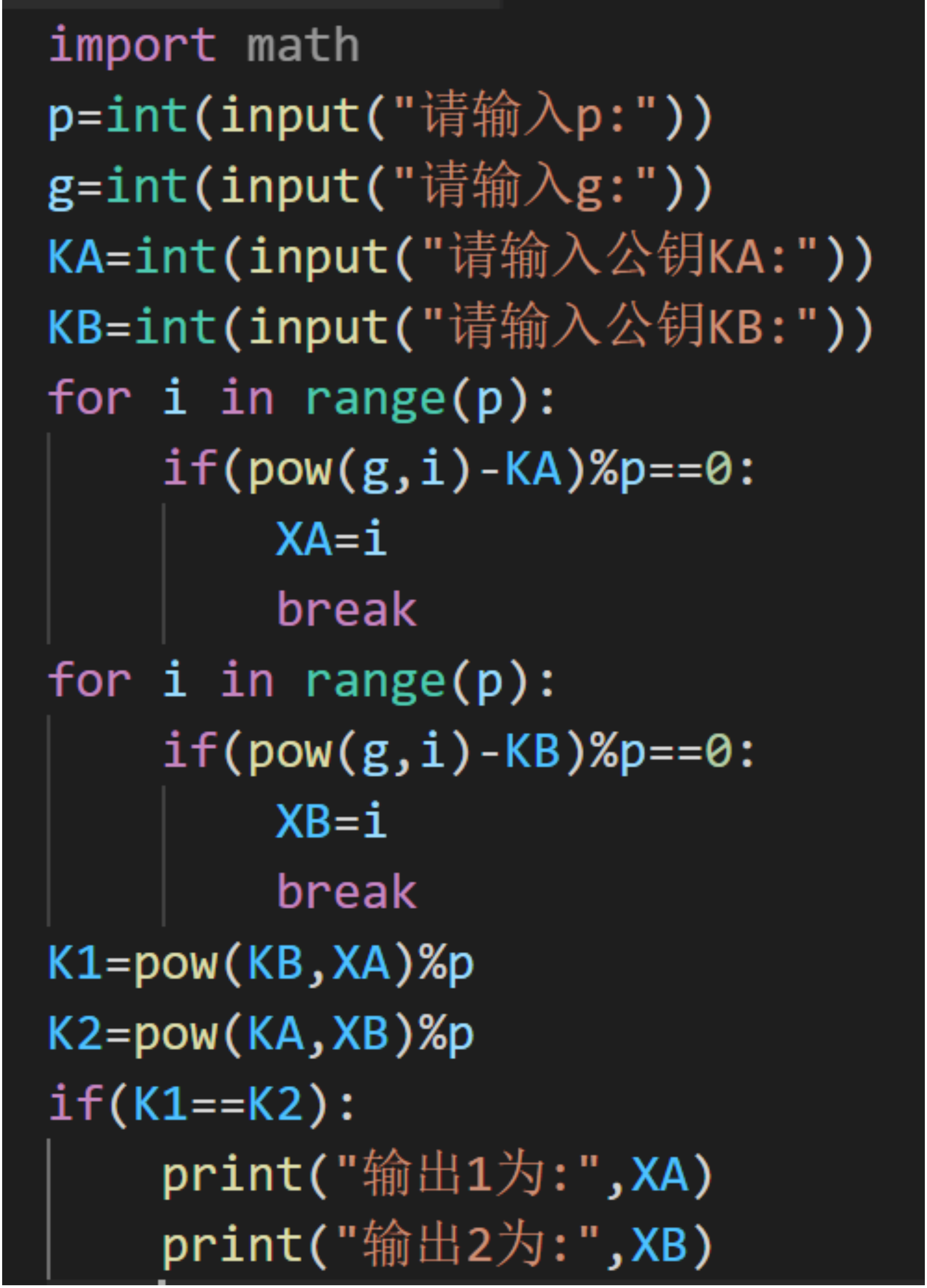
the set of all equivalence elements is G

since the sum of k equivalence classes is m.

then there exists an integer n. such thae $kn = m$

since $n|m$, $o(H) = m$, then for any subgroup S $o(S)|m$.

☆ If the element multiplies itself to form a cyclic subgroup, the order of the element is the order of the corresponding cyclic subgroup, and the cyclic subgroup is the subgroup, so the order of the cyclic subgroup is divisible by the order of the group, and the order of the element is divisible by the order of the group, that is $o(a)|m$.



```python
import math
p=int(input("请输入p:"))
g=int(input("请输入g:"))
KA=int(input("请输入公钥KA:"))
KB=int(input("请输入公钥KB:"))
for i in range(p):
    if(pow(g,i)-KA)%p==0:
        XA=i
        break
for i in range(p):
    if(pow(g,i)-KB)%p==0:
        XB=i
        break
K1=pow(KB,XA)%p
K2=pow(KA,XB)%p
if(K1==K2):
    print("输出1为:",XA)
    print("输出2为:",XB)
```