ĐẠI HỌC BÁCH KHOA – ĐẠI HỌC ĐÀ NẴNG
KHOA CÔNG NGHỆ THÔNG TIN

Môn học

Toán Ứng Dụng
Applied mathematics

Giảng Viên: Phạm Minh Tuấn

Giới thiệu

- Phạm Minh Tuấn
- E-mail: pmtuan@dut.udn.vn
- Tel: 0913230910
- Khoa Công nghệ thông tin –Trường ĐHBK – ĐHĐN

Contents

- Number Theory (Lý thuyết số)
  - Basic Number Theory
  - Primality Tests
  - Totient Function
- Combinatorics (Tổ hợp)
  - Basics of Combinatorics
  - Inclusion-Exclusion
- Geometry (Hình học)
- Game Theory (Lý thuyết trò chơi)

Bài 4.2:

Chinese remainder theorem

Problems

- The **Chinese remainder theorem** solves a group of equations of the form

$$
\begin{aligned}
x &= a_1 \bmod m_1 \\
x &= a_2 \bmod m_2 \\
\ldots \\
x &= a_n \bmod m_n
\end{aligned}
$$

- where all pairs of $m_1, m_2, \ldots, m_n$ are coprime.

- Let x_m^{-1} be the inverse of x modulo m, and

$$X_{m_k} = \frac{m_1 m_2 \cdots m_n}{m_k}$$

- Using this notation, a solution to the equations is

$$x = a_1 X_{m_1} X_{m_1}^{-1} + a_2 X_{m_2} X_{m_2}^{-1} + \cdots a_n X_{m_n} X_{m_n}^{-1}$$

- Once we have found a solution x, we can create an infinite number of other solutions, because all numbers of the form $x + k m_1 m_2 \cdots m_n$ are solutions.

For example, a solution for

- For example, a solution for
  - $x = 3 \bmod 5$
  - $x = 4 \bmod 7$
  - $x = 2 \bmod 3$

is $x = 3.21.1 + 4.15.1 + 2.35.2 = 263$.

Problem 1

- Solve a group of equations
  - x = 4 mod 7
  - x = 7 mod 11
  - x = 6 mod 17
  - x = 15 mod 23
- X = ??

TEST YOUR UNDERSTANDING

- Input
  - The first line of input consists of an integers T where $1 \le T \le 1000$, the number of test cases. Then follow T lines, each containing four integers a, n, b, m satisfying $1 \le n,m \le 10^9$, $0 \le a < n$, $0 \le b < m$. Also, you may assume gcd(n,m)=1.
- Output
  - For each test case, output two integers x, K, where K=nm and $0 \le x < K$, giving the solution x(mod K) to the equations x=a(mod n),x=b(mod m).

Sample Input

```
2
1 2 2 3
151 783 57 278
```

Sample Output

```
5 6
31471 217674
```

Solution ??

```
#include <iostream>
using namespace std;

long long d, x, y;
void extendedEuclid(long long A, long long B) {
    if(B == 0) {
        d = A;
        x = 1;
        y = 0;
    }
    else {
        extendedEuclid(B, A%B);
        long long temp = x;
        x = y;
        y = temp - (A/B)*y;
    }
}
```

```
long long modInverse(long long A, long long M)
{
    extendedEuclid(A,M);
    return (x%M+M)%M
}
int main(){
    int t;
    cin >>t;
    while (t-->0){
        long long a,n,b,m;
        cin >> a >> n >> b >> m;
        long long k = n*m;
        long long x = a * m * modInverse(m,n)
                      + b * n * modInverse (n,m);
        cout << x%k << " " << k << endl;
    }
}
```

Why this solution is not good?

TEST YOUR UNDERSTANDING 2

- Input
  - The first line of input consists of an integers T where $1 \le T \le 1000$, the number of test cases. Then follow T lines, each containing four integers a, n, b, m satisfying $1 \le n,m \le 10^9$, $0 \le a < n$, $0 \le b < m$.
- Output
  - For each test case, output two integers x, K, where K=lcm(n,m) (**least common multiple**) and $0 \le x < K$, giving the solution x(mod K) to the equations x=a(mod n),x=b(mod m).

Sample Input

```
3
10000 23000 9000 23000
10000 23000 10000 23000
1234 2000 746 2002
```

Sample Output

```
no solution
10000 23000
489234 2002000
```

Problems