Homework 4

Computer Programming (II)
Spring Semester, 2021
Time Limit: 1 second

Given two positive integers $a \geq 2$ and $b \geq 2$ satisfying $\gcd(a, b) = 1$, please find $c \in \{0,1,\dots,b-1\}$ such that $(ac \mod b)$ equals 1. That is, we want to find the multiplicative inverse of a modulo b.

Input Format

The first line is the number of test cases. Each test case consists of a and b, separated by a space.

Output Format

For each test case, please output the multiplicative inverse of a modulo b.

Technical Specification

Subtask 1 is as follows:

- There are at most 5 test cases.
- $2 \leq a,\ b \leq 50$.
- $\gcd(a, b) = 1$.

Subtask 2 is as follows:

- There are at most 100000 test cases.
- $2 \leq a,\ b \leq 999999999$.
- $\gcd(a, b) = 1$.

A Fast Algorithm

Suppose that we want to find the multiplicative inverse of 60 modulo 49. Euclid's algorithm checks that $\gcd(60,49) = 1$:

$$\begin{aligned} 60 &= 49 \cdot 1 + 11, \\ 49 &= 11 \cdot 4 + 5, \\ 11 &= 5 \cdot 2 + 1. \end{aligned}$$

The trick is to go through the above equations "backwards":

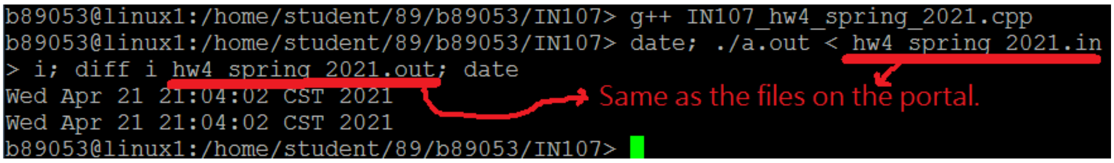
$$\begin{aligned} 1 &= 11 - 5 \cdot 2, \\ &= 11 - (49 - 11 \cdot 4) \cdot 2 \\ &= -49 \cdot 2 + 11 \cdot 9 \\ &= -49 \cdot 2 + (60 - 49 \cdot 1) \cdot 9 \end{aligned}$$

$$= 60 \cdot 9 + 49 \cdot (-11).$$

The answer is 9.

If the above algorithm produces an answer outside of $\{0,1,\dots,b-1\}$, just increment/decrement the answer by a suitable multiple of b so that it lies in $\{0,1,\dots,b-1\}$. In general, the running time is at most polylogarithmic in $a+b$.

My Screenshot



```
b89053@linux1:/home/student/89/b89053/IN107> g++ IN107_hw4_spring_2021.cpp
b89053@linux1:/home/student/89/b89053/IN107> date; ./a.out < hw4_spring_2021.in
> i; diff i hw4_spring_2021.out; date
Wed Apr 21 21:04:02 CST 2021
Wed Apr 21 21:04:02 CST 2021
b89053@linux1:/home/student/89/b89053/IN107>
```

Same as the files on the portal.