中国剩余定理 (crt)

【题目描述】

「物不知数」问题:

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?

即求满足以下条件的整数:除以3余2,除以5余3,除以7余2。该问题最早见于《孙子算经》中,并有该问题的具体解法。宋朝数学家秦九韶于1247年《数书九章》卷一、二《大衍类》对「物不知数」问题做出了完整系统的解答。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。

 $2 \times 70 + 3 \times 21 + 2 \times 15 = 233 = 2 \times 105 + 23$, 故答案为 23。

用现代数学的语言来说明的话,中国剩余定理 (Chinese Remainder Theorem, CRT) 可求解如下形式的一元线性同余方程组(其中 n_1, n_2, \dots, n_k 两两互质):

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \end{cases}$$

$$\vdots$$

$$x \equiv a_k \pmod{n_k}$$

上面的「物不知数」问题就是一元线性同余方程组的一个实例。使用中国剩余定理求解 一元线性同余方程组的步骤如下:

- 1. 计算所有模数的积 n;
- 2. 对于第 *i* 个方程:
 - (a) 计算 $m_i = \frac{n}{n_i}$;
 - (b) 计算 m_i 在模 n_i 意义下的逆元 m_i^{-1} ;
 - (c) 计算 $c_i = m_i m_i^{-1}$ (不要对 n_i 取模)。
- 3. 方程组在模 n 意义下的唯一解为: $x = \sum_{i=1}^k a_i c_i \pmod{n}$.

中国剩余定理的一个应用是,如果要计算 $a \mod n$,其中 $n = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$,那么可以先计算 $a_i = a \mod p_i^{c_i}$,然后使用中国剩余定理求解出 $a \mod n$ 的值,这样就可以在 n 是一个比较大的合数的时候减小乘法运算的规模。

Alice 想要计算两个数字 a, b 的乘积对某个整数 n 取模的结果。在学习了中国剩余定理后,她决定采用上述的方法,先对 n 进行质因数分解,然后计算答案对每个质因数取

模的结果,最后使用中国剩余定理求解出答案。但是很悲惨的是,在计算过程中,对于其中一个质因数的运算过程出现了错误,导致最终的结果也是错误的。虽然经过重新计算 她得出了正确的结果,但是她还是想知道她之前的计算过程中在哪个质因数上出错了。

【输入格式】

从文件 crt.in 中读入数据。输入的第一行包含一个整数 T,表示数据组数。

接下来 T 行,每行包含四个整数 a,b,m,n,分别表示要计算乘积的两个数,Alice 计算出的错误结果,以及模数。

【输出格式】

输出到文件 crt.in 中。输出到文件 crt.out 中。输出 T 行,每行一个整数,表示 Alice 在哪个质因数上出错了。

【样例输入】

1 1

2 3 1 10

【样例输出】

. 2

【样例解释】

将 10 质因数分解,得到 $10 = 2 \times 5$ 。接下来检查这两个质因数: $(2 \times 3) \mod 2 = 0 \neq 1$, $(2 \times 3) \mod 5 = 1$ 。因此,Alice 在 2 这个质因数上出错了。

【数据范围】

对于所有测试数据,保证: $1 \le T \le 1000$, $1 \le a, b, m, n \le 10^{18}$ 。每个测试点的具体限制见下表:

测试点编号	$T \leq$	$a, b, m, n \le$	特殊限制
$\boxed{1 \sim 2}$	1000	10^{6}	
$3 \sim 4$	1000	10^{18}	n 的所有质因数都 ≤ 100
$\boxed{5 \sim 6}$	1	10^{18}	
$7 \sim 10$	1000	10^{18}	