

/\*\*\*\*\*\*一般模线性方程组\*\*\*\*\*\*/

同样是求这个东西。。

$$X \bmod m_1 = r_1$$

$$X \bmod m_2 = r_2$$

...

...

...

$$X \bmod m_n = r_n$$

首先，我们看两个式子的情况

$$X \bmod m_1 = r_1 \dots\dots\dots (1)$$

$$X \bmod m_2 = r_2 \dots\dots\dots (2)$$

则有

$$X = m_1 * k_1 + r_1 \dots\dots\dots (*)$$

$$X = m_2 * k_2 + r_2$$

$$\text{那么 } m_1 * k_1 + r_1 = m_2 * k_2 + r_2$$

整理，得

$$m_1 * k_1 - m_2 * k_2 = r_2 - r_1$$

令  $(a, b, x, y, m) = (m_1, m_2, k_1, k_2, r_2 - r_1)$ ，原式变成

$$ax + by = m$$

熟悉吧？

此时，因为  $\text{GCD}(a, b) = 1$  不一定成立， $\text{GCD}(a, b) \mid m$  也就不一定成立。所以应该先判 若  $\text{GCD}(a, b) \mid m$  不成立，则!!! 方程无解!!!。

否则，继续往下。

解出  $(x, y)$ ，将  $k_1 = x$  反代回  $(*)$ ，得到  $X$ 。

于是  $X$  就是这两个方程的一个特解，通解就是  $X' = X + k * \text{LCM}(m_1, m_2)$

这个式子再一变形，得  $X' \bmod \text{LCM}(m_1, m_2) = X$

这个方程一出来，说明我们实现了  $(1)(2)$  两个方程的合并。

令  $M = \text{LCM}(m_1, m_2)$ ， $R = r_2 - r_1$

就可将合并后的方程记为  $X \bmod M = R$ 。

然后，扩展到  $n$  个方程。

用合并后的方程再来和其他的方程按这样的方式进行合并，最后就能只剩下一个方程  $X \bmod M = R$ ，其中  $M = \text{LCM}(m_1, m_2, \dots, m_n)$ 。

那么， $X$  便是原模线性方程组的一个特解，通解为  $X' = X + k * M$ 。

如果，要得到  $X$  的最小正整数解，就还是原来那个方法：

$$X \% = M;$$

$$\text{if } (X < 0) \ X += M;$$

这么一来~~大功告成~~