关于模数互质的中国剩余定理（crt）

这玩意我上课口胡的时候忘了，非常抱歉，这里补上。

再写一遍，我们要求解一个 x，满足 n 个形如 `x%m==r` 的方程。

拿数学式子写就是：

$$\begin{cases} x \equiv r_1 \pmod{m_1} \\ x \equiv r_2 \pmod{m_2} \\ \dots \\ x \equiv r_n \pmod{m_n} \end{cases}$$

其中，所以的 m 两两互质。

接着讲我上课没讲完的思路，核心就一句话：

在满足某一个方程的情况下，加上某些数不影响其它方程

考虑第 i 个方程举例。要保证 $x \equiv r_i \pmod{m_i}$，那肯定要先加一个模 m_i 同余于 r_i 的项，然后再加上一堆 m_i 的倍数（加倍数不影响余数，问题不大）

然后我们加的这一个同余于 r_i 的项，**不能影响**其它方程——要不然就不好考虑了。

注意到 m 两两互质。

于是，我们设 $l(i)$ 表示：n 个模数中，除去 m_i 之外所有模数的 lcm 。

> 举个例子，$n=5$，$l(3)=\operatorname{lcm}(m_1,m_2,m_4,m_5)$

于是我们可以加上一个 $k \times l(i)$ 使得它模 m_i 同余于 r_i，并且，它在其它方程中没有任何的影响（显然，因为这个 $l(i)$ 对于其它的模数，都同余于 0）

那这个 k 咋求呢...类似于解方程，把 $l(i)$ 移到右边，得到 $k \equiv l(i)^{-1} r_i \pmod{m_i}$，其中 $l(i)^{-1}$ 就是 $l(i)$ 模 m_i 的逆元。

那么，$l(i)^{-1} \times r_i \times l(i)$ 就是：**满足第i个方程并且对其它方程没有任何影响** 的一项

要满足所有方程怎么办？全部加起来即可

即，$x \equiv \sum_{i=1}^{n} l(i)^{-1} \times r_i \times l(i) \pmod{LCM}$

其中 $LCM=$ 所有模数的 lcm。

> Q：为啥 $l(i)^{-1}$ 不和 $l(i)$ 合并成 1？ A：$l(i)^{-1}$ 是模 m_i 意义的，而 x 是模 LCM 意义的，模数不一样，不能合并

> Q：你不是讲了模数不互质咋做了吗，这玩意有啥用？
>
> A：短，好写
>
> Q：那模数两两互质，又没说是质数，求逆元不是还要 $exgcd$？
>
> A：就算都需要 $exgcd$，这个基础的 crt 也比每次合并的 $excrt$ 短很多