数学 05

- 同余下的加减乘除
- 同余方程
- 中国剩余定理
- 扩展中国剩余定理（选讲）
- 题目选讲

说在前面

本讲数学推导极多，课后作业是模板题，只要看懂前面的内容就能做，选做作业有一定难度，学有余力的同学可以尝试

同余下的加减乘除

先一起回顾一下同余下的加减乘除，我们特别注意减法和除法

同余下的加法

$$(a+b)\%m=(a\%m+b\%m)\%m$$

同余下的减法，算法竞赛不考虑负数，所以要把负数变正

$$(a-b)\%m=(a\%m-b\%m+m)\%m$$

同余下的乘法

$$(a \times b)\%m = (a\%m \times b\%m)\%m$$

同余下的除法，乘以乘法逆元

$$\frac{a}{b}\%m = (a\%m \times b^{-1}\%m)\%m$$

乘法逆元可以使用扩欧或者快速幂求解，当然，后者只适用于模数 m 为素数的情况

同余方程

一次同余方程形如

$$ax \equiv b \ (mod \ m)$$

设方程的一个特解为 x_0，那么方程的通解即为

$$x \equiv x_0 \ (mod \ m)$$

若最大公因数 $(a, \ m) = 1$，则 $x_0 \equiv b \cdot a^{-1} \ (mod \ m)$，若 $(a, \ m) \neq 1$，方程无解

中国剩余定理

给定线性同余方程组

$$\begin{cases} x_1 \equiv a_1 \ (mod\ m_1) \\ x_2 \equiv a_2 \ (mod\ m_2) \\ \qquad\quad \cdots \\ x_n \equiv a_n \ (mod\ m_n) \end{cases}$$

保证 m_1，m_2，$\ldots$ m_n 两两互质

中国剩余定理可以计算上述方程组的通解

初探解的情况

设 $m = \prod_{i=1}^{n} m_i$，以及 $M_i = \frac{m}{m_i}$，$i = 1,\ 2,\ \ldots,\ n$

则上述同余方程组的通解为

$$x \equiv \sum_{i=1}^{n} a_i \cdot M_i^{-1} \cdot M_i \ (mod\ m)$$

推导解

考虑对于每一个线性同余方程

$$x_i \equiv a_i \ (mod \ m_i)$$

求出对应的一个特解 x_i ，且这个 x_i 要满足

$$\begin{cases} x_i \equiv a_j \ (mod \ m_j), \ i = j \\ x_i \equiv 0 \ (mod \ m_j), \ i \neq j \end{cases}$$

把 n 个这样的 x_i 求和，就可以得到方程组的一个特解 x

设

$$m = \prod_{i=1}^{n} m_i$$

以及

$$M_i = \frac{m}{m_i},\ i = 1,\ 2,\ \ldots,\ n$$

分析 x_i，其必然是 M_i 的整数倍，且满足

$$x_i \equiv a_i\ (mod\ m_i)$$

设

$$x_i = y \cdot M_i,\ y \in \mathbb{Z}$$

有

$$y \cdot M_i \equiv a_i\ (mod\ m_i)$$

只要能够解出 y，便能得到 x 的特解；反之，线性同余方程组无解

因为 $(M_i,\ m_i) = 1$，因此上述方程一定有解

由于不保证 m_i 是素数，所以根据扩欧算法得到乘法逆元

$$y \equiv a_i \cdot M_i^{-1} \ (mod \ m_i)$$

所以

$$x_i = a_i \cdot M_i^{-1} \ (mod \ m_i) \cdot M_i$$

将 n 个 x_i 求和得到 x 的一个特解

$$x = \sum_{i=1}^{n} a_i \cdot M_i^{-1} \ (mod \ m_i) \cdot M_i$$

为了满足题意， x 的通解为

$$x \equiv \sum_{i=1}^{n} a_i \cdot M_i^{-1} \ (mod \ m_i) \cdot M_i \ (mod \ m)$$

代码见 notes.md

扩展中国剩余定理（选讲）

给定线性同余方程组

$$\begin{cases} x_1 \equiv a_1 \ (mod\ m_1) \\ x_2 \equiv a_2 \ (mod\ m_2) \\ \quad\quad \cdots \\ x_n \equiv a_n \ (mod\ m_n) \end{cases}$$

$m_1, m_2, \ldots m_n$ 不一定两两互质

扩展中国剩余定理是为了处理模数不互质的情况

设

$$m = [m_1 m_2 ... m_n]$$

则上述方程组通解为

$$x = x_0 + q \cdot \frac{m_i}{gcd(m, m_i)},\ q \in Z$$

其中 x_0 是同余方程组的一个特解，通过 $n-1$ 次扩欧算法计算得出

精妙的思考

考虑已经解出前 $k-1$ 个方程的解 x_1

习惯的，我们设

$$m = \prod_{i=1}^{k-1} m_i$$

但为了防止溢出，设

$$m = [m_1,\ m_2, .. ,\ m_{k-1}]$$

设前 $k-1$ 个方程的通解为

$$x \equiv x_1 \ (mod\ m)$$

再设 $x_2 = x_1 + t \cdot m,\ t \in \mathbb{Z}$

将 x_2 代入第 k 个式子

$$x_1 + t \cdot m \equiv a_k \ (mod\ m_k)$$

即

$$t \cdot m \equiv a_k - x_1 \ (mod\ m_k)$$

若

$$(m,\ m_k) \nmid a_k - x_1$$

则线性同余方程组无解

若

$$(m,\ m_k) \mid a_k - x_1$$

由扩欧算法解出 t，得到特解 x_2，那么新的通解为

$$x \equiv x_2\ (mod\ m_k)$$

如此循环即可

$excrt$ 的本质便是合并方程

对于 n 个方程的线性同余方程组，本质上是作 $n-1$ 次扩展欧几里得算法

解释具体求法

处理到第 k 个方程时，具体求 x_2 的过程如下

因为

$$x_2 = x_1 + t \cdot m$$

其中

$$m = [m_1 m_2 ... m_{k-1}]$$

所以即在方程中求 t

$$t \cdot m \equiv a_k - x_1 \ (mod \ m_k)$$

先用扩欧求方程

$$t \cdot m + q \cdot m_k = (m, \ m_k)$$

的特解 t_0，然后自乘系数

$$\frac{a_k - x_1}{(m, \ m_k)}$$

进而得到通解

$$t = t_0 \cdot \frac{a_k - x_1}{(m,\ m_k)} + q \cdot \frac{m_k}{(m,\ m_k)},\ q \in \mathbb{Z}$$

为了防止溢出，将 t 取模数 $\frac{m_k}{(m,\ m_k)}$ 至最小非负数

于是得到

$$x_2 = x_1 + t \cdot m$$

代码见 notes.md

2587. 同余方程

给定正整数 a，b，m，计算同余方程 $ax \equiv b \ (mod \ m)$ 的最小正整数解

输入保证

对于 40% 数据，$2 \leq a, \ b \leq m \leq 1,000$

对于 60% 数据，$2 \leq a, \ b \leq m \leq 10,000,000$

对于 100% 数据，$2 \leq a, \ b \leq m \leq 1,000,000,000$

利用扩欧计算 $a^{-1}\ (mod\ m)$，然后计算 $b \cdot a^{-1}\ (mod\ m)$ 即可

2545. 中国剩余定理

给定正整数 n，以及 n 个 a_i，m_i，保证 m_i 互质，计算如下方程组的最小正整数解

$$\begin{cases} x_1 \equiv a_1 \ (mod\ m_1) \\ x_2 \equiv a_2 \ (mod\ m_2) \\ \quad\quad\quad\quad ... \\ x_n \equiv a_n \ (mod\ m_n) \end{cases}$$

保证 $2 \leq n \leq 10,\ 0 \leq a_i < m_i \leq 10^2,\ 1 \leq \prod a_i \leq 10^{18}$，保证 m_i 互质，保证 a_i 不全为 0

CRT 模板题

2553. 扩展中国剩余定理（选做）

给定正整数 n，以及 n 个 a_i，m_i，不保证 m_i 互质，计算如下方程组的最小正整数解

$$\begin{cases} x_1 \equiv a_1 \ (mod\ m_1) \\ x_2 \equiv a_2 \ (mod\ m_2) \\ \quad\quad\quad\quad \dots \\ x_n \equiv a_n \ (mod\ m_n) \end{cases}$$

保证 $2 \leq n \leq 10^5$，$1 \leq a_i < m_i \leq 10^{12}$，保证所有 m_i 的最小公倍数不超过 10^{18}，不保证 m_i 互质

$EXCRT$ 模板题，注意数据较大，可能爆 `long long int`，使用快速乘防止溢出

2545. 构造函数（选做）

给定质数 p，整数 n 和 n 个互不相同整数 a_i，以及整数 k

计算整数对 $(i,\ j)(1 \leq i < j \leq n)$ 的数量，使得 $(a_i + a_j)(a_i^2 + a_j^2) \equiv k\ (mod\ p)$

输入保证，$2 \leq n \leq 3 \cdot 10^5,\ 2 \leq p \leq 10^9,\ 0 \leq k \leq p-1, 0 \leq a_i \leq p-1$

难点在于对式子的变形，具体有

$$(a_i - a_j)(a_i + a_j)(a_i^2 + a_j^2) \equiv k(a_i - a_j)\ (mod\ p)$$

即

$$a_i^4 - ka_i \equiv a_j^4 - ka_j\ (mod\ p)$$

下面只需要对每一个 a_i 计算 $a_i^4 - ka_i\ (mod\ p)$，用哈希表 `unordered_map<int, int> mp` 维护，统计答案，时间复杂度 $O(n)$