> 本文主要记录隐私计算中涉及的群、环、有限域的最基本的概念以及一些常用的数论定理，**仅供参考**。

一、群

1. 群的定义

群本质是一个集合G，这个集合上定义了一个运算 $\cdot$（例如加法或乘法），满足下面的性质：

1. **封闭性**：$\forall a,b\in G$，满足 $a\cdot b\in G$；
2. **结合律**：$\forall a,b,c\in G$，满足 $(a\cdot b)\cdot c=a\cdot(b\cdot c)$；
3. **存在单位元**：$\exists e\in G$，使得 $\forall a\in G$，满足 $a\cdot e=e\cdot a=a$；
4. **存在逆元**：$\forall a\in G$，$\exists a^{-1}\in G$，使得 $a\cdot a^{-1}=a^{-1}\cdot a=e$ 。

一个群的**阶**为群中的元素个数，例如群 $G=\{1,2,3\}$的阶 $|G|=3$。

在上述性质的基础上，若运算满足交换律则称为**阿贝尔群**；

若群中的所有元素均可以由一个元素和自己反复运算得到，则称为**循环群**，这个元素叫作**生成元**。

事实上，在隐私计算或密码学中通常使用的都是循环群，因此主要记录一下循环群和其相关的知识。

2. 循环群

在一个群 G 中，对于元素 $g\in G$，记 $g^1=g$、$g^2=g\cdot g$、$g^3=g\cdot g\cdot g$、$\cdots$ 以此类推。

若 G 中所有元素均可由 g 反复与自己运算得到，即 $G=\{g^n|n=1,2,\cdots\}$，则称 G 为一个循环群，g 为该群的一个生成元（**生成元不一定唯一**），可记作 $G=\langle g\rangle$。

密码学中经常使用模素数乘法群，设 p 为一个素数，$\mathbb{Z}_p^*=\{1,2,\cdots,p-1\}$ 为一个循环群，该群上定义的运算为 **模 p 乘法**。

模素数乘法群一定是一个循环群，感兴趣的可以自行搜索证明。

循环群例子：模7乘法群 $\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$ 中 3 是一个生成元，因为在模7乘法意义下：

$$\{3^1, 3^2, 3^3, 3^4, 3^5, 3^6\} = \{3,2,6,4,5,1\} = \mathbb{Z}_7^*$$

这里引入**元素的阶**的定义：元素 $a \in G$ 的阶是指**最小的正整数** n，使得 $a^n = e$，其中 e 是单位元。

显然上述例子中单位元 $e = 1$，元素 3 的阶为 6。

我们可以知道，循环群中**生成元的阶一定等于该群的阶**（即元素个数），因为生成元可以生成群中的所有元素，而单位元一定是最后生成的（生成单位元后再和自己运算会进入一个新的循环）。

二、环和有限域

这里不给出详细定义，只进行简单的介绍以区分这些概念。

1. 环

环是一个集合，上面定义两个运算$+$和$\times$，可理解为通常的加法和乘法运算。

这个集合和加法运算可以组成一个**加法群**（拥有群的性质），这个群必须是阿贝尔群（**加法满足可交换性**）。

在乘法上应当满足**封闭性**和**结合性**，以及对加法的分配律，但不要求可交换性、不要求存在单位元和逆元。

可以简单理解为环是一个可交换的加法群上再**新定义一个乘法运算**。

2. 有限域

有限域可以简单理解为在环的基础上，该集合内除了零元素外的所有元素都有**乘法逆元**。

环和有限域的主要区别就在于：环不要求元素有乘法逆元，但在有限域上有要求。

三、常用定理

这里主要介绍在隐私计算和密码学相关的算法和证明中会用到的一些基本定理。

1. 费马小定理

> **费马小定理**：若 p 为一个素数，设 a 和 p 互质，即 $gcd(a,p)=1$，则 $a^{p-1}\equiv 1(mod\ p)$。

常用于求模素数意义下的逆元：$a^{-1}\equiv a^{p-2}(mod\ p)$。

2. 欧拉定理

在介绍欧拉定理前首先介绍**欧拉函数**：

欧拉函数 $\varphi(n)$ 代表小于等于 n 的正整数中和 n 互质的**数的个数**。

当 n 为素数的时候，$\varphi(n)=n-1$。

> **欧拉定理**：若 $gcd(a,n)=1$，则 $a^{\varphi(n)}\equiv 1(mod\ n)$。

显然欧拉定理可以理解为费马小定理的扩展，当 n 为素数时，欧拉定理就等同于费马小定理。

欧拉定理会用于很多密码学场景之中，例如RSA加密算法。

3. 中国剩余定理（CRT）

中国剩余定理用于如下形式的线性同余方程：

$$\begin{cases} x\equiv a_1(mod\ n_1) \\ x\equiv a_2(mod\ n_2) \\ x\equiv a_3(mod\ n_3) \\ \quad \cdots \\ x\equiv a_k(mod\ n_k) \end{cases}$$

求唯一解：

$$x \equiv \ ?\ (mod\ n)$$

其中，$n_1, n_2, \cdots, n_k$ 两两互质，$n = n_1 \times n_2 \times \cdots \times n_k$。

该定理首先构造出满足这 k 个方程的一个解，并证明解的唯一性。

解的构造思路非常清楚：每个方程在保证自己成立的基础上给出一个部分解，同时保证这个部分解不会影响其他方程的成立。即：设第 i 个方程的部分解为 x_i，该部分解应当满足以下两点要求：

1. $x_i \equiv a_i\ (mod\ n_i)$
2. 当 $j \neq i$ 时，$x_i \equiv 0\ (mod\ n_j)$

则最终方程的解 $x = \sum_{i=1}^{k} x_i$ 一定满足全部同余方程。

中国剩余定理给出的**部分解构造公式**为：

$$x_i = a_i \cdot \frac{n}{n_i} \cdot (\frac{n}{n_i})^{-1}$$

其中，$(\frac{n}{n_i})^{-1}$为 $\frac{n}{n_i}$ 在**模 n_i意义**下的逆元。**注意不是模 n 意义下的逆元**!

分析如下：

以第一个方程为例，考虑到部分解的第二个要求等价于 $n_2, n_3, \cdots, n_k$ 均能整除 x_1，即 $lcm(n_2, n_3, \cdots, n_k)$ 能整除 x_1。因为 $n_2, n_3, \cdots, n_k$ 两两互质，因此：

$$lcm(n_2, n_3, \cdots, n_k) = n_2 \times n_3 \times \cdots \times n_k = \frac{n}{n_1}$$

即第二个要求等价于 $\frac{n}{n_1}$ 能够整除 x_1。不妨设 $x_1 = a_1 \cdot \frac{n}{n_1}$，由于第一个要求需要 $x_1 \equiv a_1\ (mod\ n_1)$，因此在部分解 x_1 中，乘在 a_1 上的系数在模 n_1 意义下要等于 1, 因此我们需要再乘上一个 $\frac{n}{n_1}$ 在模 n_1意义下的逆元 $(\frac{n}{n_1})^{-1}$，即 $x_1 = a_1 \cdot \frac{n}{n_1} \cdot (\frac{n}{n_1})^{-1}$。

其他方程同理。

因此 $x = \sum_{i=1}^{k} x_i$ 是满足这些同余方程的一个解，且**在模 n 意义下，该解唯一**。唯一性的证明如下：

对于任意满足这 k 个方程的两个解 x, y，将两组同余方程对应作减法可以得到：

$$\begin{cases} x-y \equiv 0 (mod\, n_1) \\ x-y \equiv 0 (mod\, n_2) \\ x-y \equiv 0 (mod\, n_3) \\ \quad\quad \cdots \\ x-y \equiv 0 (mod\, n_k) \end{cases}$$

即 $n_1, n_2, \cdots, n_k$ 均整除 $x-y$，考虑到他们两两互质，我们可以得到 n 整除 $x-y$，即 $x-y \equiv 0\ (mod\, n)$，即 $x \equiv y\ (mod\, n)$，因此解在模 n 意义下唯一。

本文为作者在学习相关知识时的一种记录，便于以后的回顾。作者并没有系统地学习过密码学，因此在表述上可能会存在不严谨甚至出错的地方，文章仅供参考，欢迎大家与我交流，一起进步！

其他平台：

- 知乎（Totoro）：https://www.zhihu.com/people/totoro-14-60
- CSDN（_Totoro_）：https://blog.csdn.net/orz_Totoro
- B站（Totoro_134）：https://space.bilibili.com/279377771
- Github（Totoro134）：https://github.com/Totoro134
- 公众号（知识长生所）