# 密码学

# 数学基础

## 数学常识

几个数学定义

首先要讲的，是关于群、环、域的概念，这是离散数学当中的概念，比较难懂，而其实密码学中对这些概念并没有多少涉及，都是为了引出“有限域”这个概念，所以，我们先说有限域，在说“群、环、域”，如果不想理解“群、环、域”的概念，亦可。

有限域：顾名思义，即范围是有限个的“域”（域的概念稍后解释），它有一个特点，有限域的大小是一个素数的若干次方。举例来说，比如10以内的非负整数，就是一个有限域。一般描述有限域，通过对整数取模（mod）的余数来表示，比如所有整数模5的结果，就是一个有限域（只包含0~4），这是5这个素数的1次方。

幺元：如果对于一个二元运算+（注意+并不是指一般意义的加法，它可以指代任何二元运算），在有若干个数的集合中，有一个数，对于其他任何数，通过这个二元运算之后，结果都是其他任何数本身，则称这个数是这个集合对于运算+的幺元。以加法为例，0就是在整数这个集合中，关于加法的幺元。

零元：和幺元类似，不同处在于 是 有一个数，对于其他任何数，通过这个二元运算之后，结果都是这个数本身，则这个数是这个集合对于这个二元运算的零元。以乘法为例，0就是零元。

逆元：有一个二元运算+（注意+并不是指一般意义的加法，它可以指代任何二元运算），如果a+a’=这个运算的幺元，那么，a与a’互为逆元。以加法为例，整数这个集合中，一个数和它的相反数互为逆元。

群：群表示一种关系，定义一个集合s和一个操作+，注意+并不是指一般意义的加法，它可以指代任何二元运算，如果这个集合中的元素，关于这个运算，满足结合律，每一个元素有逆元，整个集合有关于这个运算的幺元，则称，这个关系s,+是一个群。以加法为例，加法在整数这个集合上是一个群。

环:如果有两个二元运算+,\*(注意+,\*并不是指一般意义的加法,乘法，它可以指代任何二元运算)，在一个集合上，一个二元运算满足可结合、可交换、有幺元，元素都有逆元，另一个二元运算满足可结合，则这个关系s,+，\*是一个环

整环：在环的定义中，只需满足了可结合的那个运算\*（不一定是真正意义的乘法），如果还满足了可交换、有幺元，对于a\*b=0一定能推出a=0或b=0，则这个环是整环。

域：如果一个整环，集合中有至少两个元素，且都有逆元，则是域

伽罗华域：首先，这是一个有限域，其次，这个有限域是2的若干次方。密码学里常用的是2^8

再看有限域，以模5为例，0~4的计算结果也要模5，对于普通加法和乘法，可以证明（我其实不会证），这个关系<0~4,+,\*>是一个域，且元素个数有限，所以是有限域。

## 数学定理

下面要介绍的数学定理，都很重要，不过也很简单。

欧几里德算法以及扩展欧几里德算法 ：

就是以前学过的辗转相除法，简而言之，a和b（a>b）的最大公约数，就是a模b的结果，和b求得的最大公约数（即gcd(a,b)=gcd(a mod b,b)），这个过程一直递归下去，直到a或b等于0，则非零的另一个数就是最大公约数。

而扩展欧几里德算法，则是说如果，对a，b以及二者的最大公约数，有ax+by=gcd(a,b)，这里x，y可能有若干对。扩展欧几里德算法常用来求解多项式的逆元，这个我们之后会提到。

欧拉定理

设一个函数f（欧拉函数），f(n)的结果为比n小的，与n互质的数的个数，则对任意一个整数a，若gcd(a,n)=1，有a^f(n) mod n=1.

证明：

设集合X={x1,x2,.......,xf(n)},为与n互质，比n小的数的集合，共f(n)个

而X'={a\*x1 mod n,a\*x2 mod n,........, a\*xf(n) mod n} 共f(n)个

因为gcd(a,n)==1,

所以a\*x 与n互质，

又因为X'元素都比n小

所以X=X'

所以集合X中元素的乘积模n 结果等于 X'中元素的乘积模n

提取出a的f(n)次方，两边消去X中元素的乘积

得出a^f(n) mod n=1123456789

欧拉定理有一个很有用的用处是求逆元，a\*a^(f(n)-1) mod n=1，可以改写为a\*b mod n=1,所以a在模n的有限域的乘法逆元b就等于 a^(f(n)-1) mod n

费马小定理

对于一个素数p，有a^(p-1) mod p=1

费马小定理是欧拉定理的一个特例，证明不再重复

中国剩余定理

有方程组:

求X的值

解法:

其中，M为若干个mi的乘积，ti为M/mi在有限域mi上的乘法逆元

所以，这个问题就分解成了求若干个乘法逆元、求积、求和的问题，而最难的求乘法逆元的方法，就是上面提到的欧拉定理

单变量线性同余

有ax=b mod n，求x

解：

求出gcd(a,n)=d,若d可被b整除，则有d个解，否则无解

另a'=a/d,b'=b/d,n'=n/d

x'=(a')^-1 \* b' mod n'(这里(a')^-1 表示a' 在模n'的有限域内的乘法逆元)

x0=x',xt=x0+n/d \*t (mod n) t取值从0到d-1

————————————————

版权声明：本文为CSDN博主「lqadam」的原创文章，遵循CC 4.0 BY-SA版权协议，转载请附上原文出处链接及本声明。

原文链接：https://blog.csdn.net/lqadam/java/article/details/73744061