整数集Z{0，0，1，2，……}在加法运算下是封闭的，整数加法运算是可交换的，整数加法运算是可结合的，整数加法运算的单位元是0，整数加法运算的逆运算是减法。

群是指由一个集合G和一个二元运算\*构成的代数系，且对于二元运算\*是封闭的，可结合的，拥有单位元e并且每个元素都有对应的逆元。

整数集合Z是一个加法运算上的群。

有限群是指元素数目有限的群。有限群G的元素个数称为有限群G的阶，如果G的某个子集在运算\*下也是一个群，则称为G的子群。

对于有限群G中的任意元素，的方幂运算定义，的方幂集合是重复的，第一个重复的元素是，重复出现前的元素是单位元e，不同的方幂组成的集合成为的轨道，轨道中元素个数称为元素的阶，的轨道也是G的一个子群。

定理2.1.1 拉格朗日

有限群中任意元素的阶必定整除改有限群的阶

定义为0到n-1的整数集合且中的加法和乘法是模n约简的，在加法运算下是有限群，在乘法运算下不是有限群。

中在乘法运算下有逆元的元素的集合为，中元素和n没有公因子，中所有元素都有一个逆元，单位元为元素1，是乘法运算下的一个群。

素数/质数/合数，如果除了1没有其他整数可以同时整除a和b，则a和b是互素的。

GCD(r,s)表示为两个整数r和s的最大公约数，即可同时整除r和s的最大正整数，如果r和s的最大公约数是1，则r和s互素。

是中满足GCD(a,n)=1的元素集合。

LCM(r,s)表示为两个整数r和s的最小公倍数，即可同时被r和s整除的最小整数。

定义2.1.2 欧拉函数

欧拉函数是小于等于n且与n互素的正整数的个数

=#

如果n为素数，则=n-1

对于任意的，总存在整数A和N满足A+Nn=1，因此A=1 mod n，A mod n即为中的逆元，中每个元素都存在逆元且，是乘法运算下的一个群。

定理2.1.3

对于素数p和q，=p-1，=q-1，=(p-1)(q-1)，=(p-1)

定理2.1.5 欧拉定理

若是的一个元素，则有=1 mod n

推论2.1.6 费马小定理

若p为素数且，则= mod p

一个素数n有+=n

一个双素数n=pq，其中p和q为素数，有+++=n

定理2.1.7

欧拉函数满足=n，其中∑的下标是d的整除集合，包括n和1

定理2.1.8

若n是一个素数，则包含一个在乘法运算下阶为=n-1的元素，因此在乘法运算下是一个循环群

对于任意两个非负整数a和b，存在两个非负整数Q和r，称为商和余数：a=Qb+r，如果r等于0，则称b整除a，记为b|a。

定理2.2.1 欧几里得算法

给定两个不同的整数r和s，且s大于r，他们的最大公约数可以通过迭代法得到：

s=r+

r=+

=+

……

=

余数为0时终止，最后一个非零的余数就是两个数的最大公约数。

推论2.2.2 扩展的欧几里得算法

对于任意整数r和s，存在整数R和S满足GCD(r,s)=Rr+Ss

推论2.2.3 若整数r和s互素，那么存在整数R和S满足Rr+Ss=1

推论2.2.4 集合在乘法运算下是一个群

定理2.2.5 中国剩余定理

双素数密码

为环，其中n=pq是两个不相等的大素数乘积，整数n公开，素数p和q是保密的，n是两个素数乘积，关于n的欧拉公式为，很容易通过p和q计算得到，但是通过n却不容易得到。随机选取加密指数b，，通过欧几里得算法可以验证GCD(b,)=1，如果GCD(b,)不等于1，重新选择b，然后使用扩展的欧几里得算法计算，因为b和互素，所以整数确实存在，加密密钥b是公开的，n也是公开的，解密密钥a是保密的，且不能由b和n计算得到。

加密过程：对于任意的，y=(mod n)

解密过程：对于，x=(mod n)，其中

n=pq，两个不相等的大素数乘积，，逆元为b，则对于任意，有=x mod n

DH密钥交换

用户A和B协商一个适当大小的有限群G和一个元素，用户A随机选取一个整数a并保密，用户B随机选取一个整数b并保密，用户A计算，并发送到B，B计算，用户B计算，并发送到A，A计算，A和B完成密钥的交换

Elgamal密码

G是循环群，是G的生成元，解密者秘密随机选取一个整数a，计算加密密钥，对于任意的消息，加密者秘密的选取一个整数b，计算和为加密消息。

解密计算为，得到x

群

群G是满足以下四大标准性质的任意集合：

1. 包含一个二元运算符\*，由集合中成对元素来定义，群在运算\*下是封闭的，这样对于G中任意两个元素a和b，a\*b也是G中的一个元素
2. G中包含一个元素e，称为单位元，对于G中每个元素a满足a\*e=e\*a
3. G中每个元素a都有逆元，，同时==e
4. 运算\*满足结合律，意味着(a\*b)\*c=a\*(b\*c)

阿贝尔群

群G中每个元素a和b满足a\*b=b\*a，则群为阿贝尔群

环

环R是具有两个运算+和\*即加法和乘法的代数系统，并满足以下性质：

1. R中所有元素与+运算一起必须构成一个阿贝尔群，+运算的单位元称为0
2. R在\*运算下必须是封闭的
3. 乘法的结合率，即(ab)c=a(bc)
4. 两个分配律，即(a+b)c=ac+bc，c(a+b)=ca+cb

交换环

对于环R中所有的a和b，如果乘法运算满足ab=ba，则这个环为交换环

含幺环

如果环R在乘法下含有单位元，则称为含幺环