数论入门

整除性与除法

整除性

- `a,b,m`为整数且b≠0，若`a=mb`则称b整除a,b是a的因子，记作`b|a`
- 整除的性质（以下皆为整数）
  - `a|1` => `a=±1`
  - `a|b` and `b|a` => `a=±b`
  - `b≠0` => `b|0`
  - `a|b` and `b|c` => `a|c`

    - `b|g` and `b|h` => `b|(mg+nh)`(整除线性组合)

除法

- `a = qn + r` q为商 r为余数

辗转相除法

```
int gcd(int x , int y)
{
    if(!y) return x;
    else return gcd(y , x%y);
}
```

模运算

模

- 若`a = qn +  r` and `q= ⌊a/n⌋`则称`r = a mod n`
- 若`(a mod n) = (b mod n)` 则称 `a≡b (mod n)` a与b模n同余 当 `b=0`时`n|a`
- 性质
    - `n|(a-b)` => `a≡b (mod n)`
    - `a≡b (mod n)` => `b≡a (mod n)`
    - `a≡b (mod n)` and `b≡c (mod n)` => `a≡c (mod n)`
- 运算
    - $((a \mod n)+(b \mod n)) \mod n=(a+b) mod\, n$
    - $((a \mod n)-(b \mod n)) \mod n=(a-b) mod\, n$
    - $((a \mod n)*(b \mod n)) \mod n=(a*b) mod\, n$
    - 例： 求11^4 mod 13 可以用((11^2 mod 13)*(11^2 mod 13)) mod 13 = 3

模运算的性质

- 定义Z_n = {0,1, …… ,n-1} 称Z_n为模n的剩余类，一个剩余类集
- Zn的每个数a都称为一个剩余类，里面包括了所有mod n为a的数，表示为[0],[1], …… ,[n-1] 其中[]里的是a，整个剩余类里的最小非负整数 求k属于的a的过程叫**模n的k约化**
- Z_n是有**乘法单位元（乘法幺元）**的**交换环**
- 在这个环里消去
    - 对于加法 `(a+b)≡(a+c) (mod n)` => `b≡c (mod n)`
    - 对于乘法 `(a*b)≡(a*c) (mod n)` => `b≡c (mod n)` 仅当 a与n互素

      造成乘法不能直接消去的限制的原因是，如果a与n不互素，用a乘以n的每个剩余类，将会产生重复的剩余类，从而不能覆盖n的每一个剩余类

群、环和域

群

群的定义

群是一种代数结构，由一个**集合**(G)以及一个**二元运算**(*)所组成，且必须满足

- **封闭性** ： a , b∈G => a * b ∈G
- **结合律** ：$(a*b)*c = a*(b*c)$
- **单位元** ：存在e使得 a∈G => $a*e = e*a = a$
- **逆元** ： a∈G => 存在a'使得 $a*a' = a'*a = e$

群概念里的**幂运算**定义为多次进行* 并且负的幂运算定义为逆元的幂运算

一般地说，乘法符号是群的常用符号。

置换的定义

1. Gn是n个符号元素的集合 表示为{ 1,2, ... ,n-1,n }
2. Gn到Gn的一一映射叫n个符号的一个置换
3. 置换可以用Gn的有序序列表示 如1 -> 2 2 -> 3 3 -> 2 可表示为{1,3,2}
4. Sn是Gn的集合 且可证明Sn和Sn上的关系合成运算是一个群
5. Sn的幺元是{ 1,2, ... ,n-1,n }（恒等映射）

特殊的群

- 满足交换律的群称为**交换群** 也就是**阿贝尔群**
- 阿贝尔群有两种主要运算符号—加法和乘法。
- 如果一个群的所有元素都可由某个元素进行幂运算得到，称之为**循环群** 如整数的加法群是由1生成的循环群
- 循环群G都是交换群
- 所有环都是关于它的加法运算的阿贝尔群。在交换环中的可逆元形成了阿贝尔乘法群。特别是实数集是在加法下的阿贝尔群，非零实数集在乘法下是阿贝尔群。

环

环的定义

类似于可交换群，只不过在原来的基础上又增添另一种运算，分别称他们为`+（加法）`和`·（乘法）`（这里所说的 + 与 · 一般不是的四则运算加法和乘法，虽然相似）。

一般我们用两个数相连来简单表示这里的乘法

环必须满足：

- 是加法的交换群（0表示加法幺元，-a表示逆元）
- 乘法封闭性和结合律
- 乘法对加法的分配律

特殊的环

- 满足乘法交换律 则称为 **交换环**
- 满足R中非0元素的乘积非0（也就是说乘积为0肯定有一个是0）叫**无零因子环**
- 满足含有乘法幺元（记作1）的叫 **幺环**
- 既是无零因子环又是幺环的交换环叫做**整环**

域

非零元素都含有乘法逆元(记作a^{-1})的整环叫**域**

域是一种可进行加、减(加上加法逆元)、乘和除（乘以乘法逆元）运算的代数结构。**域**的概念是**数域**以及四则运算的推广。

- 对于每个素数 p 和每个正整数 n 在同构的意义下存在惟一的p^n阶的有限域，并且所有元素都是方程 $x^{p^n} - x = 0$ 的根，该域的特征为p。

有限域

- 有限域(Galois field 伽罗华域)的元素个数叫做*阶*或者*序*
- 阶一定是一个素数p的正整数次幂 这样的域记作GF(p^n)
- 有限域最常见的例子是当 p 为素数时，整数对 p 取模

阶为p的GF (即n=1)

- $GF(p)$**被定义为 整数集合**Z_p{ 1,2,3, ... ,p-1,p } 运算是模p的加法和乘法
- 由于Z_n的n是素数，任何$a \in Z_n$都与n互质，因此a都有乘法逆元，这与这里不谋而合

最简单的GF举例

F_2:

```
+ | 0 1           ·| 0 1
--+----           --+----
0 | 0 1           0 | 0 0
1 | 1 0           1 | 0 1
```

F$_3$:

```
+ | 0 1 2        ·| 0 1 2
--+------        --+------
0 | 0 1 2        0 | 0 0 0
1 | 1 2 0        1 | 0 1 2
2 | 2 0 1        2 | 0 2 1
```

在GF(p)中求乘法逆元

对于$GF(p)$中的b，它与p互质

则 px + by = 1 = gcd (b,p)

只要解出y则y是b在域中的乘法逆元

这个方法也适用于环Z_n

多项式运算

普通多项式运算

对于n次多项式：$f(x) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$

- $n = 0$ 时称为常数多项式
- $a_n = 1$ 时称为 **首1多项式**
- 变元x称为不定元
- 系数a_n属于集合S
- 多项式运算包括加减法和乘法，当S是域的时候还有除法（整数集不是域，而有理数集合是域）
- 如果S是域 称多项式为域S上的多项式 这样的多项式集合是个环 叫**多项式环**
- 多项式的除法：在域上做普通的除法，得到的商也属于这个域（不一定整数），而非域上的多项式除法不一定有定义（结果不一定属于这个域）
- 如果域F上的多项式可以表示成两个多项式乘积，就说这个多项式**可约**
- 不可约的多项式称为**素数多项式**

GF(2)中的多项式

$GF(2)$中的多项式最有意义

- 其中加法是模2加法，**减法与加法**等价，相当于**异或**运算xor 也就是
  - $1+1=1-1=0$
  - $1+0=1-0=1$
  - $0+1=0-1=1$
  - $0+0=0-0=0$
- **乘法**是模2乘法，等价于 **逻辑与** 运算

最大公因式

最大公因式可以用辗转相除法来求

有限域GF(2^n)

研究意义

1. 很多加密算法都涉及到整数集合上的算术运算
2. 如果这个运算包括了除法 我们就必须定义在域上的运算
3. 我们希望这个整数集合是从0到2^n-1的 这样就能用一个n位的二进制字来表示了
4. 由于n>1时以2^n为模的整数集合不是域 我们无法定义除法运算 所以对于有限域$GF(2^n)$我们不用普通的模运算，而采用**多项式模运算**，这样可以构造域

多项式的模运算

多项式集合的约定

1. 设域Z_p(见这里)上的一元n-1次多项式构成集合S
2. S中的多项式具有以下形式

   $f(x)=a_n-1x^{n-1}+a_n-2x^{n-2}+...+a_1x+a_0$

   其中$a_n \in Z_p$ 也就是在$\{0,1,2,3,...,p-1\}$上取值
3. S共有 p^n 个这样的不同的多项式

运算的约定

1. 该运算遵循普通多项式运算的规则
2. 运算以p为模，即遵循Z_p上的运算规则
3. 如果乘法运算所得溢出（最高次数超过n-1），则要除以某个多项式$m(x)$然后取余数式，这个多项式是**既约（不可约）多项式**，所得余式记作$r(x)=f(x) \mod m(x)$
4. 多项式也有剩余类的概念，可以类推

域的构造和举例

符合上述约定的集合和运算构成有限域S 我们常常用p=2来构造$GF(2^n)$ 因为这样系数非0即1 好算也符合计算机的二进制原则

举例

高级加密标准(AES)用的域就是$GF(2^8)$ 既约多项式 $m(x)=x^8+x^4+x^3+x+1$

其中p=2 n=8 所有多项式的系数非0即1 最高次为7

GF(2^n)计算上的考虑

由于多项式可以用01串表示

- 加法可以用异或运算来代替
- 对于乘法$x * f(x)$ 相当于将$f(x)$左移1位低位补0，然后判断需不需要约化
    - 如果原f(x)最高位为0 则没有溢出
    - 如果原f(x)最高位为1 再加(异或)上$m(x)$
- $x^n \; mod \; p(x) = [p(x) - x^n] = [x^n + p(x)]$