附录　　密码学的数学基础

（翟起滨）

1 数的整除性

初等数论研究的基本对象是整数集合

$$Z = \{0 , \pm 1 , \pm 2 , \pm 3, \ldots\}$$

和自然数集合(即正整数集合)

$$N = \{1 , 2 , 3 , 4 , \ldots\}$$

在集合 N 中可以进行加法和乘法运算，即两个自然数之和或乘积仍然是自然数，在集合 Z 中除了加法和乘法之外还可以做减法运算，并且这些运算满足一些规律(即：加法和乘法的结合律和交换律，加法和乘法的分配律)，但是一般不能作除法，也就是说，设 a 和 b 是整数，$b \neq 0$，则 a/b 不一定是整数。即不一定存在整数 c，使得 $a = bc$。由此产生出数论中的第一个基本概念：数的整除性。

1.1 除数(因子)和整除的概念：

定义：设 Z 为有全体整数而构成的集合，若 $b \neq 0$ 且 $a , b , m \in Z$ 使得 $a = mb$

此时称 b **整除** a。记为 $b \mid a$,还称 b 为 a 的**除数(因子)**。如果不存在整数 m 使得

$a = mb$ 则称 b **不整除** a。

例如：24 的正因子是：1、2、3、4、6、8、12 和 24。

对于数的整除有以下规则成立：

1. 如果 $a \mid 1$ 则 $a = \pm 1$。

2. 如果 $a \mid b$ 且 $b \mid a$，则 $a = \pm b$。

3. 任何 $b \neq 0$ 能整除 0。

4. 如果 $b \mid g$ 而且 $b \mid h$，则对任意整数 m 和 n 有 $b \mid (mg + nh)$。

为明白最后一个规则，证明如下：

如果 $b \mid g$，则 g 是 b 的倍数，可以表示成：$g = b \times g_1$，g_1 为某一整数。

如果 $b \mid h$，则 h 是 b 的倍数，可以表示成：$h = b \times h_1$，h_1 为某一整数。

故有：

$$mg + nh = mbg_1 + nbh_1 = b \times (mg_1 + nh_1)$$

所以 b 能整除 $mg + nh$。

1.2 素数(质数)的概念:

定义：整数 $p > 1$ 被称为素数，是指 p 的因子仅有 $1, -1, p, -p$。

算术基本定理 ：任意大于 1 的整数 a 都能被因式分解为如下的唯一形式：

$$a = P_1^{\alpha_1} P_2^{\alpha_2} \ldots P_t^{\alpha_t}$$

其中 $P_t > P_{t-1} > \ldots \succ P_1$ 都是素数而且每一个 $\alpha_i > 0\ (i = 1, 2, 3, \ldots)$。

例如：$91 = 7 \times 13$；$11011 = 7 \times 11^2 \times 13$

1.3 互为素数

定义：符号 $\gcd(a,b)$ 表示 a 和 b 的最大公因子。正整数 c 是 a 和 b 的最大公因子，如果满足下列条件：

1. c 是 a 和 b 因子；
2. 任何 a 和 b 的因子也是 c 的因子。

规定，最大公因子为正数，而

$\gcd(a,b)=\gcd(a,-b)=\gcd(-a,b)=\gcd(-a,-b)$，一般 $\gcd(a,b)=\gcd(\,|a|,|b|\,)$。

此外，由于 0 均能被所有非零整数整除，若 a 不是 0，则有 $\gcd(a,0)=|a|$。

如果 $\gcd(a,b)=1$，则称 a 和 b 互素。

2 带余除法和欧几里德算法

2.1 带余除法

定理 1：（带余除法）设 $a,b\in Z,b>0$ 则存在唯一决定的整数 q 和 r，使得：

$$a=qb+r,0\le r<b$$

证明：定义实数 $a=[a]+\{a\}$，$[a]$ 前者为 a 的整数部分，$\{a\}$ 为 a 的小数部分。先证明满足条件的 q 和 r 是存在的。为此令 $q=\left[\frac{a}{b}\right]$，$r=a-qb$，则 q 和 r 都是整数，并且由于 $\frac{r}{b}=\frac{a}{b}-q=\left\{\frac{a}{b}\right\}$，而 $0\le\left\{\frac{a}{b}\right\}<1$，从而 $0\le\frac{r}{b}<1$，即 $0\le r<b$。

再证明q和r是唯一确定的。如果又有整数q'和r'使得$a=q'b+r'$，$0\le r'<b$，则$|r-r'|<b$，并且$r-r'=b(q'-q)$。这表明$r-r'$是正整数b的倍数，并且$r-r'$的绝对值又小于b。只有可能$r=r'$，于是$q=q'$，证毕。

利用定理 1 可以证明如下引理：

引理 1：考察集合$S=\{ax+by \mid x,y\in Z\}$

1. 若$m,n\in S$，则$m\pm n\in S$。
2. 若$n\in S,c\in Z$，则$cn\in S$。
3. 设d为集合S中的最小正整数，则S恰好是d的所有倍数构成的集合。
4. $d=\gcd(a,b)$。

引理 1 表明，集合S恰好是由$\gcd(a,b)$的所有倍数构成的，利引理 1 可以得到最大公因子的一些有用的性质：

引理 2：

1. 设m为正整数，则$\gcd(ma,mb)=m\times\gcd(a,b)$。
2. 若$\gcd(a,b)=d$，则$\frac{a}{d}$和$\frac{b}{d}$是互素的整数。
3. a和b的每个公因子都是$\gcd(a,b)$的因子。
4. 若$\gcd(a,m)=\gcd(b,m)=1$，则$\gcd(ab,m)=1$。
5. 若a，b是不全为 0 的整数，则对每个整数x有 $\gcd(a,b)=\gcd(a,b+ax)$。
6. 若$c\mid ab$，$\gcd(c,b)=1$，则$c\mid a$。

利用引理 2，我们可以推出求解最大公因子算法。

2.2 欧几里得算法

欧几里德算法：可以假设 $d > f > 0$，这是因为 $\gcd(a,b) = \gcd(|a|,|b|)$。

EUCLID(d,f)

1. $X \leftarrow d; Y \leftarrow f$

2. $if\ Y = 0\ return\ X = \gcd(d, f)$

3. $R = X \bmod Y$

4. $X \leftarrow Y$

5. $Y \leftarrow R$

6. goto 2

例如：要找出 $\gcd(1970,1006)$

$1970 = 1 \times 1006 + 904$ $\gcd(1006,904)$

$1006 = 1 \times 904 + 162$ $\gcd(904,162)$

$904 = 5 \times 162 + 94$ $\gcd(162,94)$

$162 = 1 \times 94 + 68$ $\gcd(94,68)$

$94 = 1 \times 68 + 26$ $\gcd(68,26)$

$68 = 2 \times 26 + 16$ $\gcd(26,16)$

$26 = 1 \times 16 + 10$ $\gcd(16,10)$

$16 = 1 \times 10 + 6$ gcd(10,6)

$10 = 1 \times 6 + 4$ gcd(6,4)

$6 = 2 \times 2 + 2$ gcd(4,2)

$2 = 2 \times 2 + 0$ gcd(2,0)

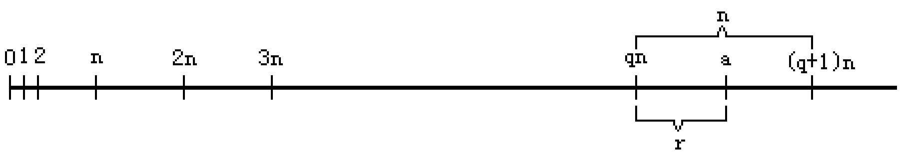
所以 gcd(1970,1066) = 2 。

3 模运算

我们已经知道，任意给定一个正整数 n 和任意一个整数 a，如果用 a 除以 n，得到商 q 和余数 r 将满足如下关系：

$a = qn + r \qquad 0 \le r < n; q = \lfloor a/n \rfloor$ （这里 $\lfloor x \rfloor$ 表示小于或者等于 x 的最大整数 ）

下图说明了给定 a 和正整数 n，总能找到 q 和 r 满足之前的关系。数轴上的点代表整数；a 必将为余数线上某一点（图中显示 a 为正数的情况，a 为负数也是类似的情况）。由 0 为起点，经过 n，$2n$，直到 qn，以致 $qn \le a$ 并且 $(q+1)n > a$ 由 qn 到 a 的距离是 r，这样就得到了唯一的值 q 和 r，剩余值 r 通常称为余数。



$$a = qn + r \qquad 0 \le r < n; q = \lfloor a/n \rfloor$$

注记：如果 $(a \bmod n) = (b \bmod n)$，则称整数 a 和 b 模 n 同余，可以书写为 $a \equiv b \bmod n$。整数的运算通过 **mod** n 而转换为模运算，这里 n 被称为模数。

例如：$73 \equiv 4 \bmod 23$；$21 \equiv -9 \bmod 10$

注意：如果 $a \equiv 0 \bmod n$ 则 $n \mid a$。

模运算有如下性质：

1. 如果 $n \mid (a-b)$ 则 $a \equiv b \bmod n$。
2. $(a \bmod n) = (b \bmod n)$ 等价于 $a \equiv b \bmod n$。
3. $a \equiv b \bmod n$ 等价于 $b \equiv a \bmod n$。
4. 如果 $a \equiv b \bmod n$ 而且 $b \equiv c \bmod n$，则有 $a \equiv c \bmod n$。

模 n 意义下的加、减、乘运算：

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$。
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a-b) \bmod n$。
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$。

下面证明第一条性质。定义 $(a \bmod n) = r_a$，$(b \bmod n) = r_b$ 则可得 $a = r_a + jn, j$ 为某一整数；$b = r_b + kn, k$ 为某一整数。有：

$$(a+b) \bmod n = (r_a + jn + r_b + kn) \bmod n$$

$$= (r_a + r_b + (k+j)n) \bmod n$$

$= (r_a + r_b) \bmod n$

$= [(a \bmod n) + (b \bmod n)] \bmod n$

注：1．指数运算可以看作是多次重复乘法：

例如：为了计算$11^7 \bmod 13$可以按照如下方式进行：

$11^2 = 121 \equiv 4 \bmod 13$

$11^4 \equiv 4^2 = 3 \bmod 13$

$11^7 = 11 \times 4 \times 3 \equiv 132 \equiv 2 \bmod 13$

因此，普通算术运算中的加法、乘法、减法都可以适用于模运算。

2．可以编制模运算的表：

模 8 运算表：

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

×	0	1	2	3	4	5	6	7
0	0	0	0	0		0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	7	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

模运算的基本定律：

定义集合 Z_n 为所有小于 n 的非负整数集合：

$$Z_n = \{0,1,\ldots,(n-1)\}$$

如果在该集合上实行模运算，Z_n 中的运算符合如下定律：

1. 交换律：

   $(w+x)\bmod n = (x+w)\bmod n \qquad (w\times x)\bmod n = (x\times w)\bmod n$

2. 结合律

   $[(w+x)+y]\bmod n = [w+(x+y)]\bmod n \qquad [(w\times x)\times y]\bmod n = [w\times(x\times y)]\bmod n$

3. 分配律

   $[w\times(x+y)]\bmod n = [(w\times x)+(w\times y)]$

4. 恒等

   $(0+w)\bmod n = w\bmod n \qquad (1\times w)\bmod n = w\bmod n$

5. $(a+b)\equiv(a+c)\bmod n \to b\equiv c\bmod n$

6. $(a\times b)\equiv(a\times c)\bmod n \to b\equiv c\bmod n,$　如果a与n互素时成立，否则不成立；

   例如：

$6\times 3=18\equiv 2\bmod 8 \qquad 6\times 7=42\equiv 2\bmod 8 \qquad$ 但是$3\neq 7\bmod 8$　。

易见，如果 p 是一个素数，则所有元素 $w\in Z_p$ 均与 p 互素。这样就能在之前所列的性质中再加上一条性质：

对每一个 $w \in Z_p$，存在它的乘法逆元 z，使得 $w \times z \equiv 1 \bmod p$。

最后一点：如果 $\gcd(a,n)=1$，则能在 Z_n 中找到 b，使得 $a \times b \equiv 1 \bmod n$。

4 数论中一些有用的定理

4.1 费马（Fermat）定理

定理 2（费马定理）：如果 p 为素数，a 是不能被 p 整除的正整数，则有：

$$a^{p-1} \equiv 1 \bmod p$$

证明：从以前的讨论中得出，如果 Z_p 中所有数均与 a 相乘模 p，结果将以某种次序涵盖 Z_p 中的数。并且，$a \times 0 \equiv 0 \bmod p$。因此，$(p-1)$ 个数 $\{a \bmod p, 2a \bmod p, \ldots, (p-1)a \bmod p\}$ 恰好是某种次序的 $\{1, 2, \ldots, (p-1)\}$。将这些数相乘可得：

$$a \times 2a \times 3a \times \cdots \times ((p-1)a)$$

$$\equiv [(a \bmod p) \times (2a \bmod p) \times \cdots \times ((p-1)a \bmod p)] \bmod p$$

$$\equiv (p-1)! \bmod p$$

但是：

$$a \times 2a \times 3a \times \cdots \times ((p-1)a) = (p-1)!a^{p-1}$$

所以：

$$(p-1)!a^{p-1} \equiv (p-1)! \bmod p$$

两端消去 $(p-1)!$，因为它与 p 互素。定理得证。

费马定理的另一种等价形式也是十分有用的：如果 p 是素数，a 是任意正整数，则：

$$a^p \equiv a \bmod p$$

4.2 欧拉函数

欧拉函数（Euler's toient function），记为 $\phi(n)$，$\phi(n)$ 表示小于 n 且与 n 互素的正整数的个数，$\phi(1)$ 被规定为 1。

例如：下表列出了 30 以内的整数的 $\phi(n)$ 值，$\phi(1)$ 被规定为 1。

某些数和它们的欧拉函数

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8
n	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$\phi(n)$	8	16	6	18	8	12	10	22	8	20	12	18	12	28	8

很显然，对于任意一个素数 p，有：

$$\phi(p) = p - 1$$ 。

现在假定有两个不同的素数 p 和 q，则对于 $n = pq$，有：

$$\phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)\times(q-1)$$

为了完全证明这一命题，考虑 Z_n 的完全余数集为：$\{0, 1, 2, \ldots, (pq-1)\}$，而不与 n 互素的余数包括集合 $\{p, 2p, \ldots, (q-1)p\}$,集合 $\{q, 2q, \ldots, (p-1)q\}$ 和 0。因此：

$$\phi(n) = pq - [(q-1) + (p-1) + 1]$$

$$= pq - (p+q) + 1$$

$$= (p-1) \times (q-1)$$

$$= \phi(p) \times \phi(q)$$

#

对于一般的整数 n，它的欧拉函数 $\phi(n)$ 的求解方法由以下定理给出：

定理 3： $\phi(1) = 1$，**当 $n \geq 2$ 的时候，设 $n = p_1^{e_1} p_2^{e_2} \cdots p_g^{e_g}$ 是 n 的标准分解式，**

则： $\phi(n) = \prod_{i=1}^{g} (p_i^{e_i} - p_i^{e_i - 1}) = n \times \prod_{i=1}^{g} (1 - 1/p_i)$。**（可用包含与排斥原理来证明这个定理。）**

4.3 欧拉定理

定理 4（欧拉定理）：对于任何与 n 互素的整数 a，有：

$$a^{\phi(n)} \equiv 1 \bmod n$$

证明：易见，如果 n 为素数，符合费马定理条件，结论成立。设 n 为任意正整数，构造小于 n 且与 n 互素的正整数集合：

$$R = \{x_1, x_2, \ldots, x_{\phi(n)}\}$$

对该集合中的每个整数乘以 a 模 n：

$$S = \{(ax_1 \bmod n), (ax_2 \bmod n), \cdots, (ax_{\phi(n)} \bmod n)\}$$

集合 S 是集合 R 的一个置换（即元素相同，顺序不同），原因如下：

1. 因为 a 和 n 互素，x_i 和 n 也互素，则 ax_i 一定和 n 也互素。因此，S 中的所有数均小于 n 并且和 n 互素。
2. S 中不存在重复的整数。如果 $ax_i \bmod n = ax_j \bmod n$，则 $x_i = x_j$。

因此：

$$\prod_{i=1}^{\phi(n)}(ax_i \bmod n) = \prod_{i=1}^{\phi(n)} x_i$$

$$\prod_{i=1}^{\phi(n)} ax_i \equiv \prod_{i=1}^{\phi(n)} x_i (\bmod n)$$

$$a^{\phi(n)}\left[\prod_{i=1}^{\phi(n)} x_i\right] \equiv \prod_{i=1}^{\phi(n)} x_i (\bmod n)$$

$$a^{\phi(n)} \equiv 1(\bmod n)$$ 。

证毕

欧拉定理的另一种等价形式为：

$$a^{\phi(n)+1} \equiv a(\bmod n)$$

这种形式在说明 RSA 算法的时候是很有用的。给定两个素数 p 和 q 以及整数 $n = pq$ 和 m，其中 $0 < m < n$，则下列关系成立：

$$m^{\phi(n)+1} = m^{(p-1)(q-1)+1} \equiv m \bmod n$$

如果$\gcd(m,n)=1$，则根据欧拉定理显然成立。假定$\gcd(m,n)\neq 1$，因为$n=pq$，它等价于m是p的倍数或m是q的倍数。

不妨设m是p的倍数的情况，显然$m=cp$，c是某个正整数。在这种情下，必然有$\gcd(m,q)=1$。否则，m是p的倍数，m是q的倍数，与$m<pq$矛盾。

我们有$m^{\phi(q)}\equiv 1 \bmod q$。易见，有

$$\left[m^{\phi(q)}\right]^{\phi(p)}\equiv 1 \bmod q \quad \text{，得到} \; m^{\phi(n)}\equiv 1 \bmod q$$

因此，存在某个整数k使得：

$$m^{\phi(n)}=1+kq$$

在等式两边同时乘$m=cp$，有：

$$m^{\phi(n)+1}=m+kcpq=m+kcn$$

$$m^{\phi(n)+1}\equiv m \bmod n \quad 。$$

事实上，对于$m=cp$时，我们也不难推出如下结论：

$$m^{k\phi(n)+1}\equiv m \bmod n \quad ;$$

这样，在 **RSA** 密码算法中就可以对明文 m 的限制仅为 $0<m<n$ 就可以了。

注记：当 $n=p$ 时，有 $a^{p-1}\equiv 1(\bmod p)$ 为费马定理。

例如：利用欧拉定理，求 3^{400} 的最末两位数字。

由于 3 和 100 互素，由欧拉定理知：$3^{40}\equiv 1 \bmod 100$。于是：

$3^{400}=(3^{40})^{10}\equiv 1^{10}\equiv 1(\bmod 100)$，所以 3^{400} 的最末两位数字是 01。

4.4 中国剩余定理（CRT）

数论中最有用的基础之一是中国剩余定理。它来源于如下简单的例子：

例如：（孙子算经）今有物不知其数。三三数之余二，五五数之余三，七七数之余二。问物几何？

答曰：$23\equiv 2\times 70+3\times 21+2\times 15(\bmod 105)$

（口诀：三人同行七十稀，五树梅花廿一枝，七子团圆月正半，除百零五便得知。）

问题是：70，21，15 是如何得到的？

原问题为求解同余方程组：

$$\begin{cases} x\equiv 2(\bmod 3) \\ x\equiv 3(\bmod 5) \\ x\equiv 2(\bmod 7) \end{cases}$$

注意：若 x_0 为上述同余方程组的解，则 $x_1=x_0+k\times 105$ 也为上述同余方程组的解。有意义的是，解题口诀提示我们先解下面三个特殊的同余方程组：

$$\begin{cases} x\equiv 0(\bmod 3) \\ x\equiv 1(\bmod 5) \\ x\equiv 0(\bmod 7) \end{cases} \qquad \begin{cases} x\equiv 0(\bmod 3) \\ x\equiv 0(\bmod 5) \\ x\equiv 1(\bmod 7) \end{cases} \qquad \begin{cases} x\equiv 1(\bmod 3) \\ x\equiv 0(\bmod 5) \\ x\equiv 0(\bmod 7) \end{cases}$$

的特殊解：

$$\begin{pmatrix}1\\0\\0\end{pmatrix}=70 \qquad \begin{pmatrix}0\\1\\0\end{pmatrix}=21 \qquad \begin{pmatrix}0\\0\\1\end{pmatrix}=15$$

中国剩余定理：设自然数 $m_1, m_2, \cdots, m_r$ 两两互素，并记 $N = m_1 m_2 \cdots m_r$，则同余方程组：

在模 N 同余的意义下有唯一解。

证明：考虑方程组：

$$\begin{cases} x \equiv 0(\bmod m_1) \\ \quad \cdots \\ x \equiv 0(\bmod m_{i-1}) \\ x \equiv 1(\bmod m_i) \\ x \equiv 0(\bmod m_{i+1}) \\ \quad \cdots \\ \quad \cdots \\ x \equiv 0(\bmod m_r) \end{cases} \qquad (1 \le i \le r)$$

由于各个 m_i 两两互素，这个方程组做变量替换，令 $x = (N / m_i) \times y$ 方程组等价于解同余方程组：

$$(N / m_i) y = 1(\bmod m_i) \quad (1 \le i \le r)。$$

若要得到特解，只要令

$$x_i = (N / m_i) \times y_i$$

则方程组的解为：$x_0 = b_1 x_1 + b_2 x_2 + \cdots + b_r x_r \pmod N$

在模 N 同余的意义下唯一。证毕。

5 群论中的若干基本概念

定义（群）设 G 为非空集合，若在 G 中定义一个运算“$\cdot$”，使得 $\forall a, b \in G$（表示从 G 中取出得任意元素 a, b）有 $a \cdot b \in G$，并且满足如下公理：

1. 结合律成立：$\forall a, b, c \in G$ 有 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$；
2. G 中存在单位元 e：$\forall a \in G$，有 $e \cdot a = a \cdot e = a$；
3. G 中存在相应的逆元：$\forall a \in G$，有 $a^{-1} \in G$，使得 $a \cdot a^{-1} = a^{-1} \cdot a = e$；

则称 G 对运算“$\cdot$”形成一个群，具体表示为 $(G, \cdot)$，一般记为 G。

注：

1. $|G|$ 表示群 G 内的元素的个数；若 $|G| < +\infty$（G 内的元素有限），则称 G 为有限群；若 $|G| = +\infty$，称 G 为无限群。
2. 若 $\forall a, b \in G$，有 $a \cdot b = b \cdot a$，称 G 为交换群（或称 G 为 Abel 群）。
3. G 为群，H 是 G 的一个非空子集。如果相对于 G 的那个运算来说，H 也是一个群，则称 H 是 G 的一个子群，记为 $H \le G$。

我们可以发现全体整数的集合 Z 对整数的加法形成一个群 Z^+。取定一个正整数 n，则由 n 的一切整倍数所形成的集合 H_n 是 Z^+ 的一个子群。易见，对于同余式：

$$a \equiv b (\bmod n)$$

相当于说$a-b \in H_n$；于是，上述同余式可以写为：

$$a \equiv b (\bmod H_n)$$

定义（左陪集）：设G是一个群，H是G的一个子群。设$a \in G$，那么集合$\{ah \mid h \in H\}$被称为群G中相对于子群H的a左陪集，表示为aH，即$aH = \{ah \mid h \in H\}$，a为左陪集代表元。自然，也有右陪集的概念。

注：

1. 有关左陪集的重要性质：

   (1). $aH = bH \Leftrightarrow a^{-1}b \in H$

   (2). $aH = H \Leftrightarrow a \in H$

   (3). $b \in aH \Leftrightarrow aH = bH$

2. $\forall a,b \in G$,有$aH = bH$或者$aH \cap bH = \phi$。

3. G可以按照子群H的左陪集分解为一些两两不交的等价类。若$g_1, g_2 \in G$，它们是在同一类中，是指$g_1^{-1}g_2 \in H$，即$g_1H = g_2H$；形式地记为：$a \equiv^{(左)} b (\bmod H)$

4. 易见，$G = \bigcup_{g \in G} gH$

5. G为群，$H \le G$。H在G中的左陪集的个数称为H在G中的指数，记为$[G:H]$。

6. 若G为有限群，$H \le G$，则有：$|G| = |H| \cdot [G:H]$

定义（正规子群）：G 为群，H 是 G 的子群，若 $\forall g \in G$ 有 $gH = Hg$ 则称 H 是 G 的正规子群，记为 $H \trianglelefteq G$。

注：

1. 如果 G 是交换群，那么它里面的任何一个子群都是 G 的正规子群。

2. 设 $H \trianglelefteq G$，则 G/H 对自己的乘法构成群，这里

$$G/H = \{aH \mid a \in H, H\text{是}G\text{的正规子群}\}。$$

证明：$\forall aH, bH \in G/H$，有：

$$(aH)(bH) = a(Hb)H = abHH = abH \in G/H$$

由于群 G 满足结合律，自然 G/H 关于陪集的运算也满足结合律；另一方面，可以验证 H 为 G/H 中的单位元，并且 $(aH)(a^{-1}H) = aa^{-1}H = H$，说明 G/H 中的每个元素都有逆元。所以 G/H 是群。

定义（商群）：设 G 是群，$H \trianglelefteq G$，则 G/H 关于子集的乘法构成的群称为 G 关于 H 的商群。

注：群 G 的商群 $\overline{G} = G/H$ 是类比于整数加群 Z^+ 模整数 n 而得到的剩余类加群：

$$Z^+ / < n >= \{[0],[1],[2],\cdots,[n-1]\}$$

定义（循环群）：若群 G 可以由一个元素的方幂生成，即

$G=\{\cdots,g^{-3},g^{-2},g^{-1},g^{0}=1,g,g^{2},g^{3},\cdots\}$，此时，称$G$为循环群，其中$g$为$G$的生成元，记为$G=< g >$。

例如：循环群的几个例子：

1. 全体整数的集合Z对于整数的加法形成一个循环群，记为Z^{+}，它的生成元仅有 1 和-1。Z^{+}为无限循环群。

2. n次复单位根对复数乘法形成一个n阶循环群$U_n=<\xi>,\xi$为n次本原单位根。

3. 整数同余类环$Z/< n >$中的全部元素对同余类加法所形成的群Z_n^{+}，是一个阶为n的循环群。若a和n互素，则由a决定的模n同余类$[a]$就是Z_n^{+}的生成元。事实上，$\forall[b]\in Z_n^{+}$，必有一个整数k使得$a\cdot k\equiv b(\bmod n)$。这样，我们有：

$$k[a]=[a]+[a]+\cdots+[a]=[k\cdot a]=[b]\text{（有}k\text{个}[a]\text{）}$$

4. 整数同余类环$Z/< n >$的乘法可逆元的全体组成的集合对同余类乘法形成一个群Z_n^{*}，这个群是交换群，一般不是循环群，以Z_{12}^{*}为例，

$$Z_{12}^{*}=\{[1],[5],[7],[11]\}$$

它不是循环群。仅当n为素数p的时候，Z_n^{*}为循环群。

6 环和域的基本概念

6.1 环

定义（环）：所谓一个（结合）环，指的是这样一个集合R，在它里面定义了加法“＋”和乘法“·”两种运算，并且满足下列条件：

1. 集合R相对于加法“＋”来说构成交换群；

2. 集合R相对于乘法“·”来说封闭，且满足结合律；

3. 分配律成立：$\forall a,b,c \in R$， $a \bullet (b+c) = a \bullet b + a \bullet c$，并且有：

   $(b+c) \bullet a = b \bullet a + c \bullet a$；

注：

1. $\forall a \in R, a^m a^n = a^{m+n}$　　$(a^m)^n = a^{mn}$，注意，当乘法不满足交换律的时候，公式$(ab)^n = a^n b^n$一般不成立。

2. 若环R对“·”来说满足交换律，称它为交换环。

3. 环R被称为含有单位元的环，是指R内含有乘法单位元“1”，使得$\forall a \in R$有$a \bullet 1 = 1 \bullet a = a$。

例如：环的若干例子：

1. **整数环**Z:易见全体整数的集合对数的加法形成一个群；对数的乘法形成一个含有乘法单位元的半群；两种运算由分配律连接起来。Z为含有单位元“1”的交换环。它是最具体最容易被接受的数环。

2. **剩余类环**Z_n**:**Z_n为整数模n剩余类的集合

$$Z_n = \{[0],[1],\cdots,[n-1]\}$$

它对剩余类的加法和乘法构成一个含有单位元“[1]”的交换环。

3. 各式各样的数域都对通常的数的加法和乘法形成一个含有“1”的交换环。

4. 设 F 表示任意数域。定义

   $F[x]=\{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid a_i \in F, n\text{为正整数}\}$，易验证 F[x]相对于多项式加法和乘法构成数域 F 上的一元多项式环。

5. 取大于 1 的正整数 n，则 n 的一切整数倍形成的集合 nZ 对数的加法和乘法形成了一个不含单位元“1”的交换环。

6.2 整环

定义（整环）：含有乘法单位元“1”而无零因子的交换环称为整环。

注：

1. 无零因子是指，由 $a \cdot b = 0$ 可以推出 $a=0$ 或者 $b=0$。反之，如果 $a \neq 0$、$b \neq 0$，但是 $a \cdot b = 0$，则称 a 为 0 的左零因子，b 为 0 的右零因子。

2. 整环是类比于我们熟知的整数环，提取了整数环中的主要特征，例如乘法的消去律。

3. 任何一个整环都至少含有 2 个元素。恰含有 2 个元素的整环是存在的，例如 $F_2=\{0,1\}$ 它对模 2 的加法乘法运算形成一个整环，事实上，它为二元域。

定义（除环）：一个环被称为除环（或斜域），是指该环的非零元全体对“•”形成一个群。

定义（域）：一个可交换的除环称为域。

注：

1. F_p 为整数模 p 的剩余类环， p 为素数，可以验证它为域。因为 F_p 中的元素有限，称它为有限域；又因为 p 为素数，又称之为素域。

2. 域首先必是整环；反之则不然。例如，整数环 Z ，域 F 上的多项式环 $F[x]$ 都是整环，但它们都不是域。然而，对有限整环来说，我们有重要定理：

定理 5：任意一个由有限个元素组成的整环 R 必定是有限域。

定理 6：在整环 R 的加法群 R^+ 中，或者每个非零元素都生成一个无限阶的循环群；或者存在一个素数 p ， R^+ 中的每个元素都生成一个 p 阶循环子群。

证明： R 为整环，于是 $1\in R$ 。 R^+ 作为 R 的加法群含有由 1 生成的循环子群

$$<1>=\{k\cdot 1\,|\,k\in Z\}$$

1. 如果 $<1>$ 为无限循环群：

$\forall a\in R, a\neq 0,$ 来证 $<a>$ 也为无限循环群。若否，设 a 的阶为 m ，于是：

$$0=m\cdot a=\underbrace{a+a+\cdots+a}_{m}=(\underbrace{1+1+\cdots+1}_{m})\cdot a=(m\cdot 1)\cdot a$$

由于整环无零因子，必有 $m\cdot 1=0$ ，说明 $|<1>|$ 为 m 的因子，与 $<1>$ 为无限循环群矛盾。所以 $<a>$ 也为无限循环群。

2. 如果 $<1>$ 为有限循环群：

首先断定 R^+ 元素 1 的阶必为某个素数 p 。事实上，如果假设 $|<1>|=m=p_1p_2$，其中 $1<p_1<m, 1<p_2<m$ 。我们有：

$$(p_1\cdot 1)(p_2\cdot 1)=\underbrace{(1+1+\cdots+1)}_{p_1}\underbrace{(1+1+\cdots+1)}_{p_2}=\underbrace{1+1+\cdots+1}_{m}=m\cdot 1=0$$

由于整环无零因子，所以 $p_1\cdot 1$ 和 $p_2\cdot 1$ 这两者中必然有一个为 0，这与 $|<1>|=m$ 矛盾。所以 m 必为素数，设 $m=p$ 为一个素数。$\forall a\in R, a\neq 0$，有

$$p\cdot a=\underbrace{a+a+\cdots+a}_{p}=\underbrace{(1+1+\cdots+1)}_{p}\cdot a=(p\cdot 1)a=0$$

说明 R^+ 中的每个非零元素都生成一个 p 阶的循环子群，证毕。

注：当 R 为整环时，上述定理中的两种情况必有而且仅有一种成立。前一种情况称整环 R 的特征为 0（$char\ R=0$）；后一种情况称整环 R 的特征为 p（$char\ R=p$）。易见，有限域作为特殊的整环，它的特征必定为 p。

推论 1：F 为有限域，则 F 中的元素的个数 $|F|$ 是其特征的方幂，即 $|F|=p^n$。

推论 2：在一个特征为 p 的整环 R 中，对任意自然数 m 有：

$$(a+b)^{p^m}=a^{p^m}+b^{p^m},\quad (ab)^{p^m}=a^{p^m}b^{p^m},\forall a,b\in R$$

推论 3：在一个特征为 p 的整环 R 中，由等式 $a^{p^m}=b^{p^m}$ 对某个自然数成立，可以断定 $a=b$。

2.6.3 子环和环同构

定义（子环）：设 R 是一个环，$R_1\subseteq R.R_1\neq\phi$，如果 R_1 对 R 的运算“＋”和“•”也形成一个环，称 R_1 为 R 的一个子环。

定义（环同构）：设R和R'是两个环。如果有一个从R到R'之上的 1-1 映射φ，且$\forall a,b \in R$有：

$$\varphi(a+b)=\varphi(a)+\varphi(b)$$

$$\varphi(ab)=\varphi(a)\cdot\varphi(b)$$

此时，称φ为从R到R'上的同构映射，也称R和R'同构。

注：同构映射φ把R中的“0”元映射成为R'中的“0”元；若R为含有单位元“1”的环，则φ把R中的“1”元映射成为R'中的“1”元；把R中的子环映射成为R'中的子环。

定理 7：任何一个特征为 0 的整环R（或者域F）都包含了一个整子环（子域），它同构于整数环Z（有理数域Q）；任何一个特征为$p>0$的整环R（或者域F）都包含一个子整环同构于F_p。

注：由此定理知，整环或者域都包含有一个最小的整环（或者最小的域）做它们的出发点。

下面讨论交换环R的商环。我们已经知道，对群G的一个正规子群H来说，可以给出商群$\overline{G}=G/H$，这个商群以H的各个陪集作为元素，使得G/H成为G的一个缩影。如何把这个现象类比到商环呢？先从最具体的整数环Z入手，设R为整数环Z，它的子环：

$$R_1=\langle n\rangle=\{n\cdot k\mid k\in Z\}$$

$\forall m,l\in Z$，称 m,l 模 R_1 同余，即 $m\equiv l(\mathrm{mod}R_1)$，相当于 $n\,|\,m-l$，由数论的写法 $m\equiv l(\mathrm{mod}\,n)$。$R$ 对 R_1 的商环就是：

$$Z/R_1=Z_n=\{[0],[1],\cdots,[n-1]\}$$

我们已知在 Z_n 的乘法为 $[a][b]=[ab]$，它的意义是：$\forall a+r_1\in[a],\forall b+r_2\in[b]$，有：

$[a][b]=(a+r_1)(b+r_2)=ab+ar_2+r_1b+r_1r_2=[ab]$，相当于：

$$ar_2+r_1b+r_1r_2\in<n>=R_1$$

这就诱导出一般交换环 R 中的理想子环的想法。

定义（理想）：交换环 R 的一个子环 R_1 称为 R 中的一个理想子环（简称理想），如果 $\forall a\in R,r\in R_1$ 有 $ar\in R_1$。

注：

1. 设 $b_1,b_2\cdots,b_n$ 是整环 R 中的任意一组元素，则形如：

$$r=a_1b_1+a_2b_2+\cdots+a_nb_n,\forall a_i\in R$$

的元素全体是 R 中的理想 R_1，它称为由 $b_1,b_{2,}\cdots,b_n$ 这些元素生成的理想，记为：$<b_1,b_{2,}\cdots,b_n>$。

特别，由单独一个元素 b 所生成的理想 $<b>$ 被称为 R 中的一个主理想，由 R 中的一切形如 ab 的元素组成，$<b>=\{ab\,|\,a\in R\}$。

2. 整数环 Z 中，Z 的任何一个子环都是一个理想；Z 的任何一个理想都是主理想。原因是，Z^+ 是循环群，Z^+ 的任何一个子群也必然是循环群 H_n。

3. 域 F 上的多项式环 $F[x]$ 中，不一定每一个子环都是理想子环，例如，有理数域上的一元多项式环 $Q[x]$ 中，带整系数的那些多项式组成一个子环，但不是理想。然而，可以证明多项式环 $F[x]$ 中的每一个理想都是主理想。

定理 8：设 R 是一个交换环， R_1 是 R 的一个理想。如果将两个模 R_1 同余类 $[a],[b]$ 的和与积分别定义为同余类 $[a+b],[ab]$，即：

$$[a]+[b]=[a+b],\quad [a]\cdot[b]=[ab]$$

则由全部模 R_1 同余类所组成的集合 $\overline{R}=R/R_1$ 对上述运算构成环，称为 R 对 R_1 的商环。

2.7 有限域

定义（子域，扩域）：设 E 为一个域， F 为 E 中的一个非空子集。如果相对于 E 中的加法和乘法来说 F 是一个域，则称 F 为 E 的一个子域（或者基域）， E 为 F 的一个扩域（或扩张）。

注：

1. 任何一个特征为 0 的域 E 都包含一个子域 F ，它同构于有理数域 Q；任何一个特征为 p 的域 E 都包含了一个子域 F ，它同构于素域 F_p。易见，扩域 E 对 E 中的加法运算和 F 中的元素与 E 中的元素的乘法运算形成 F 上的一个向量空间。如果 E 作为 F 上的向量空间是 n 维的，则 E 被称为 F 的一个 n 次

扩张，否则 E 称为 F 的无限次扩张。前者记为 $[E:F]=n$，后者记为 $[E:F]=\infty$。

2. 特征为 0 的域 E 可以视为由有理数域 Q 扩张而来；特征为 p 的域 E 可视为由素域 F_p 扩张而来。对于特征为 p 的域 E 来说，若设 E 的乘法单位元为 e，则 e 的全体整倍元的集合为 $\{e,2e,\cdots,(p-1)e \mid pe=\overline{o}\}\cong F_p$。这就说明 E 可视为由 F_p 扩张而来。若设 $[E:F_p]=n$，则存在 n 个元素 $u_i(1\le i\le n)$ 使得 E 中任意元 u 可以唯一的表示成为：

$$u=a_1u_1+a_2u_2+\cdots+a_nu_n \qquad a_i\in F_p$$

从而可知 $|E|=p^n$

定理 9（域扩张）:设 F 为任意域，而

$$m(x)=x^d+m_1x^{d-1}+m_2x^{d-2}+\cdots+m_d,m_i\in F$$

为 F 上的一个 d 次不可约多项式，则同余类环 $E=F[x]/<m(x)>$ 可视为 F 上的一个有限次扩域，并且有：$[E:F]=d$。

证明：首先证明 $E=F[x]/<m(x)>$ 为域。设 $f(x)\in F[x]$，$\forall q(x)\in F[x]$ 有：

$q(x)m(x)+f(x)$ 模 $m(x)$ 的同余类设为 $[f(x)]$，知它是 E 中的一个元素，若 $f(x)\notin[0]$，知 $(f(x),m(x))$=1，因此必有多项式 $u(x)\in F[x]$，使得：

$$u(x)f(x)+v(x)m(x)=1$$

于是有：$[u(x)]\cdot[f(x)]=[1]$，或者说$[f(x)]^{-1}=[u(x)]$。这说明

$E=F[x]/<m(x)>$中的每个非零元素都有乘法逆元，所以它是一个域。下面证明$[E:F]=d$。

E中由零次多项式，亦即F中的元素所决定的那些模$m(x)$同余类$[k],k\in F$组成E中的一个子域$\overline{F}$；而映射$\sigma(k)=[k]$是F到$\overline{F}$之上的一个同构映射。这样，F中的元素k的同余类$[k]$仍然可视为k，把x决定的模$m(x)$的同余类$[x]$可以记为α，这样一来$F[x]$中的任意多项式

$$[f(x)]=a_0+a_1x+\cdots+a_nx^n$$

对应于

$$[f(x)]=[a_0+a_1x+\cdots+a_nx^n]=[a_0]+[a_1][x]+\cdots+[a_n][x^n]=a_0+a_1\alpha+\cdots+a_n\alpha^n$$
$$=f(\alpha)$$

特别，我们有$m(\alpha)=[m(x)]=0$,于是借助于F上不可约多项式$m(x)$所造出的扩域E中，元素α $(=[x])$是$m(x)$的一个零点。不仅如此，假如F上的另一个多项式$l(x)$也以α为零点，那么由$[l(x)]=l(\alpha)=0$，可知有$m(x)\,|\,l(x)$。事实上，$\forall f(x)\in F[x]$有

$$f(x)=q(x)m(x)+r(x),$$

其中：

$$r(x)=r_0+r_1x+\cdots+r_{d-1}x^{d-1}$$

于是

$$[f(x)] = f(\alpha) = r_0 + r_1\alpha + \cdots + r_{d-1}\alpha^{d-1}$$

也即E中任意元素都可以表示成为$1,\alpha,\cdots,\alpha^{d-1}$的线性组合。

另一方面，若有$a_0,a_1,\cdots,a_{d-1} \in F$，使得$\sum_{i=0}^{d-1} a_i\alpha^i = 0$，相当于说 $m(x) \mid a_0 + a_1x + \cdots + a_{d-1}x^{d-1}$，仅当$a_0 = a_1 = \cdots = a_{d-1} = 0$。说明$1,\alpha,\cdots,\alpha^{d-1}$关于域$F$是线性无关的，于是它们为$E$在$F$的一个基，有$[E:F] = d$。证毕。

注：

1. 对于关系式$m(\alpha) = [m(x)] = 0$来说，意味着扩域E是基域F上的不可约多项式$m(x)$的一个零点α添加到F上去而得到的，可把E记为$F(\alpha)$。特别的，如果F是素域F_p，而$m(x)$是F_p上的一个d次不可约多项式，则$F_p(\alpha)$是由p^{α}个元素构成的域。事实上，任何一个有限域都可以从某个素域F_p出发，通过添加F_p上某个不可约多项式的一个零点得到。

2. 当我们把$F(\alpha)$中的元素表示成为$f(\alpha) = r_0 + r_1\alpha + \cdots + r_{d-1}\alpha^{d-1}$这种形式的时候，表达式中的系数$r_i(0 \le i \le d-1)$是唯一确定的，因此可以把$F(\alpha)$中的元素表示为$F$上的$d$维向量$\gamma = (\gamma_0,\gamma_1,\cdots,\gamma_{d-1})$。

例如：$m(x) = x^4 + x^3 + 1$是F_2上的一个四次不可约多项式。易见，$F_2[x]/<x^4 + x^3 + 1>$为F_2上的一个四次扩域。如果把$[x]$记为α，那么这个域中的 16 个元素可以表示为：

$$\gamma = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3, a_i \in F_2$$

这 16 个元素可以表示为：

$\gamma_0 = (0,0,0,0)$，$\gamma_1 = (1,0,0,0)$，$\gamma_2 = (0,1,0,0)$，$\gamma_3 = (1,1,0,0)$，$\gamma_4 = (0,0,1,0)$，

$\gamma_5 = (1,0,1,0)$，$\gamma_6 = (0,1,1,0)$，$\gamma_7 = (1,1,1,0)$，$\gamma_8 = (0,0,0,1)$，$\gamma_9 = (1,0,0,1)$，

$\gamma_{10} = (0,1,0,1)$，$\gamma_{11} = (1,1,0,1)$，$\gamma_{12} = (0,0,1,1)$，$\gamma_{13} = (1,0,1,1)$，$\gamma_{14} = (0,1,1,1)$，

$\gamma_{15} = (1,1,1,1)$

请读者自行计算$\alpha^5,\alpha^6,\cdots,\alpha^{15}$的表达式。

我们可以用线性代数的知识证明下面的

定理 10（望远镜公式）：设域E是域F的有限次扩张，域K是域E的有限次扩张，则域K是域F的有限次扩张，并且有：$[K:F]=[K:E][E:F]$

事实上，我们已经注意到作为有限域F一身兼具了两个交换群。其一，F相对于“＋”来说，它是交换群，并且F^+中的每个非 0 元都以某个素数p作为它的阶，即$\forall g \in F^+, g \neq 0,$有$g^p = p \cdot g = 0$，$p$称为域$F$的一个特征。其二，$F^* = F \setminus \{0\}$相对于“×”而言也是交换群。若$F$为$F_p$的$n$次扩张，此时$F = F_q, q = p^n$，即$F$为$p^n$元有限域。此时$|F^*| = q-1$，于是$\forall \alpha \in F^*$，必然有：$\alpha^{q-1} = 1$，也就是$\alpha^q = \alpha$，进一步就是$\alpha^q - \alpha = 0$，于是可以断定有限域$F$中全部$q$个元素都满足方程

$$x^q - x = 0$$

即F中的q个元素的多项式$G(x) = x^q - x$的q个零点。易见，$G(x) \in F_p[x]$，$G(x)$在F中有分解式

$$G(x)=\prod_{\alpha\in F}(x-\alpha)$$

称$G(x)$为有限域F的一揽子多项式。

我们有重要的结论

定理 11：有限域F的乘法群F^*是一个$q-1$阶的循环群。

F^*为循环群意味着存在$\alpha\in F^*$使$F^*=<\alpha>$，此时α称为$q-1$次的本原单位根；同时α也称为有限域F中的本原元。

设α为有限域F中的本原元，则F中任意非零元β都可以表示成为：$\beta=\alpha^k$的形式，其中k称为β对本原元α的指数，记为：$k=ind_\alpha\beta$

同时k也称为以α为底β的对数，也可以记为$k=\log_\alpha\beta$。

注：

1. 对于α来说，β的对数仅在模$q-1$的条件下唯一确定，所以规定 $0\le k\le q-1$。

2. $k=ind_\alpha\beta$这个函数实际上是定义在F^*之上而在整数同余类环Z_{q-1}中取值的一个对数函数，有如下性质：

   (1) $ind_\alpha\beta_1\beta_2=ind_\alpha\beta_1+ind_\alpha\beta_2 \pmod{q-1}$

   (2) $ind_\alpha\beta^k=k\cdot ind_\alpha\beta \pmod{q-1}$

3. 设α为有限域F的一个本原元，则F的非零元素β是本原元的充要条件是$(ind_\alpha\beta,q-1)=1$。

下面的问题是，如何在 F 中找出一个本原元使其成为对数的底？在这里我们已经知道 F 为 F_p 的 n 次扩张，事实上

$F \cong F_p[x]/<f(x)>$， $f(x)$ 为 $F_p[x]$ 中的 n 次不可约多项式

$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$。设 $\alpha=[x]$，有：

$$F=\{k_0\cdot 1+k_1\cdot\alpha+\cdots+k_{n-1}\alpha^{n-1}\mid k_i\in F, i=1,2,\cdots,n-1\}$$

注意，F 中的任意元都为如下一揽子多项式的零点：

$$G(x)=x^{p^n}-x$$

易见，$f(x)\mid G(x)$。$f(x)$ 的零点 $\alpha\in F$；α 的周期就是使等式 $\alpha^t=1$ 成立的最小正整数 t。而这个等式等价于同余式

$$x^t\equiv 1(\mathrm{mod}\, f(x))$$

由于这个事实，把使上式成立的最小正整数称为多项式 $f(x)$ 的周期，记为 $\Pi(f(x))$，当然也视为 $\alpha=[x]$ 的周期，自然有 $t=\Pi\left(f(x)\right)\mid p^n-1$；如果 $t=\Pi\left(f(x)\right)=p^n-1$，则在 F^* 中有 $O(\alpha)=p^n-1$，有 $F^*=<\alpha>$。α 为 F 的本原元，此时称 α 的极小多项式 $f(x)$ 是 $F_p[x]$ 中的本原多项式。

问题是，使得 $F\cong F_p[x]/<f(x)>$ 中的 $f(x)$ 是 n 次不可约多项式，不一定是 n 次本原多项式。为了在这个给定的 F 中找出一个本原元，只能设计一种计算 F 中元素周期的方法，对 F 中的元素累次求它的周期，一旦碰上周期为 p^n-1 的元素 β 就是要找的本原元，它的极小多项式 $m_\beta(x)$ 为 n 次不可约多项式，并且有 $F_p[x]/<f(x)>\cong F_p[x]/<m_\beta(x)>$，进一步有 $F=F(\alpha)=F(\beta)$。

$\forall\beta\in F^*$，易见 $\beta=b_0\cdot 1+b_1\cdot\alpha+\cdots+b_{n-1}\alpha^{n-1}$。我们知 $F_p(\beta)$ 为 F_p 与 F 之间的中间域 $F_p\subseteq F_p(\beta)\subseteq F$，所以 β 在 F_p 上有一个极小多项式 $m(x)$，它是 F_p 上的一个不可约多项式。知

$$F_p(\beta)\cong F_p[x]/<m(x)> \quad \text{它为 } d \text{ 次扩张}$$

由 $[F_p(\beta):F_p]$ 是 $[F:F_p]$ 因子，所以

$$\deg m(x)=d\mid n\Rightarrow p^{\alpha}-1\mid p^n-1$$

求 β 的周期，相当于求使同余式 $x^h\equiv 1(\bmod m(x))$ 成立的最小的正整数 h；注意 $\beta=[x]$，$\Pi\big(m(x)\big)=O(\beta)$。我们知道 $F_p(\beta)$ 的乘法群 $F_p{}^*(\beta)$ 为 F^* 的子群，并且 $\left|F_p^*(\beta)\right|=p^{\alpha}-1$，$d=\deg m(x)$。于是有

$$\Pi\big(m(x)\big)\mid(p^{\deg m(x)}-1)$$

这一结果有助于我们计算 F_p 上不可约多项式的周期，相当于计算 F^* 中元素的周期。给出实际例子如下：

考虑 F_2 上的两个不可约多项式

$$m_1(x)=x^4+x^3+x^2+x+1$$

$$m_2(x)=x^4+x^3+1$$

易验证，它们都为 F_2 上的不可约多项式，有：$2^{\deg m_i(x)}-1=2^4-1=15$（$i=1,2$）。因此，这两个多项式的周期应该为 15 的约数，其中 1 和 3 这两个约数显然是不可能的（为什么？），因此只要讨论 5 和 15 这两个数。由

$$x^5-1=(x-1)(x^4+x^3+x^2+x+1)$$

易见 $x^5 \equiv 1(\bmod m_1(x))$，所以 $\Pi\left(m_1(x)\right)=5$。其次由于

$$x^4 = x^3 + 1(\bmod m_2(x)) \quad \text{以及}$$

$$x^5 \equiv x^4 + x \equiv x^3 + x + 1 \not\equiv 1(\bmod m_2(x))$$

所以，$\Pi\left(m_2(x)\right) \neq 5$，只有 $\Pi\left(m_2(x)\right)=15$。知 $m_2(x)$ 为 F_2 的四次扩张中的本原多项式，$m_2(x)$ 也就是一个四次本原多项式。

定义（本原多项式）：$f(x)$ 为素域 F_p 上的一个 n 次不可约多项式，而 $f(x) \neq x$。如果 $f(x)$ 的周期为 p^n-1，则称 $f(x)$ 为 F_p 上的 n 次本原多项式，简称为本原多项式。

注：素域 F_p 的 m 次扩张 F_{p^m}，若设 $p^m = q$，知 F_{p^m} 为 q 元域，也可以设 $F_{p^m} = F_q$。将 F_q 作为基域，也可以考虑 F_q 上的不可约多项式及其它引起的扩张问题。若 F_q 上的一个 n 次不可约多项式为 q^n-1，同样称 $f(x)$ 为 F_q 上的本原多项式。

下面给出计算 n 次不可约多项式周期的一个方法：

为了说明方便，将域 F 的特征定为 2，即 $char\ F=2$。设 $f(x)\in F_2[x]$，而且 $f(x)$ 在 $F_2[x]$ 上是不可约的，$\deg f(x)=n, F \cong F_2[x]/<f(x)>$。计算 $f(x)$ 的周期：

1. 分解 $2^n-1=q_1,q_2,\cdots,q_w=N$

2. 令 $[x]=\alpha$，**通过第一序列检验**：$N_1=\dfrac{N}{q_1}, N_2=\dfrac{N}{q_2},\cdots,N_w=\dfrac{N}{q_w}$ 检验，来看是

   否有一个整数 k 使得 $\alpha^{N_k} \equiv 1(\bmod f(x))$。如果当 $1 \le k \le s-1$ 时，$\alpha^{N_k} \neq 1$，但

是$\alpha^{N_s}=1$。**通过第二序列：** $N_{s,1}=\dfrac{N_s}{q_{s+1}},N_{s,2}=\dfrac{N_s}{q_{s+2}},\cdots,N_{s,w-s}=\dfrac{N_s}{q_w}$检验，来看下式是否成立：$\alpha^{N_{s,k}}\equiv 1(\bmod f(x))$。如果当$1\le k\le t-1$时$\alpha^{N_{s,k}}\ne 1$但是$\alpha^{N_{s,t}}=1$。通过第三序列：$N_{s,t,1}=\dfrac{N_{s,t}}{q_{s+t+1}},N_{s,t,2}=\dfrac{N_{s,t}}{q_{s+t+2}},\cdots,N_{s,t,w-t-s}=\dfrac{N_{s,t}}{q_w}$检验，来看下式是否成立：$\alpha^{N_{s,t,k}}\equiv 1(\bmod f(x))$，以次类推。最后得知$N_{s,t,\cdots,v}$为$\Pi\left(f(x)\right)$的倍数，而对任意$k\ge 1$来说，$N_{s,t,\cdots,v}$都不是$\Pi\left(f(x)\right)$的倍数。我们算出：$\Pi\left(f(x)\right)=N_{s,t,\cdots,v}$。

下面考虑计算F中元素α的方幂的问题。

计算α的方幂α^M：α为F_2上的n次不可约多项式$f(x)$的零点。首先将α的幂指数M表示成为2进制数：

$$M=2^{h_1}+2^{h_2}+\cdots+2^{h_g}，其中 h_1>h_2>\cdots>h_g$$

从而有：

$$\alpha^M=\alpha^{2^{h_1}}\cdot\alpha^{2^{h_2}}\cdots\cdot\alpha^{2^{h_g}}$$

于是，计算α^M的问题可以归结为计算一系列形如α^{2^h}的幂的问题。如何方便地计算α^{2^h}：

设

$$\alpha^{2^k}=a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1},\quad k=0,1,2,\cdots,n-1,$$

则

$$\left(\alpha^{2^k}\right)^2=\alpha^{2^{k+1}}=a_0+a_1\alpha^2+\cdots+a_{n-1}\alpha^{2(n-1)}$$

$$=(a_0,a_1,\cdots,a_{n-1})\begin{bmatrix}1\\ \alpha^2\\ \vdots\\ \alpha^{2(n-1)}\end{bmatrix}$$

在$0\le k\le n-1$的时候，也容易算出α^{2k}关于基$1,\alpha,\cdots,\alpha^2,\alpha^{n-1}$的表达式：

$$\alpha^{2k}=a_{k,0}+a_{k,1}\alpha+\cdots+a_{k,n-1}\alpha^{n-1}\quad（0\le k\le n-1）$$

记：

$$Q=\begin{bmatrix}a_{00} & a_{01} & \cdots & a_{0n-1}\\ a_{10} & a_{11} & \cdots & a_{1n-1}\\ \vdots & \vdots & \vdots & \vdots\\ a_{n-1\,0} & a_{n-1\,1} & \cdots & a_{n-1\,n-1}\end{bmatrix}$$

知：

$$\begin{bmatrix}1\\ \alpha^2\\ \vdots\\ \alpha^{2(n-1)}\end{bmatrix}=Q\begin{bmatrix}1\\ \alpha\\ \vdots\\ \alpha^{n-1}\end{bmatrix}$$

这样，如果已知α^{2^h}在基$1,\alpha,\cdots,\alpha^{n-1}$下的坐标为$(a_0,a_1,\cdots,a_{n-1})$那么$\alpha^{2^{h+1}}$的坐标便是：

$$(a_0',a_1',\cdots,a_{n-1}')=(a_0,a_1,\cdots,a_{n-1})Q$$

下面我们关心的是有限域F_q上的不可约多项式$f(x)\in F_q[x]$。如果设$\deg f(x)=n$，即$f(x)$为$F_q[x]$中的n次不可约多项式，则$f(x)$可以引起F_q上的n次扩张，使得$f(x)$在F_{q^n}上有n个相异根$\alpha,\alpha^q,\alpha^{q^2},\cdots,\alpha^{q^{n-1}}$。（为什么？请证明。）

定义（共轭）：设 F_{q^n} 是 F_q 的一个扩张。即 $\alpha \in F_{q^n}$，那么元素 $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}$ 被称为相关于 F_q 的 α 共轭系，称 α^{q^i} 是 α^{q^j} 的共轭元素。

注：

1. $\alpha \in F_{q^n}$，α 相关于 F_q 的 n 个共轭元素是两两相异的等价于 α 在 F_q 上的极小多项式的次数为 n。
2. $\alpha \in F_{q^n}$，α 在 F_q 上的极小多项式的次数为 d，此时 $d \mid n$，并且 α 相关于 F_q 的共轭元素 $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}$ 中只有 $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{d-1}}$ 是两两相异的。在前述的共轭元素系列中，每一个元素有 n/d 次重复。
3. $\forall \alpha \in F^*{}_{q^n}$,则 α 相关于 F_q 的全体共轭元在群 $F_{q^n}^*$ 中有相同的周期。
4. $\alpha \in F_{q^n}$，且 α 在 F_q 上的极小多项式的次数为 n，则 F_{q^n} 作为 F_q 的 n 维向量空间有两类重要的基：

   (1) 多项式基：$1, \alpha, \cdots, \alpha^{n-1}$；

   (2) 正规基：$\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}$；

我们注意到对 $\forall \alpha \in F_{q^n}$ 来说，存在 α 在 F_q 上的极小多项式 $f(x) \in F_q[x]$。设 $\deg f(x) = d$，易见 $d \mid n$，（其中 $n = [F_{q^n} : F_q]$），我们称 $g(x) = f(x)^{n/d}$ 为 α 在 F_q 上的特征多项式。$f(x)$ 在 F_{q^n} 中的根为 $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{d-1}}$，它们是两两相异的。我们有：

$$g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

并且：

$$g(x) = f(x)^{n/d} = [(x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{d-1}})]^{n/d}$$

$$= (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{d-1}})(x-\alpha^{q^d})\cdots(x-\alpha^{q^{n-1}})$$

把最后的表达式展开，比较系数可知：

$$\sum_{i=0}^{n-1}\alpha^{q^i} = -a_{n-1} \in F_q$$

我们有

定义（迹函数）：$\forall \alpha \in F_{q^n}$， α 在 F_q 上的迹函数定义为：

$$Tr_{F_{q^n}/F_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}$$

设 $E = F_{q^n}$， $F = F_q$， 则 $Tr_{E/F}(\alpha) = \sum_{i=0}^{n-1}\alpha^{q^i}$ 。

注：

1. 若 $E = F_{p^n}$， $F = F_p$ 为素域，此时 $Tr_{E/F}(\alpha)$ 被称为绝对迹，记为 $Tr(\alpha)$，平时讨论最多的还是相对迹。

2. 由 $\sum_{i=0}^{n-1}\alpha^{q^i} = -a_{n-1} \in F_q$ 可知 Tr 为从扩域 F_{q^n} 到基域 F_q 的一个映射，这是一个十分有意义的映射。

我们有重要的定理

定理 12：设 $K = F_q, F = F_{q^n}$， 那么迹函数 $Tr_{F/K}$ 满足如下特征：

1. $Tr_{F/k}(\alpha+\beta) = Tr_{F/K}(\alpha) + Tr_{F/K}(\beta) \quad ,\forall \alpha,\beta \in F$

2. $Tr_{F/k}(c\cdot\alpha) = cTr_{F/k}(\alpha) \quad ,\forall c \in K, \alpha \in F$

3. 若将 F 和 K 分别视为 K 上的线性空间，则 $Tr_{F/k}$ 是从 F 到 K 上的线性变换；

4. $\forall a \in K$, 有 $Tr_{F/k}(a) = na$；

5. $\forall \alpha \in F$，有 $Tr_{F/k}(\alpha^q) = Tr_{F/k}(\alpha)$

这里仅证明 3，其它的证明留为作业。

证明： $Tr_{F/k}$ 为是从 F 到 K 上的线性变换，只要证明 $\exists \alpha \in F$,使得 $Tr_{F/k}(\alpha) \neq 0$ 即可（原因：$\forall b \in K$, 一定存在 $c \in K$ 使得 $Tr_{F/k}(c\alpha) = b$，取 $c = b / Tr_{F/K}(\alpha)$ 即可）。下面证明这一点。我们知道对于 $\beta \in F$ 有 $Tr_{F/k}(\beta) = 0$ 的充分条件是 β 是 $K[x]$ 中的如下多项式的根：

$$L(x) = x^{q^{n-1}} + x^{q^{n-1}} + \cdots + x^q + x$$

然而，这个多项式在 F 内至多有 q^{n-1} 个相异根，然而 F 中有 q^n 个相异元素，所以必定存在 $\alpha \in F$ 使得 $Tr_{F/k}(\alpha) \neq 0$。得证。

定理 13：设 $F(=F_{q^n})$ 为有限域 $K(=F_q)$ 的 n 次扩张，且 K, F 都视为域 K 上的向量空间，则 F 到 K 上的线性变换全体恰由从 F 到 K 上的如下映射 L_β 构成：

$$\{L_\beta \mid \beta \in F^*, L_\beta(\alpha) = Tr_{F/k}(\beta\alpha), \forall \alpha \in F\}$$

并且在这个集合中，对 $\beta \neq \gamma$ 来说有 $L_\beta \neq L_\gamma$。

证明： 由定理 12 中的 3 知，映射 $L_\beta()\forall\beta\in F^*$ 为从 F 到 K 上的线性变换。对 $\beta,\gamma\in F^*$ 且 $\beta\neq\gamma$ 来说有：

$$L_\beta(\alpha)-L_\gamma(\alpha)=Tr_{F/k}(\beta\alpha)-Tr_{F/k}(\gamma\alpha)=Tr_{F/k}(\beta\alpha-\gamma\alpha)=Tr_{F/k}\big((\beta-\alpha)\alpha\big)$$

注意：$Tr_{F/k}$ 为从 F 到 K 上的线性变换，于是可以适当的选取 $\alpha\in F$，使得 $Tr_{F/k}\big((\beta-\alpha)\alpha\big)\neq 0$，所以 $L_\beta\neq L_\gamma$；这说明 $\{L_\beta\mid\beta\in F^*\}$ 的阶为 $|F|-1=q^n-1$。

另一方面，对于从 F 到 K 上的任意线性变换 φ 来说，取 F 在 K 上的一个基 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 在 φ 下的像唯一确定。$\varphi(\alpha_i)$ 可能取自 K 中的任意元素，有 q 种取法，于是从 F 到 K 上的非 0 的相异的线性变换的个数为 q^n-1。综上所述，从 F 到 K 上的非 0 的线性变换全体刚好为 $\{L_\beta\mid\beta\in F^*\}$。证毕。