original chenyang updated to chapter 13

目录

整数的可除性

素数判断

- **Eratoshenes筛法**
  对任意给定的正整数 N，要求出所有不超过 N 的素数，列出 N 个整数，从中删除不大于 $\sqrt{N}$的所有素数的倍数，将其依次删除，余下的整数就是所要求的不超过 N 的素数
- **整数分解**
  寻求$n = (s+t)(s-t)$

最大公约数

广义欧几里得除法

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}
0	a	b	a/b	$a \mod b$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
n	$\dots$	(a,b)	$\dots$	0

贝祖等式

广义欧几里得除法

j	s_j	t_j	q_{j+1}	r_{j+1}
-3				a
-2	1	0		b
-1	0	1	q_0	r_0
0	s_0	t_0	q_1	r_1
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
n	s_n	t_n	q_{n+1}	$r_{n+1} = 0$

$$\begin{cases} s_j = (-q_j)s_{j-1} + s_{j-2} \\ t_j = (-q_j)t_{j-1} + t_{j-2} \\ q_{j+1} = \left[\frac{r_{j-1}}{r_j}\right] \\ r_{j+1} = (-q_{j+1})r_j + r_{j-1} \end{cases}$$

最大公因数和最小公倍数

- $[a,b] = \frac{a \cdot b}{(a,b)}$
- 多个整数
  - 递归法

- 算术基本定理

线性丢番图方程

$ax+by=c$

> - **STEP1: 判断有解**
>   若$(a,b)\mid c$，则有解
> - **STEP2: 求一个解**
>   贝祖等式得到s和t，则$x_0=\frac{c}{(a,b)}s,y_0=\frac{c}{(a,b)}t$
> - **STEP3: 求所有解**
> $x=x_0+\frac{b}{(a,b)}n,y=y_0-\frac{a}{(a,b)}n$

同余

同余性质

$d\cdot a\equiv d\cdot b\ (\mod m)\Longrightarrow a\equiv b\ (\mod m),(d,m)=1$

$a\equiv b\ (\mod m)\Longrightarrow d\cdot a\equiv d\cdot b\ (\mod d\cdot m),d>0$

$a\equiv b\ (\mod m)\Longrightarrow a/d\equiv b/d\ (\mod m/d),d\mid(a,b,m)$

$a\equiv b\ (\mod m)\Longrightarrow a\equiv b\ (\mod d),d\mid m$

$a\equiv b\ (\mod m_i)\Longrightarrow a\equiv b\ (\mod [m_1,m_2,\cdots,m_k])$

剩余

- **概念解释**

符号/概念	定义
$Z/mZ=\{C_0,C_1,\cdots,C_{m-1}\}$	模m的完全剩余系
$F_p=Z/pZ$	$m=p$为素数
C_a	模m的a的剩余类
剩余	一个剩余类中的任一数
$(Z/mZ)^*=\{C_a\mid 0\le a\le m-1\},(a,m)=1$	简化剩余类
$F_p^*=(Z/pZ)^*$	$m=p$为素数

- **定理**
  - 设m是一个正整数，a是满足$(a,m)=1$的整数。如果k遍历模m的一个简化剩余系，则$a\cdot k$也遍历模m的一个简化剩余系
  - 设m_1,m_2是互素的两个正整数。如果k_1,k_2分别遍历模m_1和模m_2的简化剩余系，则$k_3=m_2\cdot k_1+m_1\cdot k_2$遍历$m_1\cdot m_2=12$的简化剩余系

欧拉函数

设m是一个正整数，则m个整数$1,\cdots,m$中与m互素的整数的个数，记作$\varphi(m)$

- 对于素数幂$m=p^\alpha$，有$\varphi(m)=p^\alpha-p^{\alpha-1}$
- $|(Z/mZ)^*|=\varphi(m)$
- 若$(m,n)=1$，则$\varphi(m\cdot n)=\varphi(m)\cdot\varphi(n)$
- 若$m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$，则$\varphi(m)=m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_s}\right)$
- 若p,q为两个素数，则$\varphi(p\cdot q)=p\cdot q-p-q+1$

- $\sum_{d|m} \varphi(d) = m$

同余定理

- **欧拉定理**
  若$(a, m) = 1$，则$a^{\varphi(m)} \equiv 1 \pmod m$
- **费马小定理**
  若p为素数，则$a^p \equiv a \pmod p$
- **Wilson定理**
  若p为素数，则$(p-1)! \equiv -1 \pmod p$

模重复平方计算法

$b^n \pmod m$

> - **STEP1: 将n写成二进制**
> $n = n_0 + n_1 2 + \cdots + n_{k-1} 2^{k-1}$
> - **STEP2: 计算**
> $a = 1$
> $$\begin{cases} a_0 \equiv a \cdot b^{n_0} \pmod m, b_1 \equiv b^2 \pmod m \\ a_1 \equiv a_0 \cdot b_1^{n_1} \pmod m, b_2 \equiv b_1^2 \pmod m \\ \cdots \\ a_{k-2} \equiv a_{k-3} \cdot b_{k-2}^{n_{k-2}} \pmod m, b_{k-1} \equiv b_{k-2}^2 \pmod m \\ a_{k-1} \equiv a_{k-2} \cdot b_{k-1}^{n_{k-1}} \pmod m \end{cases}$$
> a_{k-1}即为$b^n \pmod m$

RSA加密

利用大整数分解的困难性

- 公钥(加密)：(e, n)
- 私钥(解密)：(d, n)

$n = p \cdot q$，p和q为两个大素数

$(e, \varphi(n)) = 1$

$e \cdot d \equiv 1 \pmod{\varphi(n)}$

> - **加密**
> $E(P) = C \equiv P^e \pmod n$
>   - 准备好p, q，计算$n = p \cdot q, \varphi(n)$
>   - 假设一个与$\varphi(n)$互质的e，求出d
>   - 使用公钥加密信息m：$m^e \equiv c \pmod n$
> - **解密**
> $D(C) = C^d \equiv (P^e)^d \equiv P^{e \cdot d}$
> $\equiv P^{k \cdot \varphi(n)+1} \equiv \left(P^{\varphi(n)}\right) P \equiv P \pmod n$
>   - 求解$c^d \pmod n$

同余式

一次同余式

- **一次同余式有解**
  $a \cdot x \equiv b \pmod m$有解$\Longleftrightarrow (a, m) \mid b$

$x\equiv\frac{b}{(a,m)}\cdot\left(\left(\frac{a}{(a,m)}\right)^{-1}\left(\mod \frac{m}{(a,m)}\right)\right)+t\cdot\frac{m}{(a,m)}(\mod m)$
$t=0,1,\cdots,(a,m)-1$

- **一次同余式求解**

> - **STEP1: 验证有解**
> - **STEP2: 求解** $\frac{a}{(a,m)}\cdot x\equiv 1\left(\mod \frac{m}{(a,m)}\right)$
>   广义欧几里得除法得到特解 $x_0'\equiv c\left(\mod \frac{m}{(a,m)}\right)$
> - **STEP3: 求同余式** $\frac{a}{(a,m)}\cdot x\equiv\frac{b}{(a,m)}\left(\mod \frac{m}{(a,m)}\right)$
>   得到特解 $x_0\equiv\frac{b}{(a,m)}\cdot x_0'\equiv\frac{b}{(a,m)}\cdot c\equiv d\left(\mod \frac{m}{(a,m)}\right)$
> - **STEP4: 写出全部解**
> $x\equiv d+t\cdot\frac{m}{(a,m)}(\mod m),t=0,1,\cdots,(a,m)-1$

同余式组求解

中国剩余定理

$$\begin{cases}x\equiv b_1(\mod m_1)\\ \vdots\\ x\equiv b_k(\mod m_k)\end{cases}$$

> 令 $m=m_1\cdot m_2\cdots m_k=m_i\cdot M_i$
> $M_i'\cdot M_i\equiv 1(\mod m_i),i=1,\cdots,k$
> $x\equiv\sum_{i=1}^{k}b_i\cdot M_i'\cdot M_i(\mod m)$

复杂取模运算简化

$a^n(\mod m)$

> - **STEP1: 分解** m
> $m=m_1\cdots m_k$
> - **STEP2: 欧拉定理**
> $\begin{cases}a^{n_1}\equiv 1(\mod m_1)\\ \vdots\\ a^{n_k}\equiv 1(\mod m_k)\end{cases}\Longrightarrow\begin{cases}a^{n}\equiv b_1(\mod m_1)\\ \vdots\\ a^{n}\equiv b_k(\mod m_k)\end{cases}$
> - **STEP3: 利用 中国剩余定理 求解**
> $a^n\equiv b(\mod m)$

应用

- RSA解密加速
- 残差数字系统

高次同余式

- **高次同余式解数**
  若 $m=m_1\cdots m_k$，则同余式 $f(x)\equiv 0(\mod m)$ 与同余式组
  $\begin{cases}f(x)\equiv 0(\mod m_1)\\ \vdots\\ f(x)\equiv 0(\mod m_k)\end{cases}$
  等价。若 T_i 为同余式 $f(x)\equiv 0(\mod m_i)$ 的解数，则同余式解数 $T=T_1\cdots T_k$
- **高次同余式求解**
  $f(x)\equiv 0(\mod p^\alpha)$

> - **STEP1: 验证有解**
> $x=x_1(\mod p)$ 为 $f(x)\equiv 0(\mod p)$ 的一个解，$(f'(x_1),p)=1$

> - STEP2: 递推
> $x \equiv x_\alpha\ (\bmod\ p^\alpha)$
> $\begin{cases} t_{i-1} \equiv -\frac{f(x_{i-1})}{p^{i-1}} \cdot \left(f'(x_1)^{-1}\ (\bmod\ p)\right)\ (\bmod\ p) \\ x_i \equiv x_{i-1} + t_{i-1} \cdot p^{i-1}\ (\bmod\ p^i) \\ i = 2, \cdots, a \end{cases}$

素数模的同余式简化

$f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0\ (\bmod\ p), a_n \not\equiv 0\ (\bmod\ p)$

> $f(x) = q(x)(x^p - x) + r(x)$
> $f(x) \equiv 0\ (\bmod\ p) \Longleftrightarrow r(x) \equiv 0\ (\bmod\ p)$

二次同余式与平方剩余

二次同余式化简

- **一般二次同余式化简**
  $ax^2 + bx + c \equiv 0\ (\bmod\ m), a \not\equiv 0\ (\bmod\ m)$

> $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$
> $\begin{cases} ax^2 + bx + c \equiv 0\ (\bmod\ p_1^{\alpha_1}) \\ \vdots \\ ax^2 + bx + c \equiv 0\ (\bmod\ p_k^{\alpha_k}) \end{cases}$

- **素数幂的同余式化简**
  $ax^2 + bx + c \equiv 0\ (\bmod\ m), a \not\equiv 0\ (\bmod\ m)$
  p为奇素数，$(2a, p) = 1$

> - STEP1: 两端同时乘以$4a$
> - STEP2: $(2ax + b)^2 \equiv b^2 - 4ac\ (\bmod\ p^\alpha)$
> - STEP3: 令$y = 2ax + b$，有$y^2 \equiv b^2 - 4ac\ (\bmod\ p^\alpha)$

即简化为$x^2 \equiv a\ (\bmod\ m)$的形式

二次剩余

- **定义**
  m为正整数，若$x^2 \equiv a\ (\bmod\ m), (a, m) = 1$有解，则$a$为$m$的二次剩余，否则为二次非剩余
- **欧拉判别条件**
  p为奇素数，$(a, p) = 1$
  - a是模p的平方剩余$\Longleftrightarrow a^{\frac{p-1}{2}} \equiv 1\ (\bmod\ p)$
  - a是模p的非平方剩余$\Longleftrightarrow a^{\frac{p-1}{2}} \equiv -1\ (\bmod\ p)$

  推论:
  - p为奇素数，$(a_1, p) = 1, (a_2, p) = 1$，则$a_1 \cdot a_2$为模$p$的平方非剩余$\Longleftrightarrow a_1, a_2$同为模$p$的平方剩余或平方非剩余
  - 平方剩余与平方非剩余数量相等

Legendre符号

- **定义**
  p为素数
  $\left(\frac{a}{p}\right) = \begin{cases} 1 & a\text{为模}p\text{的平方剩余} \\ -1 & a\text{为模}p\text{的非平方剩余} \\ 0 & p \mid a \end{cases}$

- **欧拉判别法则**
  p为奇素数，对整数a
  $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$
- **性质**
  - $\left(\frac{1}{p}\right) = 1$
  - $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
  - p为奇素数，则
    - $\left(\frac{a+p}{p}\right) = \left(\frac{a}{p}\right)$
    - $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
    - 设$(a,p)=1$，则$\left(\frac{a^2}{p}\right) = 1$
- **高斯引理**
  p为奇素数，a为整数，$(a,p)=1$，整数$a \cdot 1, a \cdot 2, \cdots, a \cdot \frac{p-1}{2}$中模$p$的最小正剩余大于$\frac{p}{2}$的个数是$m$，则$\left(\frac{a}{p}\right) = (-1)^m$

模p平方剩余判断

> - METHOD1: **定理**
>   设p为奇素数
>   - $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
>   - 若$(a,2p)=1$，则$\left(\frac{a}{p}\right) = (-1)^{T_{(a,p)}}$，其中$T_{(a,p)} = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{a \cdot k}{p}\right]$
> - METHOD2: **二次互反律**
>   若p,q为互素奇素数，则$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{p}{q}\right)$

雅可比符号

- **定义**
  设$m = p_1 \cdots p_r$是奇素数p_i的乘积
  $\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right)$
  $\left(\frac{a}{m}\right) = \begin{cases} -1 & 可判断a是模m平方非剩余 \\ 1 & 不可判断a是模m平方剩余 \end{cases}$
- **性质**
  - 若$m = p_1 \cdots p_r$是奇数
    - $\left(\frac{a+m}{m}\right) = \left(\frac{a}{m}\right)$
    - $\left(\frac{a \cdot b}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$
    - 设$(a,m)=1$，则$\left(\frac{a^2}{m}\right) = 1$
    - $\frac{m-1}{2} \equiv \frac{p_1-1}{2} + \cdots \frac{p_r-1}{2} \pmod{2}$
    - $\frac{m^2-1}{2} \equiv \frac{p_1^2-1}{2} + \cdots \frac{p_r^2-1}{2} \pmod{2}$
    - $\left(\frac{1}{m}\right) = 1$
    - $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$
    - $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$
  - 若m,n均为奇数
    - $\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}} \left(\frac{m}{n}\right)$

模平方根

- **模$4k+3$平方根**
  p为形如$4k+3$的素数，求同余式$x^2 \equiv a \pmod{p}$

> - STEP1: **二次互反律验证有解**
> $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \equiv 1 \pmod{p}$

- STEP2: 定理
  解为$x\equiv \pm a^{\frac{p+1}{4}} \pmod p$

- **模$4k+1$平方根**
  p为奇素数，$p-1=2^t\cdot s$，$t\geq 1$，s为奇数，求同余式$x^2\equiv a \pmod p$

- STEP1: 验证有解
- STEP2: 求解b和a^{-1}
  n为模p的平方非剩余，$b=n^s \pmod p$
- STEP3: 求解
  $x_{t-1}\equiv a^{\frac{s+1}{2}} \pmod p$
  $j_{k-1}=\begin{cases} 0 & \left(a^{-1}x_{t-k}^2\right)^{2^{t-k-1}}\equiv 1 \pmod p \\ 1 & \left(a^{-1}x_{t-k}^2\right)^{2^{t-k-1}}\equiv -1 \pmod p \end{cases}$
  $x_{t-k-1}=x_{t-k}b^{j_{k-1}2^{k-1}}$
- x_0为解

- **模m平方根**
  $m=2^\delta\cdot p_1^{\alpha_1}\cdots p_k^{\alpha_k}$

- STEP1: 等价同余式组
  原同余式等价于
  $\begin{cases} x^2\equiv a \pmod{2^\delta} \\ x^2\equiv a \pmod{p_1^{\alpha_1}} \\ \cdots \\ x^2\equiv a \pmod{p_k^{\alpha_k}} \end{cases}$
- STEP2: 求$x^2\equiv a \pmod{p^\alpha}$
  - 求$x^2\equiv a \pmod p$
  - 若$\alpha>1$，使用**高次同余式求解方法**求$x^2-a\equiv 0 \pmod{p^\alpha}$有解的条件及个数
- STEP3: 求$x^2\equiv a \pmod{2^\alpha}$
  - 验证有解
    $\begin{cases} a\equiv 1 \pmod 4 & \alpha=2 \\ a\equiv 1 \pmod 8 & \alpha\geq 3 \end{cases}$
  - 求解
    - $\alpha=2$
      $x\equiv \pm 1 \pmod 4$
    - $\alpha=3$
      $x\equiv \pm 1,\pm 3 \pmod 8$
    - $\alpha\geq 4$
      若同余式$x^2\equiv a \pmod{2^{\alpha-1}}$的解为$x=\pm\left(x_{\alpha-1}+t_{\alpha-1}2^{\alpha-2}\right),t_{\alpha-1}=0,\pm 1,\cdots$
      $x^2\equiv a \pmod{2^\alpha}$的解为
      $x=\pm\left(x_\alpha+t_\alpha 2^{\alpha-1}\right)=\pm\left(x_{\alpha-1}+\left(\frac{a-x_{\alpha-1}^2}{2^{\alpha-1}} \pmod 2\right)\cdot 2^{\alpha-2}+t_\alpha 2^{\alpha-1}\right),t_\alpha=0,\pm 1,\cdots$
      解为$x_\alpha,x_\alpha+2^{\alpha-1},-x_\alpha,-\left(x_\alpha+2^{\alpha-1}\right)$
- STEP4: 利用 **中国剩余定理** 求解

Rabin加密

- STEP1: 生成密钥
  解密者生成2个大素数p,q，计算$n=pq$
  加密者密钥为n，解密者密钥为(p,q)
- STEP2: 加密信息m
  计算$c\equiv m^2 \pmod n$
- STEP3: 解密信息
  求解同余式$\begin{cases} m^2\equiv c \pmod p \\ m^2\equiv c \pmod q \end{cases}$

$x^2+y^2=p$

- STEP1: 求m_0
  寻找$x=x_0$，使得$x^2\equiv -1\pmod p$，存在$y_0=1$使得$x_0^2+y_0^2=m_0\cdot p$
- STEP2:求u_i,v_i
  $u_i\equiv x_i\pmod{m_i}$
  $v_i\equiv y_i\pmod{m_i}$
- STEP3: 求x_i,y_i
  $x_{i+1}=\frac{u_i\cdot x_i+v_i\cdot y_i}{m_i}$
  $y_{i+1}=\frac{u_i\cdot y_i-v_i\cdot x_i}{m_i}$
- STEP4: 求m_i
  $x_i^2+y_i^2=m_i\cdot p$
  当$m_k=1$时，x_k,y_k即为方程的解

原根与指标

指数

- **定义**
  - 指数
    设$m>1$为整数，a是与m互素的正整数，则使得$a^e\equiv 1\pmod m$成立的最小正整数e叫做a对模m的指数，记作$\operatorname{ord}_m(a)$
  - 原根
    若$e=\varphi(m)$，则a为模m的原根
- **定理**
  - $a^d\equiv 1\pmod m\Longleftrightarrow \operatorname{ord}_m(a)\mid d$
  - 设p为奇素数，$\frac{p-1}{2}$为素数，若$a\not\equiv 0,1,-1\pmod p$，则$\operatorname{ord}_p(a)=\frac{p-1}{2}$或$p-1$
  - $b\equiv a\pmod m\Longrightarrow \operatorname{ord}_m(b)=\operatorname{ord}_m(a)$
  - $a^{-1}a\equiv 1\pmod m\Longrightarrow \operatorname{ord}_m\left(a^{-1}\right)=\operatorname{ord}_m(a)$
  - $1=a^0,a,\cdots,a^{\operatorname{ord}_m(a)-1}$
  - $a^d\equiv a^k\pmod m\Longleftrightarrow d\equiv k\pmod{\operatorname{ord}_m(a)}$
  - $\operatorname{ord}_m\left(a^d\right)=\frac{\operatorname{ord}_m(a)}{(d,\operatorname{ord}_m(a))}$
  - 设g为模m的原根，则g^d为模m的原根$\Longleftrightarrow (d,\varphi(m))=1$
  - 设$k\mid \operatorname{ord}_m(a)$，则使得$\operatorname{ord}_m\left(a^d\right)=k,1\le d\le \operatorname{ord}_m(a)$成立的正整数$d$满足$\frac{\operatorname{ord}_m(a)}{k}\mid d$，且共有$\varphi(k)$个这样的$d$
  - 模m有原根$\Longrightarrow$模m有$\varphi(\varphi(m))$个不同的原根
  - $(\operatorname{ord}_m(a),\operatorname{ord}_m(b))=1\Longleftrightarrow \operatorname{ord}_m(a\cdot b)=\operatorname{ord}_m(a)\cdot\operatorname{ord}_m(b)$
- **求指数**

> 根据$a^d\equiv 1\pmod m\Longleftrightarrow \operatorname{ord}_m(a)\mid d$，求出$m$的因数，挨个验证

原根

- **定理**
  - 模p原根
    - p为奇素数$\Longrightarrow$模p的原根存在，且有$\varphi(p-1)$个
    - g是模p的原根$\Longleftrightarrow g^{p-1}\not\equiv 1\pmod{p^2}$或$(g+p)^{p-1}\not\equiv 1\pmod{p^2}$
  - 模p^α原根
    - 若p为奇素数，则g为模p原根，$g^{p^{k-2}(p-1)}=1+u_{k-2}\cdot p^{k-1},(u_{k-2},p)=1\Longrightarrow g$为模$p^k$原根
    - g为模p原根$\Longrightarrow g$或$g+p$为模p^2原根
    - g为模p^2原根$\Longrightarrow g$为模p^α原根
    - g为模p^α原根$\Longrightarrow g$与$g+p^\alpha$中的奇数为模$2p^\alpha$原根
- **求奇素数p原根**

> - STEP1: 求一个原根g
>   求出$p-1$的所有素因数$q_1,\cdots,q_s$，则g是模p的原根$\Longleftrightarrow \forall i,g^{\frac{p-1}{q_i}}\not\equiv 1\pmod p$
> - STEP2: 求所有原根
>   对于$(d,\varphi(m))=1$，g^d为原根

- **求p^α原根**

- **STEP1: 求p的一个原根g**
- **STEP2: 求p^α的原根**
  - 若$g^{p-1} \not\equiv 1 \pmod{p^2}$，则$g$为原根
  - 若$(g+p)^{p-1} \not\equiv 1 \pmod{p^2}$，则$g+p$为原根

- **求$2p^\alpha$原根**

- **STEP1: 求p^α的一个原根g**
- **STEP2: 求$2p^\alpha$的原根**
  g与$g+p^\alpha$中的奇数为原根

- 模m存在原根$\Longleftrightarrow m = 2, 4, p^\alpha, 2p^\alpha$

指标

- **定义**
  设$m > 1$为整数，a是与m互素的正整数，g为模m的一个原根，则存在唯一的$1 \le r \le \varphi(m)$，使得$g^r \equiv a \pmod{m}$，记作$r = \mathrm{ind}_g a$
- **定理**
  - 整数r满足$g^r \equiv a \pmod{m} \Longrightarrow r \equiv \mathrm{ind}_g a \pmod{\varphi(m)}$
  - 以g为底的对模m有相同指标r的所有整数全体是模m的一个简化剩余类
  - $\mathrm{ind}_g a_1 \cdots a_n \equiv \mathrm{ind}_g a_1 + \cdots + \mathrm{ind}_g a_n \pmod{\varphi(m)}$
  - $\mathrm{ind}_g a^n \equiv n \cdot \mathrm{ind}_g a \pmod{\varphi(m)}$

n次同余式

- **定义**
  设$m > 1$为整数，a是与m互素的正整数，若$x^n \equiv a \pmod{m}$有解，则a为对模m的n次剩余
- **求解$x^n \equiv a \pmod{m}$**

- **STEP1: 验证有解**
  $(n, \varphi(m)) \mid \mathrm{ind}_g a$，$g$为模$m$的原根
  解数为$(n, \varphi(m))$
- **STEP2: 等价同余式**
  等价于$n \mathrm{ind}_g x \equiv \mathrm{ind}_g a \pmod{\varphi(m)}$
- **STEP3: 查指标表解出$n \mathrm{ind}_g x$，解出$x \pmod{m}$**

- **求解$n^x \equiv a \pmod{m}$**

- **STEP1: 等价同余式**
  等价于$x \mathrm{ind}_g n \equiv \mathrm{ind}_g a \pmod{\varphi(m)}$
- **STEP2: 查指标表解出$x \pmod{\varphi(m)}$**

ElGamal加密

利用离散对数对大素数取模计算的困难性

- **STEP1: 获取密钥(p, r, b)**
  - p: 选择一个素数p
  - r: p的原根为r
  - a: 选取整数a，$0 \le a \le p-1$
  - b: $b \equiv r^a \pmod{p}$
- **STEP2: 加密信息M**
  - k: 选取整数k，$1 \le k \le p-2$
  - γ: $\gamma \equiv r^k \pmod{p}, 0 \le \gamma \le p-1$
  - δ: $\delta \equiv M \cdot b^k \pmod{p}, 0 \le \delta \le p-1$

- STEP3: 解密信息(γ, δ)
  $M \equiv \overline{\gamma^a}\delta \pmod p$

素性检验

伪素数和Fermat素性检验

- **判断素数**
  n为素数$\Longleftrightarrow$对任意$b, (b,n)=1$，$b^{n-1} \equiv 1 \pmod n$或$\mathrm{ord}_n(b) \mid n-1$
- **n对基b的伪素数**
  n为奇合数，$(b,n)=1$，$b^{n-1} \equiv 1 \pmod n$
  - 存在无穷个对基2的伪素数
  - 若n为对基b_1, b_2的伪素数，则n为对基$b_1 \cdot b_2$的伪素数
  - 若n为对基b的伪素数，则n为对基b^{-1}的伪素数
  - 若存在b使得$b^{n-1} \not\equiv 1 \pmod n$，则模$n$的简化剩余系中至少有一半的的数满足$b^{n-1} \not\equiv 1 \pmod n$
- **Fermat素性检验**

> - STEP1: 随机选取整数b和安全参数t
> - STEP2: 计算$r \equiv b^{n-1} \pmod n$
> - STEP3: 若$r \neq 1$，则n为合数
> - STEP4: 重复t次

- **Carmichael数**
  合数n满足对任意$b, (b,n)=1$，$b^{n-1} \equiv 1 \pmod n$
  存在无穷多个Carmichael数
- **证明n为Carmichael数**

> - STEP1: $n = p_1 \cdots p_s$
> - STEP2: $b^{p_i - 1} \equiv 1 \pmod{p_i}$
> - STEP3: $b^{n-1} \equiv 1 \pmod{p_i}$

Euler伪素数和Solovay-Stassen素性检验

- **n对基b的Euler伪素数**
  n为奇合数，$(b,n)=1$，$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod n$
  - 若n对基b的Euler伪素数，则n对基b的伪素数
- **Solovay-Stassen素性检验**

> - STEP1: 随机选取整数$b, 2 \le b \le n-2$和安全参数t
> - STEP2: 计算$r \equiv b^{\frac{n-1}{2}} \pmod n$
> - STEP3: 若$r \neq 1$且$r \neq n-1$，则n为合数
> - STEP4: 计算$s = \left(\frac{b}{n}\right)$
> - STEP5: 若$r \neq s$，则n为合数
> - STEP6: 重复t次

强伪素数和Miller-Rabin Primality素性检验

- **n对基b的强伪素数**
  n为奇合数，$(b,n)=1$，$n-1=2^s t$，t为奇数，$b^t \equiv 1 \pmod n$或存在$0 \le r < s$使得$b^{2^r t} \equiv -1 \pmod n$
  - 存在无穷个对基2的强伪素数
  - 若n对基$b\,(1 \le b \le n-1)$的强伪素数可能性至多为25
- **Miller-Rabin Primality素性检验**

> - STEP1: 安全参数k，$n-1=2^s t, t$为奇数

- STEP2: 随机选取整数$b, 2 \leq b \leq n-2$
- STEP3: 计算$r_0 \equiv b^t \pmod n$
  - 若$r_0 = 1$或$r_0 = n-1$，则通过检验，可能为素数。回到第二步
  - 否则进入下一步
- STEP3: 计算$r_1 \equiv r_0^2 \pmod n$
  - 若$r_1 = n-1$，则通过检验，可能为素数。回到第二步
  - 否则进入下一步
- STEP4: 计算$r_2 \equiv r_1^2 \pmod n$
  $\dots$
- STEPs+1: 计算$r_{s-1} \equiv r_{s-2}^2 \pmod n$
  - 若$r_{s-1} = n-1$，则通过检验，可能为素数。回到第二步
  - 否则n为合数
    k次测试后，n为合数的概率为0.25^k

梅森素数和Lucas-Lehmer Primality素性检验

- **梅森素数**
  $M_m = 2^m - 1$为梅森数
  若p为素数且$M_p = 2^p - 1$为素数，则M_p为梅森素数
- **LLT**

> 设p为素数
> $r_k = r_{k-1}^2 - 2 \pmod{M_p}, 0 \leq r_k \leq M_p$，其中$r_1 = 4, k \geq 2$
> $r_{p-1} \equiv 0 \pmod{M_p} \iff M_p$

随机数生成

> - METHOD1: **线性同余法**
>   - 选取种子x_0
>   - 选取m, a, c，使得$2 \leq a < m, 0 \leq c < m, 0 \leq x_0 \leq m$
>   - $x_{n+1} \equiv a \cdot x_n + c \pmod m$
> - METHOD2: **纯乘法同余法**
>   - 选取素数m（通常为梅森素数$M_{31} = 2^{31} - 1$），a取其原根，最大周期长度为$m-1$
>   - $x_{n+1} \equiv a \cdot x_n \pmod m$
> - METHOD3: **平方伪随机**
>   - $x_{n+1} \equiv x_n^2 + 1 \pmod m$

群

群和子群

- **群的定义**

> 非空集合G满足
> - G1: **结合律** $\forall a, b, c \in G, (ab)c = a(bc)$
> - G2: **单位元** $\exists e \in G, \forall a \in G, ae = ea = a$
> - G3: **可逆性** $\forall a \in G, \exists a^{-1} \in G, aa^{-1} = a^{-1}a = e$

- **Abel群/交换群**
  群G满足
  - G4: **交换律** $\forall a, b \in G, ab = ba$
- **定义和性质**

- 群G的元素个数叫做群G的阶，记作$|G|$
- 单位元唯一
- 逆元唯一
- $(a_1a_2\cdots a_n)^{-1}=a_n^{-1}\cdots a_2^{-1}a_1^{-1}$
- $a^ma^n=a^{m+n}$，$(a^m)^n=a^{mn}$
- $x,y\in G$，G为Abel群，$(xy)^n=x^ny^n$
- $\begin{cases}ax=b\\ya=b\end{cases}$在$G$中有解，$G$满足结合律$\Longleftrightarrow G$为一个群

- **子群**
  - 定义
    - 子群：H为G的一个子集，H为一个群，记作$H\leq G$
    - 平凡子群：$H=\{e\}$和$H=G$
    - 真子群：H不是平凡子群
  - 性质
    - $H\leq G\Longleftrightarrow\begin{cases}H\text{是满足}G\text{下的封闭二元运算}\\G\text{的单位元在}H\text{内}\\\forall a\in H,a^{-1}\in H\end{cases}$
    - $H\leq G\Longleftrightarrow\forall a,b\in H,ab^{-1}\in H$
    - $H_1,H_2\leq G\Longrightarrow H_1\cap H_2\leq G$
  - 生成
    - X为G子集，设$\{H_i\}_{i\in I}$为G的包含X的所有子群，则$\cap_{i\in I}H_i$为G的由X生成的子群，记作$<X>$
      - X的元素为$<X>$生成元
      - 若$G=<a_1,\cdots,a_n>$，则G为有限生成的
      - 若$G=<a>$，则G为a生成的循环群
    - G为交换群，$X=<a_1,\cdots,a_t>$，$<X>=\begin{cases}\{a_1^{n_1}\cdots a_t^{n_t}\mid a_i\in X,n_i\in Z,1\leq i\leq t\} & G\text{为乘法群}\\\{n_1a_1\cdots n_ta_t\mid a_i\in X,n_i\in Z,1\leq i\leq t\} & G\text{为加法群}\end{cases}$，
      特别的，$\forall a\in G,<a>=\begin{cases}\{a^n\mid n\in Z\} & G\text{为乘法群}\\\{na\mid n\in Z\} & G\text{为加法群}\end{cases}$

> $(Z_m,+)$的所有子群
>
> - 对$n\neq m$且$n\mid m$，$<n>$为子群
> - $<0>=\{0\}$

> 乘法群Z_p^*的所有子群和生成元
>
> - **STEP 1:** $p-1=q_1\cdots q_s$，模p原根为g
> - **STEP 2:**
>   - $<g>$生成$p-1$阶子群
>   - $<g^{q_i}>$生成$\frac{p-1}{q_i}$阶子群
>   - $<1>=\{1\}$

> Z/nZ^*的所有生成元
>
> - **STEP 1:** 模n原根为g
> - **STEP 2:** 求所有d，$(d,\varphi(n))=1$
> - **STEP 3:** 生成元为g^d

正规子群和商群

- **陪集**
  - 定义
    设H为G的子群，a为G中的任意元，则$aH=\{ah\mid h\in H\}$为G中的左陪集，$Ha=\{ha\mid h\in H\}$为右陪集
    aH中的元素叫aH的代表元
    若$aH=Ha$，则aH为G中H的陪集
  - 定理
    - $\forall a\in G,aH=\left\{c\mid c\in G,a^{-1}c\in H\right\},Ha=\left\{c\mid c\in G,ca^{-1}\in H\right\}$
    - $\forall a,b\in G,aH=bH\Longleftrightarrow b^{-1}a\in H$
    - $\forall a,b\in G,aH\cap bH=\emptyset\Longleftrightarrow b^{-1}a\notin H$

- $\forall a \in H, aH = H = Ha$

> 群$(Z_{ha}, +)$子群$< a >$的所有陪集
>
> STEP 1: $< a >$生成子群$\{0, a, 2a, \cdots, (h-1)\,a\}$
>
> STEP 2: 陪集为$\{m+0, m+a, m+2a, \cdots, m+(h-1)\,a\}, m = 0, \cdots, a-1$

- **商集**
  - 定义
    $G/H = \{aH \mid a \in G\}$
    G/H中左（右）陪集的个数叫做H在G中的指标，记作$[G : H]$
  - 拉格朗日定理
    $H \le G \Longrightarrow |G| = [G : H]\,|H|$
    $K, H \le G, K \le H \Longrightarrow [G : K] = [G : H]\,[H : K]$
- **正规子群**
  $H \le G, H$满足$\forall a \in G, aH = Ha$
- **商群**
  N为G的正规子群，$(aN)\,(bN) = (ab)\,N$，G/N构成一个商群

> $m+ < a >$在$Z_{ka}/ < a >$里的阶
>
> - 写出$< a >$
> - $(m+ < a >) \cdot \operatorname{ord}(m+ < a >) =< a >$

同态和同构

- **定义**
  - 同态：$f : G \to G', \forall a, b \in G, f\,(ab) = f\,(a)\,f\,(b)$
  - 单同态：f为单射
  - 满同态：f为满射
  - 同构：f为双射，记作$f : G \cong G'$
  - 自同态：$G = G'$
  - 像：$f : X \to Y, A \subseteq X, B \subseteq Y, A$在$Y$中的像$f\,[A]$为$\{f\,(a) \mid a \in A\}$
  - 逆像：B在X中的逆像$f^{-1}[B]$为$\{x \in X \mid f\,(x) \in B\}$
  - 核/核子群：$\ker(f) = f^{-1}[\{e'\}] = \{x \in G \mid f\,(x) = e'\}$

> 同态映射$f : Z \to (Z_p, +)$，$\ker(f) =< pZ >$

- 像子群：$g\,(G)$

  核子群即由G中所有能通过f映射成为G'中的单位元的元素所组成的集合
  像子群即G中所有元素通过f映射后组成的集合
- **性质**
  - f为G到G'的同态（同构），g为G'到G''的同态（同构）$\Longrightarrow f \circ g$为$G$到$G''$的同态（同构）
  - f为G到G'的同态
    - $f\,(e) = e'$
    - $\forall a \in G, f\left(a^{-1}\right) = f^{-1}(a)$
    - $\ker(f) \le G$且f为单同态$\Longleftrightarrow \ker(f) = \{e\}$
    - $H' \le G' \Longrightarrow f^{-1}(H') \le G$
- **证明$f : G \to G'$同构**

> - STEP1: **f为同态映射**
>   证明$f : G \to G', \forall a, b \in G, f\,(ab) = f\,(a)\,f\,(b)$
> - STEP2: $\ker(f) = \{e\}$**或f为单射**
>   证明$f\,(m) = f\,(n) \Longrightarrow m = n$
> - STEP3: **f为满射**
>   证明$m = f^{-1}(n), f\,(m) = n$

- **同态分解定理**

- 自然同态
  $f:G\to G'$同态$\Longrightarrow \ker(f)$为G的正规子群
  N为G的正规子群$S:G\to G/H(a\to aN)$是核为N的同态，S为自然同态
- 同态基本定理
  $f:G\to G'$同态$\Longrightarrow$ $\exists$唯一$G/\ker(f)\to f(G)$同构$\bar{f}:a\ker(f)\to f(a)$ $f=i\circ\bar{f}\circ s$，其中s为$G\to G/\ker(f)$自然同态，$i:c\to c$为$f(G)\to G'$恒等同态
  $s:G\to G/N$同态$\Longrightarrow \forall a\in G, f(a)=\bar{f}\circ s(a)$

循环群

- **定义**
  若$\exists a\in G, G=<a>$，则G为循环群，a为G的生成元
  使等式$a^n=e$成立的最小正整数n称为a的阶，记为$\operatorname{ord}(a)$
  若a为n阶元，则n阶循环群$G=\{a^0=e,a^1,a^2,\cdots,a^{n-1}\}$
- **定理**
  - 加群Z的每个子群H都是循环群，且$H=<0>$或$H=<m>=mZ$, m为H中的最小正整数
  - 每一个无限循环群同构于加群Z，每一个阶为m的有限循环群同构于加群Z/mZ
  - $m=\operatorname{ord}(a)$
    - $a^k=e\Longleftrightarrow m\mid k$
    - $a^r\equiv a^k\Longleftrightarrow r\equiv k\pmod m$
    - $\forall 1\le d\le m, \operatorname{ord}(a^d)=\frac{m}{(d,m)}$
  - 循环群的子群是循环群
  - G为循环群，G的生成元为$\begin{cases}a和a^{-1} & G是无限的\\ a^k,(k,m)=1 & G是有限的\end{cases}$
  - 若G为乘法群$(Z_m,\cdot)$，则生成元a为模m的原根，G中共有$m-1$个元素
  - 若G为有限交换群，则$\exists a_1,\cdots,a_n\in G, \operatorname{ord}(a_{i+1})\mid\operatorname{ord}(a_i), 1\le i\le s-1, G=<a_1,\cdots,a_s>$

置换群

- **n元置换**

> 设$S=\{1,\cdots,n\}, \sigma:S\to S, k\to\sigma(k)=i_k$，表示为$\sigma=\begin{pmatrix}1&2&\cdots&n-1&n\\ i_1&i_2&\cdots&i_{n-1}&i_n\end{pmatrix}$

- $\sigma^{-1}=\begin{pmatrix}i_1&i_2&\cdots&i_{n-1}&i_n\\ 1&2&\cdots&n-1&n\end{pmatrix}$
- 若S中部分元素$\{i_1,\cdots,i_k\}$满足$\sigma(i_1)=i_2,\sigma(i_2)=i_3,\cdots,\sigma(i_k)=i_1$，则称为k-轮变换，简称轮换，记作$\sigma=(i_1,\cdots,i_k)$
  - $k=1$时为恒等置换
  - $k=2$时为对换
  - $\sigma=(i_1,\cdots,i_k), \tau=(j_1,\cdots,j_l)$，若$k+l$个元素均不相同，则$\sigma,\tau$不相交
  - 任意一个置换都可以表示为一些不相交轮换的乘积，且表达式唯一
  - k-轮换可以表示为2-轮换，$(a_1\cdots,a_k)=(a_1,a_k)(a_1,a_{k-1})\cdots(a_1,a_2)$
- **置换群**
  n元置换全体组成的集合S_n置换的乘法构成n元置换群，阶为$n!$
  设G为n元群，则G同构一个n元置换群

环与域

环

- **定义**

> 若$<R,+>$构成交换群，$<R,\cdot>$构成半群（$\forall a,b,c\in R,(ab)c=a(bc)$），$\cdot$关于$+$适合分配律（$\forall a,b,c\in R,(a+b)c=ac+bc, a(b+c)=ab+ac$），则$<R,+,\cdot>$为环

- 交换环：$\forall a,b\in R, a\cdot b=b\cdot a$

- 含幺环：$\exists e=1_R,\forall a\in R,a\cdot 1_R=1_R\cdot a=a$
- 非零元a为左零因子：$\exists b\in R,b\neq 0,ab=0$
    - 零因子：a同时为左零因子和右零因子，R为零因子环
- a为左逆元：$\exists b\in R,ab=1_R$
    - 逆元：a同时为左逆元和右逆元
- 整环：R为交换环、含幺环、无零因子环
- **性质**
    - $\forall a\in R,0a=a0=0$
    - $\forall a,b\in R,(-a)\,b=a\,(-b)=-ab$
    - $\forall a,b\in R,(-a)\,(-b)=ab$
    - $\forall n\in Z,\forall a,b\in R,(nab)=a\,(nb)=nab$
    - $\forall a_i,b_j\in R,\left(\sum\limits_{i=1}^{n}a_i\right)\left(\sum\limits_{j=1}^{n}b_j\right)=\sum\limits_{i=1}^{n}\sum\limits_{j=1}^{n}a_ib_j$

环与域

- **域**
  整环R满足$\forall a\in R^*=R-\{0\}\,,a^{-1}\in R$
- **交换环上的整除**
  设R为交换环，$a,b\in R,b\neq 0$，若$c\in R,a=cb$，则称作b整除a，记作$b\mid a$，a为b的倍元，b为a的因子
    - 若b,c均不为单位元，则b是a的真因子
    - $p\in R$，若p不是单位元，且没有真因子，则p为不可约元/素元
    - $a,b\in R$，若$\exists u\in R,a-ub$，则a,b为相伴的
- **环的同态与同构**
  R,R'为两个环，$f:R\to R'$
    - 环同态
        - $\forall a,b\in R,f\,(a+b)=f\,(a)+f\,(b)$
        - $\forall a,b\in R,f\,(ab)=f\,(a)\,f\,(b)$
    - 同构
      f为满射
- **特征和素域**
    - > R为环，若$\exists p_{min}\in\mathbb{Z}^*,\forall a\in R,pa=0$，则$R$的特征为$p$，若不存在，则为$0$
      >
      > p为素数
      >
      > - $\forall a,b\in R,(a+b)^p=a^p+b^p$
    - 设p为素数，$f\,(x)=a_nx^n+\cdots+a_1x+a_0$，$f\,(x)^p\equiv f\,(x^p)\,(\mod p)$
    - 若一个域不含真子域，则其为素域
        - 设F为域，若F特征为0，则F有一个与Q同构的域；若F特征为p，则F有一个与F_p同构的域，F_p为在Z_p运算下的域
- **理想和商环**
    - I为R的子环，若$\forall r\in R,\forall a\in I,ra\in I$，则$I$为$R$的左理想
      若同时为左理想和右理想，则为理想
        - $\{0\}\,,R$均为R的平凡理想
        - P为R的理想，若$P\neq R,\forall A,B,AB\in P\implies A\in P\vee B\in P$，则$P$为$R$的素理想
        - M为R的理想，若$M\neq R,\forall$理想$N,M\subset N\in R\implies N=N\vee N=R$，则$M$为$R$的极大理想
        - 整环Z或含幺环R的每一个素理想都是极大理想
        - R为含幺交换环，M为R的理想，则M为极大理想或素理想$\iff R/M$为域
        - 若R为环，I为R的理想，则R/I对加法运算$(a+I)+(b+I)=(a+B)+I$和乘法运算$(a+I)\,(b+I)=ab+I$构成一个环
          当R为交换环或含幺环时，R/I也为交换环或幺环
    - 群G的正规子群H将G分为若干陪集，相似的，环R的理想I将R分为不相交的陪集
    - $f:R\to R'$为同态$\implies\ker\,(f)$为R的理想
      I为环R的理想$\implies S:R\to R/I,a\to a+I$为核为$I$的同态
    - 同态基本定理：
      R为环，$f:R\to R'$为同态$\implies\exists$唯一$R/\ker\,(f)$到像子环$f\,(R)$同构$\bar{f}:a+\ker\,(f)\to f\,(a)\,,f=i\circ\bar{f}\circ s$，其中$s$为$R$到商环$R/\ker\,(f)$的自然同态，$i:c\to c$为$f\,(R)$到$R'$的恒等同态

多项式环

- **定义**
  R为整环，x为变量，R上的多项式记作$R[x]=\{f(x)=a_nx^n+\cdots+a_1x+a_0 \mid a_i\in R, 0\le i\le n, n\in R\}$
  对于多项式加法和乘法，$R[x]$为整环
- **多项式整除和不可约多项式**
  - $g(x)\mid f(x)$：$\exists q(x), f(x)\mid q(x)\cdot g(x)$
  - $g(x), h(x)\ne 0, g(x)\mid f(x), h(x)\mid g(x)\Longrightarrow h(x)\mid f(x)$
    - $g(x), h(x)\ne 0, g(x)\mid f(x), h(x)\mid g(x)\Longrightarrow \forall s(x), t(x), h(x)\mid s(x)\cdot f(x)+t(x)\cdot g(x)$
    - 不可约多项式：除1和$f(x)$外，$f(x)$没有其他非常数因式，否则$f(x)$为合式
  - 设$f(x)$是域K上的n次可约多项式，$p(x)$是$f(x)$的次数最小的非常数饮食，则$p(x)$一定是不可约多项式，且$\deg p\le\frac{1}{2}\deg f$
  - 设$f(x)$是域K上的n次可约多项式，若$\forall$不可约多项式$p(x), \deg p\le\frac{1}{2}\deg f, p(x)\nmid f(x)$，则$f(x)$为不可约多项式
- **多项式欧几里得除法**
  - 设整环R上两个多项式$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0, g(x)=x^m+\cdots+b_1x+b_0$，则存在$q(x), r(x), f(x)=q(x)\cdot g(x)+r(x)$
    $q(x)$为不完全商，$r(x)$为余式
    - 对于$f(x)$有$a\in R$，存在$q(x)$和常数$c=f(a), f(x)=q(x)(x-a)+f(a)$
    - 对于$f(x)$有$a\in R$，$x-a\mid f(x)\Longleftrightarrow f(a)=0$
    - $g(x)\mid f(x)\Longleftrightarrow r(x)=0$
  - 最大公因式：$f(x), g(x), d(x)\in R[x]$
    - $d(x)\mid f(x), d(x)\mid g(x)$
    - $h(x)\mid f(x), h(x)\mid g(x)\Longrightarrow h(x)\mid d(x)$
      则$d(x)$为最大公因式，记作$(f(x), g(x))$
      若$(f(x), g(x))=1$，则$f(x)$和$g(x)$互质

求最大公因式（广义欧几里得除法）
假设$\deg f<\deg g$

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}
0	$g(x)$	$f(x)$	$g(x)/f(x)$	$g(x) \mod f(x)$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
n	$\cdots$	$(g(x), f(x))$	$\cdots$	0

- 设域K上两个多项式$f(x), g(x)$，则存在$q(x), h(x)\in K[x], f(x)=q(x)\cdot g(x)+h(x), \deg h<\deg g$
  - $(f(x), g(x))=(g(x), h(x))$
- 设域K上两个多项式$f(x), g(x)$，$\deg g\ge 1, (f(x), g(x))=r_k(x), r_k(x)$为广义欧几里得除法中最后一个非零余式

$$s_k(x)\cdot f(x)+t_k(x)\cdot g(x)=(f(x), g(x))$$
$$\begin{cases} s_{-2}(x)=1\\ s_{-1}(x)=0\\ t_{-2}(x)=0\\ t_{-1}(x)=1\\ s_j(x)=(-q_j(x))s_{j-1}(x)+s_{j-2}(x)\\ t_j(x)=(-q_j(x))t_{j-1}(x)+t_{j-2}(x)\end{cases}$$

- **多项式同余**
  - 给定$K[x]$中一个首一多项式$m(x)$，若$m(x)\mid f(x)-g(x)$，则$f(x)\equiv g(x)\pmod{m(x)}$
    - $\forall a(x), a(x)\equiv a(x)\pmod{m(x)}$
    - $a(x)\equiv b(x)\pmod{m(x)}\Longrightarrow b(x)\equiv a(x)\pmod{m(x)}$
    - $a(x)\equiv b(x), b(x)\equiv c(x)\pmod{m(x)}\Longrightarrow a(x)\equiv c(x)\pmod{m(x)}$
    - $$a_1(x)\equiv b_1(x), a_2(x)\equiv b_2(x)\pmod{m(x)}\Longrightarrow a_1(x)+a_2(x)\equiv b_1(x)+b_2(x), a_1(x)\cdot a_2(x)\equiv b_1(x)\cdot b_2(x)\pmod{m(x)}$$
  - $a(x)\equiv b(x)\pmod{m(x)}\Longleftrightarrow a(x)=b(x)+s(x)\cdot m(x)$
  - $r(x)$为$f(x)$模$m(x)$的最小余式
  - 构造有限域：设K为一个域，$p(x)$为$K[x]$中的不可约多项式，则商环$K[x]/p(x)$对于加法式和乘法式构成一个域

- **本原多项式**
  - 设p为素数，$p(x)$是$F_p[x]$中的n次不可约多项式，则$F_p[x]/p(x)=\{a_{n-1}x^{n-1}+\cdots+a_1x+a_0 \mid a_i\in F_p\}$记作$F_{p^n}$，这个域元素个数为$p^n$
  - 设p为素数，$f(x)$为$f_p[x]$中的n次多项式，则使得$x^e\equiv 1(\mod f(x))$成立的最小正整数e叫做$f(x)$在F_p上的指数，记作$\operatorname{ord}_p(f(x))$
    - 整数d使得$x^d\equiv 1(\mod f(x))$,则$\operatorname{ord}_p(f(x))\mid d$
    - $g(x)\mid f(x)\Longrightarrow \operatorname{ord}_p(f(x))\mid d$
    - $(f(x),g(x))=1\Longrightarrow \operatorname{ord}_p(f(x)\cdot g(x))=[\operatorname{ord}_p(f(x)),\operatorname{ord}_p(g(x))]$
    - $f(x)$为$F_p[x]$上的n次不可约多项式，则$\operatorname{ord}_p(f(x))\mid p^n-1$
  - 若$\operatorname{ord}_p(f(x))=p^n-1$，则称$f(x)$为$F_p$上的本原多项式
  - 设p为素数，$f(x)$为$F_p[x]$上的本原多项式，则$f(x)$是$F_p[x]$上的不可约多项式

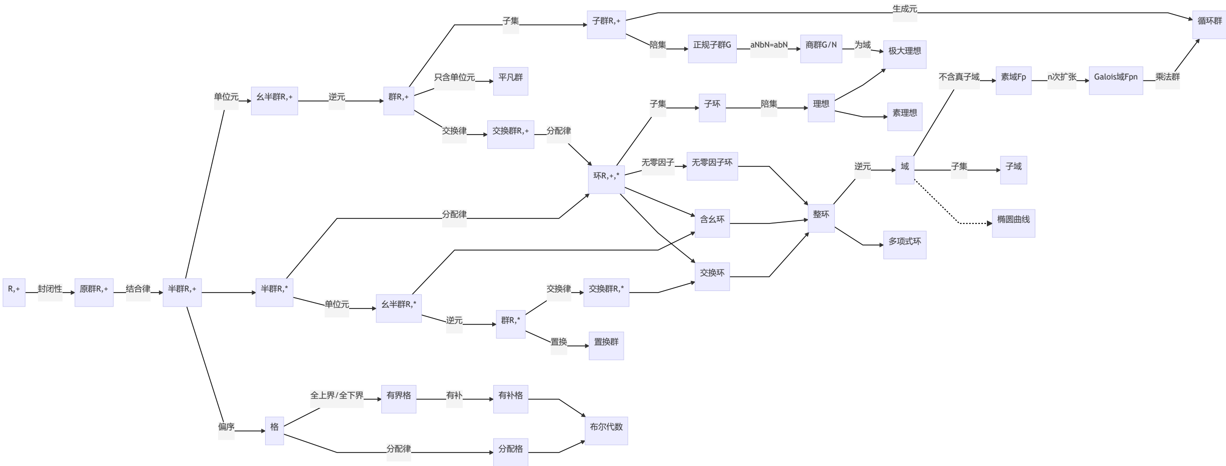
> **判别本原多项式**
>
> 设p为素数，n为正整数，$f(x)$是$F_p[x]$中的n次多项式，若$x^{p^n-1}\equiv 1(\mod f(x))$，对于$p^n-1$的所有不同素因数$q_1,\cdots,q_s$，$x^{\frac{p^n-1}{q_i}}\not\equiv 1(\mod f(x)),i=1,\cdots,s$，则$f(x)$是$n$次本原多项式

有限域

- **域的扩张**
  - 设F为一个域，如果K是F的子域，则称F为K的扩域
  - F为域K的一个扩张，将F看成K上的向量空间，若是有限维的，则称F为K的有限维扩张，K上向量空间F的维数称为扩张次数，记为$[F:K]$
  - 设R为一个整环，K是包含R的一个域，F是K的扩张
    - F的元素u称为R上的代数数，若存在一个非零多项式$f\in R[x]$使得$f(u)=0$
      - 如果F的每个元素都是K上的代数数，F称为K的代数扩张
    - F的元素u称为R上的超越数，若不存在任何非零多项式$f\in R[x]$使得$f(u)=0$
      - 如果F中至少有一个元素是K上的超越数，F称为K的超越扩张
  - E是域F上的一个扩张$F(\alpha)$，α为F上的代数数，则$E=F(\alpha)$上的元素β可以表示为$\beta=b_0+b_1\alpha+\cdots+b_{n-1}\alpha^{n-1},b_i\in F$
- Galois域
  - 由素域F_p的n次扩张构成的有限域F_{p^n}为一种Galois域
  - 有限域F_{p^n}上的生成元g称为F_{p^n}的本原元，$F_{p^n}=\{0\}\cup<g>$，g定义的多项式叫本原多项式
    - 有限域F_{p^n}上的乘法群$F_{p^n}^*$是一个循环群
- **有限域的表示**
  - $f(x)$表现形式
    $F_{p^n}=\{f(x)=a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in F_p[x]\}$
    - 易于加法运算
  - g表现形式
    $F_{p^n}=\{0\}\cup<g>=\{0,g^0=1,g,g^2,\cdots,g^{p^n-2}\}$
    - 易于乘法运算
- **有限域的本原元**

> **寻找本原元**
> 给定有限域F_{p^n}，其中p为素数，设p^n-1的所有不同素因数为$q_1,\cdots,q_s$，则g是F_{p^n}中本原元的充要条件为
> $g^{\frac{p^n-1}{q_i}}\neq 1,i=1,\cdots,s$
> 寻找本原元：Gauss算法
>
> - STEP1:
>   令$i=1$，取F_q中任一非零元a_i，计算其阶，记为$\operatorname{ord}(a_i)=k_i$
> - STEP2:
>   若$k_i=q-1$，则a_i为本原元，停止循环；否则转至STEP3
> - STEP3:
>   取F_q中另一非零元，满足b不是a_i的整数次幂，计算其阶，记为$\operatorname{ord}(b)=h$，若$h=q-1$，则令$a_i+1=b$为一本原元，停止循环；否则转至STEP4
> - STEP4:
>   取整数t,s，使得$t\mid k_i,s\mid h,(t,s)=1,ts=[k_i,h]$，令$a_{i+1}=a_i^{\frac{k_i}{t}}b^{\frac{h}{s}}$，则$\operatorname{ord}(a_{i+1})=k_{i+1}=ts$，$i$增加1，转至STEP2

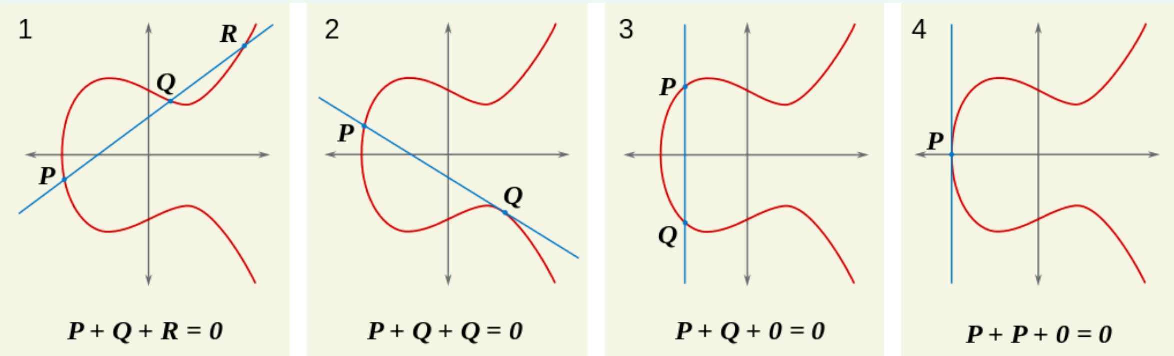
> **g的幂的运算**
> $g = a_n x^n + \cdots + a_1 x + a_0 = (\overline{a_n \cdots a_0})$
>
> - 乘除：正常运算
> - 加法：异或运算



椭圆曲线

基本概念

- **Weierstrass方程**
  域K上的椭圆曲线E方程为$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
  其中$a_1, a_2, a_3, a_4 \in K, \Delta \neq 0$
  $\Delta = -d_2^2d_8 - 8d_4^2 - 27d_6^3 + 9d_2d_4d_6$
  $d_2 = a_1^2 + 4a_2$
  $d_4 = 2a_4 + a_1a_3$
  $d_6 = a_3^2 + 4a_6$
  $d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$
  - 无穷远点$\{0(\infty, \infty)\} = \left\{(x, y) \in L \times L : E: y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\right\}$
- **简化Weierstrass方程**
  $(x', y') \to \left(\frac{x-3a_1^2-12a_2}{36}, \frac{y-3a_1x}{216} - \frac{a_1^3+4a_1a_2-12a_3}{24}\right)$
  得到$E: {y'}^2 = {x'}^3 + a_4x' + a_6$
  $\Delta = -16\left(4a_4^3 + 27a_6^2\right) \neq 0$
- **椭圆曲线与群**
  - K为$\mathbb{R}$，K的特征不为$2, 3$时：
    $y^2 = x^3 + a_4x + a_6$
    $\Delta = -16\left(4a_4^3 + 27a_6^2\right) \neq 0$
  - K为F_p，p为大于3的素数，K的特征不为$2, 3$时：
    $y^2 = x^3 + a_4x + a_6 \pmod p$
    $\Delta = -16\left(4a_4^3 + 27a_6^2\right) \neq 0 \pmod p$
  - K为F_{2^n}，K的特征为2时：
    $y^2 + xy = x^3 + a_2x^2 + a_6$
    $\Delta = a_6 \neq 0$
  - 其解为一个二元组$< x, y >, x, y \in K$，将此二元组描画到椭圆曲线上便为一个点，称其为解点
  - 解点构成群
    - 单位元：$0(\infty, \infty)$简记为0
    - 逆元：解点$R(x, y) = R^{-1}(x, -y)$，$0(\infty, \infty) = -0(\infty, \infty)$
    - 加法：$kP = P + \cdots + P$，有时记为P^k

> **椭圆曲线加法**
>
> 
>

椭圆曲线在$\mathbb{R}$上的加法

K为$\mathbb{R}$，K的特征不为$2, 3$时：
$y^2 = x^3 + a_4x + a_6$
$\Delta = -16\left(4a_4^3 + 27a_6^2\right) \neq 0$

求逆运算$-P = (x_1, -y_1)$

> - $P(x_1, y_1) \neq Q(x_2, y_2)$，$P, Q$不互逆
> $\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \\ \lambda = (y_2 - y_1) / (x_2 - x_1) \end{cases}$
> - $P(x_1, y_1) = Q(x_2, y_2) = 2P(x_1, y_1)$
> $\begin{cases} x_3 = \lambda^2 - 2x_1 \\ y_3 = \lambda(x_1 - x_3) - y_1 \\ \lambda = \left(3x_1^2 + a_4\right) / (2y_1) \end{cases}$

椭圆曲线在F_p上的加法

K为F_p，p为大于3的素数，K的特征不为$2,3$时：
$y^2=x^3+a_4x+a_6 \pmod p$
$\Delta=-16\left(4a_4^3+27a_6^2\right)\neq 0 \pmod p$

求逆运算$-P=(x_1,p-y_1)$

> - $P(x_1,y_1)\neq Q(x_2,y_2)$，$P,Q$不互逆
> $\begin{cases} x_3=\lambda^2-x_1-x_2 \pmod p \\ y_3=\lambda(x_1-x_3)-y_1 \pmod p \\ \lambda=(y_2-y_1)\cdot(x_2-x_1)^{-1} \pmod p \end{cases}$
> - $P(x_1,y_1)=Q(x_2,y_2)=2P(x_1,y_1)$
> $\begin{cases} x_3=\lambda^2-2x_1 \pmod p \\ y_3=\lambda(x_1-x_3)-y_1 \pmod p \\ \lambda=\left(3x_1^2+a_4\right)\cdot(2y_1)^{-1} \pmod p \end{cases}$

- F_p上E的阶为$\#(E(F_p))=p+1+\sum_{x=0}^{p-1}\left(\frac{x^3+a_4x+a_6}{p}\right)$，括号为勒让德符号
- 当循环群E的阶n是足够大的素数时，这个循环群中的离散对数问题是困难的

椭圆曲线在F_{2^n}上的加法

K为F_{2^n}，K的特征为2时：
$y^2+xy=x^3+a_2x^2+a_6$
$\Delta=a_6\neq 0$
求逆运算$-P=(x_1,x_1+y_1)$

> - $P(x_1,y_1)\neq Q(x_2,y_2)$，$P,Q$不互逆
> $\begin{cases} x_3=\lambda^2+\lambda+x_1+x_2+a_2 \\ y_3=\lambda(x_1+x_3)+x_3+y_1 \\ \lambda=(y_2+y_1)/(x_2+x_1) \end{cases}$
> - $P(x_1,y_1)=Q(x_2,y_2)=2P(x_1,y_1)$
> $\begin{cases} x_3=\lambda^2+\lambda+a_2 \\ y_3=x_1^2+(\lambda+1)x_3 \\ \lambda=\left(x_1^2+y_1\right)/(x_1) \end{cases}$

ElGamal加密

> - **STEP1: 密钥准备**
> 选取素数p，获取p的一个原根r，一个秘密整数$0\leq a\leq p-1$
> - **STEP2: 公钥**(p,r,b)
> $b\equiv r^a \pmod p$
> - **STEP3: 加密信息**P
> 选取随机数$1\leq k\leq p-2$
> $\gamma=r^k \pmod p$
> $\delta\equiv P\cdot b^k \pmod p$
> - **STEP4: 解密**
> $D(C)=\overline{\gamma^a}\delta$