1 数论

1.1 整除性

1.1.1 整除的定义$a|b \Leftrightarrow \exists d \in \mathbb{Z}, b = ad$

1.1.2 整除的性质

> （1）自反性
>
> （2）$a|b$且$b|a$，则$b = \pm a$（类似反对称性）
>
> （3）传递性
>
> （4）$a|b \Rightarrow a|(bc)$
>
> （5）线性构成：$a|b, a|c \Rightarrow a|(bx + cy)$
>
> （6）$a, b > 0, a|b \Rightarrow a \leqslant b$

【注记】

> 1° 利用（6），$a|b \Rightarrow |a|\,|\,|b| \Rightarrow |a| \leqslant |b| \Rightarrow -|b| \leqslant a \leqslant |b|$，可知$b$的因子只有有限个；
>
> 2° 0有无数多个因子

1.1.3 最大公因子

【定义】$d = (a, b) \Rightarrow \begin{cases} d|a, d|b, & \text{(是公因子)} \\ c|a, c|b \Rightarrow c \leqslant d, & \text{(最大)} \end{cases}$

【命题1】d可用a, b线性表示，即$\exists x, y \in \mathbb{Z}, d = ax + by$;

> 研究集合$S = \{ax + by | x, y \in \mathbb{Z}\}$，其关于乘法、加法封闭，并且有最小正元。
>
> 记这个最小正元为d，则$S = \{kd | k \in \mathbb{Z}\}$，这是因为如果有一个中间数$d' = kd + r, 0 < r < d$，由加法封闭性，$r \in S$，这与$d$是最小正元矛盾。
>
> 下面来证明这个d就是所求的最大公因子(a, b)。
>
> 设$d = ax + by \in S$，因为$a|(ax + by), b|(ax + by)$，一定有$(a, b)|(ax + by)$，则$(a, b)|d$，即$(a, b) \leq d$;
>
> 又因为$a \in S, b \in S$，则$d|a, d|b$（利用d是最小元）；
>
> 于是d是a,b的约数，自然$d \leq (a, b)$，由“$\leq$”的反对称性知道$d = (a, b)$。

【推论】若$(a,m)=(b,m)=1$，则$(ab,m)=1$；

> $$\begin{cases} ax_0+my_0=1 \\ bx_1+my_1=1 \end{cases} \Rightarrow abx_0x_1+m(ax_0y_1+bx_1y_0+my_0y_1)=1$$

【命题2】若m是正整数，则$(ma,mb)=m(a,b)$

> $(ma,mb)=xma+ymb=m(xa+yb)=m(a,b)$；
>
> 这里需要注意第三个等号不是显然的；
>
> 的取值需要满足$xma+ymb$是$\{xma+ymb|x,y\in\mathbb{Z}\}$中的最小元；
>
> 满足这条件时，$xa+by$一定是$\{xa+yb|x,y\in\mathbb{Z}\}$中的最小元；
>
> 因此第三个等号才能成立。

【推论】

（1）若$n=ax+by$，则一定有$(a,b)|n$；（重要）

（2）若$(a,b)=1$，则$S=\mathbb{Z}$；

（3）$(a,b)=d\Rightarrow(\frac{a}{d},\frac{b}{d})=1$；（重要）

（4）$(a,b)=(ma_1,mb_1)=m(a_1,b_1)\Rightarrow m|(a,b)$；（$a,b$的公因子是最大公因子的因子）

（5）若$ab\neq 0,\forall x\in\mathbb{Z},(a,b)=(a,b+ax)$；

> 设$g=(a,b),h=(a,b+ax)$
>
> $g|a,g|b\Rightarrow g|(b+ax)$
>
> $\Rightarrow g$是$a,b+ax$的公因子$\Rightarrow g$是h的因子【利用（4）】
>
> 同理可推得h是g的因子，所以$h=g$。

（6）若$c|ab$，$(c,b)=1\Rightarrow c|a$。

> $c|ab,c|ac\Rightarrow c$是a,b公因子$\Rightarrow c|(ab,ac)\Rightarrow c|a(b,c)\Rightarrow c|a$

1.1.4 辗转相除法

设$a\geq b>0$，则$(a,b)=(bq_0+r_0,b)=(b,r_0)=(r_0q_1+r_1,r_0)=(r_0,r_1)\dots$

1.1.5 最小公倍数

【定义】$c=[a,b]\Rightarrow\begin{cases} a|c,b|c,c>0 \\ a|e,b|e\Rightarrow c\leqslant|e| \end{cases}$

【命题3】a,b的公倍数都是最小公倍数的倍数

> 仿照最大公因数，研究集合$S=\{a,b\text{的公倍数}\}$;

【推论】

（1）$m\in\mathbb{N}_+,[ma,mb]=m[a,b]$；（如何证明？）

（2）$\forall a,b\in\mathbb{N}_+,[a,b](a,b)=ab$;

（先证互素时成立，再证不互素时$[a,b](a,b)=[\frac{a}{d},\frac{b}{d}](\frac{a}{d},\frac{b}{d})d^2=\frac{ab}{d^2}d^2=ab$）

1.1.6 素因子分解唯一性定理

$\forall m\in\mathbb{N}_+,m=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_l^{\alpha_l}$，且分解的形式唯一确定

若$a=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_l^{\alpha_l},b=m=p_1^{\beta_1}p_2^{\beta_2}\dots p_l^{\beta_l}$，则$\begin{cases}(a,b)=\prod\limits_{i=1}^{l}p_i^{\min\{\alpha_i,\beta_i\}}\\ [a,b]=\prod\limits_{i=1}^{l}p_i^{\max\{\alpha_i,\beta_i\}}\end{cases}$。（如何证明？）

1.2 线性不定方程

$\{ax+by\}=\{kd\}$，类似地，若要$a_1x_1+a_2x_2+\dots+a_mx_m=n$有解$\mathbf{x}=(x_1,x_2,\dots,x_m)$，则$(a_1,a_2,\dots,a_m)|n$。

【命题4】若x_0,y_0是$ax+by=n$的一组解，则通解为$x=x_0+\frac{b}{(a,b)}t,y=y_0-\frac{a}{(a,b)}t.$

> $\begin{cases}ax_0+by_0=n\\ ax+by=n\end{cases}\Rightarrow a(x-x_0)+b(y-y_0)=0$
>
> 所以$b|a(x-x_0)$，所以$\frac{b}{(a,b)}|\frac{a}{(a,b)}(x-x_0)$
>
> 因为$\left(\frac{b}{(a,b)},\frac{a}{(a,b)}\right)=1$，由【若$c|ab$，$(c,b)=1\Rightarrow c|a$】知$\frac{b}{(a,b)}|(x-x_0)$，y同理。

1.3 同余

1.3.1 定义

$a\equiv b(\mod m)\Leftrightarrow m|(a-b)$

1.3.2 模m同余的性质（用上述定义验证）

（1）自反性

（2）对称性

（3）传递性

（4）封闭性：$\begin{cases}a\equiv b(\mod m)\\ c\equiv d(\mod m)\end{cases}\Rightarrow\begin{cases}a+c\equiv b+d(\mod m)\\ ac\equiv bd(\mod m)\end{cases}$

可用来化简指数，如：$5^n \equiv (-1)^n \equiv x(\mod 6)$

（5）大模化小：$a \equiv b(\mod m), m = kd \Rightarrow a \equiv b(\mod d)$

（6）向右自由放大，模不变：$a \equiv b(\mod m) \Rightarrow ax \equiv bx(\mod m)$

利用定义：$\frac{a-b}{m} = k \Rightarrow \frac{(a-b)x}{m} = kx$

（7）双向自由放缩，模改变：$ax \equiv bx(\mod mx) \Leftrightarrow a \equiv b(\mod m)$

利用定义：$\frac{ax-bx}{mx} = \frac{a-b}{m} = k$

（8）互素时向右缩小，模不变：$ax \equiv bx(\mod m), (x, m) = 1 \Leftrightarrow a \equiv b(\mod m)$（重要）

其实是做除法：若 $ac \equiv bc(\bmod m), c \neq 0$，则 $a \equiv b(\bmod m/\gcd(c, m))$, 其中gcd(c,m)表示最大公约数。

（9）模可合并：$a \equiv b(\mod m_i), 1 \le i \le r \Leftrightarrow a \equiv b(\mod [m_1, m_2, \ldots, m_r])$（重要）

1.3.3 线性同余方程解法（$ax \equiv b(\mod m)$，求$x \equiv t(\mod m)$）（重要）

1.3.3.1 $ax \equiv b(\mod m)$有解当且仅当$(a, m)|b$；

（1）当a, m互素时方程有唯一解$x \equiv x_0(\mod m)$；

（2）否则，方程有(a, m)个解，此时方程$\frac{a}{(a,m)}x \equiv \frac{b}{(a,m)}(\mod \frac{m}{(a,m)})$的解唯一，为$x \equiv x_0(\mod \frac{m}{(a,m)})$，这也是原方程的一个特解（$x = x_0(\mod m)$），则原方程的通解是$x \equiv x_0 + \frac{m}{(a,m)}t(\mod m), 0 \le t \le (a, m) - 1$。

1.3.3.2 单解举例：求解$14x \equiv 27(\mod 31)$

1.3.3.3 多解举例：求解$6x \equiv 30(\mod 33)$

1.3.4 中国剩余定理（解方程组$x \equiv a_i(\mod m_i)$）

若m_i两两互素，则方程组有解，且解模$m_1 m_2 \ldots m_r$唯一。解可以按照如下方式构造：

（1）令$M = m_1 m_2 \ldots m_r, M_i = \dfrac{M}{m_i}$（有$(M_i, m_i) = 1$）

（2）引入逆元b_i：$\forall i, M_i b_i \equiv 1(\mod m_i)$有解，且$j \neq i$时，$M_j b_i \equiv 0(\mod m_i)$；

（3）令$y=\sum_{j=1}^{r}M_jb_ja_j$，则$y=\sum_{i\neq j}M_jb_ja_j+M_ib_ia_i$，模$m_i$为1

（4）$y\equiv\sum_{i\neq j}M_jb_ja_j+M_ib_ia_i(\mod m_1m_2\dots m_r)$是原方程组的解

解的唯一性证明：设$y_1-y_2\equiv 0(\mod m_i)\Rightarrow y_1-y_2\equiv 0(\mod [m_1,m_2,\dots,m_r])$

1.3.5 线性同余方程组有解对方程结构的要求

仅考虑两个方程的情况，$\begin{cases}x\equiv a_1(\mod m_1)\\x\equiv a_2(\mod m_2)\end{cases}$有解当且仅当$(m_1,m_2)|(a_1-a_2)$。

证明：$\begin{cases}x=k_1m_1+a_1\\x=k_2m_2+a_2\end{cases}$，则$m_1k_1+m_2k_2=a_2-a_1$。

1.4 欧拉定理和欧拉函数

1.4.1 模m的完系：$\{[0],[1],\dots,[m-1]\}$；

定理：若$\{x_1,\dots,x_m\}$是模m的完系，则$\{ax_1,\dots,ax_m\}$也是模m的完系。

1.4.2 模m的同余类：$[i]=A_i=\{x|x\in\mathbb{Z},x\equiv i(\mod m)\},0\leq i\leq m-1.$

1.4.2.1 性质：

（1）$\bigcup_{i=0}^{m-1}A_i=\mathbb{Z}$;

（2）若某元素与m互素，则该元素所在的同余类中所有元素都与m互素。

1.4.3 模m的缩系：$\{[i]|(i,m)=1\}$；

若$\{r_1,\dots,r_{\phi(m)}\}$是模m的缩系，则$\{ar_1,\dots,ar_{\phi(m)}\}$也是模m的缩系。

注意：

1、这里的定义和完系的定义写法都是不严谨的，**应该只取一个代表元**，而不是整个同余类。

2、缩系中的元素不一定是素数，只是和m互素。

1.4.4 欧拉函数$\phi(m)$（与m互素的同余类个数，即不超过m且与m互素的正整数个数）

规定$\phi(1)=1$，且若p为素数，则$\phi(p)=p-1$；

1.4.4.1 欧拉定理

若$(a,m)=1$，则$a^{\phi(m)}\equiv 1(\mod m)$；

1.4.4.2 费马定理

若p是素数，且$(a,p)=1$，则$a^{p-1}\equiv 1(\mod p)$；（逆不成立）

1.4.4.3 欧拉函数的算法

（1）如果p为素数，则$\phi(p^n) = p^n - p^{n-1}$，即1~$p^n$这$p^n$个数减去与$p^n$有公因子$p$的数的个数。

（2）如果$(m,n)=1$，则$\phi(mn)=\phi(m)\phi(n)$。（先把1~mn分成m个模m的同余类，与m互素的有$\phi(m)$个，每个同余类都是模n的完系，故每个同余类中都有$\phi(n)$个数满足要求，这就是**列表法**证明。）

（3）$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$，两边取欧拉函数，则$\phi(n) = \prod \phi(p_i^{\alpha_i}) = \prod p_i^{\alpha_i}\left(1-\frac{1}{p_i}\right) = n\prod\left(1-\frac{1}{p_i}\right)$。

1.4.4.4 举例：把$x \equiv 2^{340} (\mod 341)$化成简单形式；

1.4.4.5 威尔逊定理

p为素数，则$(p-1)! \equiv -1 (\mod p)$

> $x^p - x \equiv x(x-1)\dots(x-(p-1)) (\mod p)$
>
> $x^{p-1} - 1 \equiv (x-1)(x-2)\dots(x-(p-1))$
>
> 令$x=0$，即证（有点扯，虽然但是）

1.5 整数的因子及完全数

1.5.1 正因子数：$n \in \mathbb{N}_+, d(n) = \sum_{d|n} 1$

当m、n互素时有性质：$d(mn) = d(m)d(n)$

> 证明：设$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_l^{\alpha_l}$，则$p_i^{\alpha_i}$有$1, p_i, \dots, p_i^{\alpha_i}$这$\alpha_i + 1$个因子，$a$的一个因子是从这$l$组因子中每组取一个组成的。
>
> 因此$d(n) = \prod(\alpha_i + 1)$。

1.5.2 正因子和：$\sigma(n) = \sum_{d|n} d$

当m、n互素时有性质：$\sigma(mn) = \sigma(m)\sigma(n)$

> 证明：设$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_l^{\alpha_l}$，则某个因子可表示为$y = p_1^{f_1} p_2^{f_2} \dots p_l^{f_l}$，这里的上标随机选取，求和相当于$l$维求和，则$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$。

1.5.3 完全数：这样的$n:\sigma(n)=2n$.

定理：（1）若p为素数，且2^p-1为素数，则$2^{p-1}(2^p-1)$为完全数；

（2）若n为偶完全数，则必有$n=2^{p-1}(2^p-1)$；

1.6 原根与指数

目的：求解$x^n\equiv c(\mod m)$

讨论：当$(c,m)=1$时，$x_0^n\equiv c(\mod m)$是一个特解，$y^n\equiv 1(\mod m)$是齐次的通解（可能有多个y），则$x=x_0y$是原方程的解。

注意这里齐次方程变成了$x^n=1$，非齐次方程变成了$x^n=c$。

1.6.1 阶：满足$a^n\equiv 1(\mod m)$的最小正整数l称为a模m的阶。（在a、m互素时讨论）

研究方式：同样是研究$\{n|a^n\equiv 1(\mod m)\}$，与最大公因数等类似。

（1）由欧拉定理，特别地有$l|\phi(m)$。

（2）若$a^{n_1}\equiv a^{n_2}(\mod m)$，则$n_1\equiv n_2(\mod l)$。

推论：a^k模m的阶为$\frac{l}{(l,k)}$。（证明方法：利用整除关系的反对称性）

1.6.2 原根：若$(g,m)=1,g$模m的阶为$\phi(m)$，称g为模m的原根；

> 以下懒得打≡符号了，用=代替。

1.6.2.1 原根该从哪里找？（计算）

（1）取$0\le i,j\le\phi(m)-1,i\ne j$，显然$g^i\ne g^j(\mod m)$，则$\{g^0,g^1,\dots,g^{\phi(m)-1}\}$构成模m的缩系！

（2）每个与m互素的a与且仅与某个g^i同余，则原根可以从上述缩系中寻找。

（3）若$(p,\phi(m))=1$，则g^p也是模m的原根。

1.6.2.2 什么数有原根？

引理1：同余多项式$P_n(x)=0(\mod p)$至多有n个解（归纳法）

引理2：n≥1时，有$\sum_{d|n}\phi(d)=n$

> **定理**：若p为素数，$l|(p-1)$，则模p阶为l的数恰好有$\phi(l)$个
>
> 特别，取$l=\phi(p)$，则模p阶为$\phi(p)$的数有$\phi(p-1)$个。（有$\phi(p-1)$个模p的原根）
>
> 可以证明，有原根的数为$2,4,p^k,2\cdot p^k$

1.6.3 指数：设g为模p的原根，则{$g^0,g^1,\ldots,g^{p-2}$}为模p的缩系，对于任意与p互素的n，存在缩系中某个元素g^m，使得$n\equiv g^m(\mod p)$成立，称m为n对于原根g的模p指数，记为$m=\mathrm{ind}_g n$。

性质：

（1）若g^l=n(mod p)，又$g^{\mathrm{ind}_g n}=n(\mod p)$，则$l=\mathrm{ind}_g n(\mod p-1)$（这里的$l$不是阶哈）

> 若$g^a=g^b$(mod p)，则g^{a-b}=1(mod p)
>
> 所以阶$l|(a-b)$，而g是原根，所以$l=\phi(p)=p-1$；
>
> 所以$a-b=0(\mod p-1)$，即$a=b(\mod p-1)$

（2）p不是ab的因子，$\mathrm{ind_g}ab = \mathrm{ind_g}a + \mathrm{ind_g}b(\mathrm{mod}\ p - 1)$

（3）p不是a的因子，$\mathrm{ind_g}a^k = k\cdot\mathrm{ind_g}a(\mathrm{mod}\ p - 1)$

1.6.4 现在我们终于可以来解$x^k=n(\mod m),m=\prod p_i^{a_i}$了！

> （1）化为$\begin{cases}x^k=n(\mod p_1^{a_1})\\ \ldots\\ x^k=n(\mod p_t^{a_t})\end{cases}$
>
> （2）每个方程化为$x^k=n(\mod p_i)$
>
> （3）化为$k\cdot\mathrm{ind}_g x=\mathrm{ind}_g n(\mod p_i-1)$
>
> （4）等价于解方程$ax=b(\mod p_i-1)$，有解的充要条件是$(a,p_i-1)|\mathrm{ind}_g n$。