第二讲 初等数论

2

本讲提要

- ❑ 整数的基本概念(续)
- ❑ 同余

1.1 整数唯一分解定理

引理1 若p是一素数，a是任一整数，则有$p\mid a$或$(p, a)=1$。

引理1证明.

$(p,a)\mid p \Rightarrow (p,a)=1$或$(p,a)=p$。其中$(p,a)=p\Rightarrow p\mid a$。

引理2 若p是素数，$p|ab$，则$p\mid a$或$p\mid b$。

引理2证明.

若$p\nmid a$，则由引理1得$(p,a)=1$，而$p\mid ab$，由第一讲定理5知$p\mid b$。

一般形式：若素数$a\mid a_1a_2\ldots a_n$，则必有$a\mid a_1$或$a\mid a_2\ldots$或$a\mid a_n$。

1.1 整数唯一分解定理(续)

定理1(整数唯一分解定理) 任何大于1的正整数都能分解成素 数的乘积,即对于整数$a>1$，有

$a = p_1 p_2 \cdots p_n$，$p_1 \le p_2 \le \cdots \le p_n$， (1)

其中p_1，p_2,⋯，p_n都是素数,并且若

$a = q_1 q_2 \cdots q_m$，$q_1 \le q_2 \le \cdots \le q_m$， (2)

其中q_1，q_2,⋯，q_m都是素数，则$m = n$，$q_i = p_i (i = 1,2,\cdots, n)$。

定理1证明.

首先，证明式(1)成立。数学归纳法，当 $a = 2$时式(1)显然成立。

假定一切小于a的正整数都成立，考虑 a如果为素数显然成立， 如果为合数则必有分解 $a = bc, 1 < b \le c < a$,可知b和c都能表示为素数乘积，因此a也能表示为素数乘积， 故式(1)成立。

其次,证明唯一性。由式(1)和式(2)知$p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$， 由引理2的一般形式可知$p_1 \mid q_j$，$q_1 \mid p_k$，由于$q_j$，$p_k$为素数，所以$p_1 = q_j$，$q_1 = p_k$。同时有$p_1 \ge q_1$和$q_1 \ge p_1$，因此，$p_1 = q_1$。进一步，由$p_2 \cdots p_n = q_2 \cdots q_m$可以得$p_2 = q_2$，以此类推，最后可得 ，$m = n$，$p_n = q_m$。

1.1 整数唯一分解定理(续)

整数唯一分解定理成立与素数和整数的定义有关。例如，考虑自然数的子集S $=\{3k+1\mid k=0,1,2,\cdots\}$，如果定义其素数是恰有两个因子在$S$中，例如,4,7,10,13,19,22,25,$\cdots$都是$S$中的素数，那么$S$中的数100就有两种分解形式：

$100=4\cdot 25$ 或$100=10\cdot 10$。

1.1 整数唯一分解定理(续)

算术基本定理说明，任 意大于1的整数能够唯一写成

$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$， $\alpha_i > 0 (i = 1, \cdots, k)$，其中 $p_i < p_j (i < j)$

是素数。

因此，对于 $a > 0$ 和 $b > 0$，且

$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$， $\alpha_i \geq 0 (i = 1, \cdots, k)$，

$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$， $\beta_i \geq 0 (i = 1, \cdots, k)$，

则

$(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_k^{\min(\alpha_k, \beta_k)}$，

$[a, b] = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \cdots p_k^{\max(\alpha_k, \beta_k)}$。

由于 $x + y = \max(x, y) + \min(x, y)$，

所以， $ab = [a, b](a, b)$，即 $[a, b] = \dfrac{ab}{(a, b)}$。

1.2 一次不定方程

二元一次不定方程是指

$$a_1x + a_2y = n, \qquad (3)$$

其中a_1，a_2，n是给定的整数，$a_1a_2 \neq 0$。

定理2 方程(3)有整数解的充分必要条件是

$$(a_1, a_2) \mid n。$$

定理2证明.

$\rightarrow$有解时显然成立。

$\leftarrow$不失一般性，设$(a_1, a_2) = 1$及$a_1 > 0$，$a_2 > 0$。由上一讲定理4知，存在$a_1u + a_2v = 1$，于是$x = nu$，$y = nv$就是一组解。

1.2 一次不定方程 (续)

定理3 设$(a_1, a_2) = 1$，则方程 (3)的全部解可表示为

$$x = x_0 + a_2 t，\ y = y_0 - a_1 t,$$

其中x_0，y_0为方程 (3)的一组解， t为任意整数。

定理3证明.

正确性.

$a_1(x_0 + a_2 t) + a_2(y_0 - a_1 t) = a_1 x_0 + a_2 y_0 = n$。

通解性.

设x_1，y_1为任意一组解，则 $a_1 x_1 + a_2 y_1 = n$，知$a_1 x_0 + a_2 y_0 = n$。

$\therefore a_1(x_1 - x_0) + a_2(y_1 - y_0) = 0$。 (4)

$\because (a_1, a_2) = 1$。$\therefore$由上讲定理 5，

$a_2 \mid x_1 - x_0 \Rightarrow x_1 = x_0 + a_2 t$。

将x_1代入(4)得

$a_1(x_0 + a_2 t - x_0) + a_2(y_1 - y_0) = 0$，整理得： $y_1 = y_0 - a_1 t$。

1.2 一次不定方程(续)

定理4 设$s \ge 2$，s元一次不定方程

$$a_1x_1 + a_2x_2 + \cdots + a_sx_s = n，a_1a_2\cdots a_s \ne 0,$$

有整数解x_1，x_2,⋯，x_s的充分必要条件是

$$(a_1, a_2, \cdots, a_s) \mid n。$$

定理4证明. 模仿定理2，结合上一讲定理 7。

1.2 一次不定方程(续)

定理5 考虑不定方程$a_1x_1+a_2x_2=n,(a_1,a_2)=1$，$a_1>0$，$a_2>0$。

(1) 在$n>a_1a_2$时，有正整数解$x_1>0$，$x_2>0$; (2) 但在$n=a_1a_2$时，上述方程没有正整数解 $x_1>0$，$x_2>0$。

定理5证明.

(1) $a_1x_1+a_2x_2=n$的全部解由定理 3可表示为：$x_1=x_1'+a_2t$，$x_2=x_2'-a_1t$，其中x_1'，x_2'是方程的一组解。t可任意选择。因此，不难知道，可取 t_0使

$0<x_2=x_2'-a_1t_0\le a_1$,

又由$n>a_1a_2$可得

$a_1(x_1'+a_2t_0)=n-a_2x_2=n-a_2(x_2'-a_1t_0)>a_1a_2-a_2a_1=0$。

故对上述t_0，$x_1=x_1'+a_2t>0$，因此，$n>a_1a_2$时有解$x_1>0$, $x_2>0$。

1.2 一次不定方程(续)

定理5证明.（续）

(2) 如果$n=a_1a_2,(a_1,a_2)=1$时，有解$x_1>0$，$x_2>0$，则

$a_1a_2=a_1x_1+a_2x_2$。

$\because (a_1,a_2)=1$，故$a_1 \mid x_2$，$a_2 \mid x_1 \Rightarrow a_1 \le x_2$，$a_2 \le x_1$，

得$a_1a_2=a_1x_1+a_2x_2 \ge 2a_1a_2$，这不可能。

2.1 同余定义与概念

定义1 给定正整数m，如果用m去除两个整数a和b所得的余数相同，我们就说a，b对m同余，记为$a\equiv b(\bmod m)$，如果余数不同，a，b对m就不同余，记为$a\not\equiv b(\bmod m)$。

性质1 (1)自反性$a\equiv a(\bmod m)$;

(2) 对称性 $a\equiv b(\bmod m)$，则$b\equiv a(\bmod m)$;

(3) 传递性$a\equiv b(\bmod m), b\equiv c(\bmod m), a\equiv c(\bmod m)$。

定理6 整数a，b对模m同余的充分必要条件是$m\mid a-b$。

定理6证明.

$\rightarrow a=mq_1+r$，$b=mq_2+r$。$\therefore a-b=m(q_1-q_2)$。$\therefore m\mid a-b$。

$\leftarrow a=mq_1+r_1$，$b=mq_2+r_2, 0\le r_1$，$r_2<m$。

$a-b=m(q_1-q_2)+r_1-r_2, \therefore m\mid r_1-r_2$。又$\because |r_1-r_2|<m, \therefore r_1=r_2$。

2.1 同余定义与概念(续)

定理7 如果$a \equiv b \pmod{m}$，$\alpha \equiv \beta \pmod{m}$,则有

(1) $ax + \alpha y \equiv bx + \beta y \pmod{m}$，其中$x$，$y$为任意整数；

(2) $a\alpha \equiv b\beta \pmod{m}$;

(3) $a^n \equiv b^n \pmod{m}$;

(4) $f(a) \equiv f(b) \pmod{m}$，$f(x)$为任意给定整系数多项 式。

定理7证明.

(1) $\because m \mid a - b$，$m \mid \alpha - \beta$。

$\therefore m \mid x(a-b) + y(\alpha - \beta) = (ax + \alpha y) - (bx + y\beta)$。

(2) $m \mid \alpha(a-b) + b(\alpha - \beta) = \alpha a - b\beta$。

(3) 由(2)反复可得。

(4) 由(1)、(3)反复可得。

2.1 同余定义与概念(续)

定理8 如果$ac \equiv bc \pmod{m}$，且若$(m,c)=d$，则

$$a \equiv b\left(\bmod \frac{m}{d}\right)。$$

定理8证明.

由定理6知$m \mid ac-bc=c(a-b) \Rightarrow \frac{m}{d}\left|\frac{c}{d}(a-b)\right.$,

又$\because \left(\frac{m}{d},\frac{c}{d}\right)=1 \Rightarrow \frac{m}{d}\left|a-b\right.$。

$\therefore a \equiv b\left(\bmod \frac{m}{d}\right)$。

2.1 同余定义与概念(续)

定理9 若$a \equiv b \pmod{m_i}$，$i=1,2,\cdots$，n，则

$a \equiv b \pmod{[m_1, m_2, \cdots, m_n]}$。

定理9证明.

可知$m_i \mid a-b$，$i=1,2,\ldots$，n。

$a-b$，m_i按标准分解式展开可知$[m_1, m_2, \cdots, m_n] \mid a-b$。

$\therefore\ a \equiv b \pmod{[m_1, m_2, \cdots, m_n]}$。

2.2 剩余类和完全剩余系

定义2 设m是一个给定整数，$C_r(r=0,1,\cdots，m-1)$表示所有形如$qm+r$的整数组成的集合，其中$q=0,\pm 1,\cdots$，则C_0，$C_1,\cdots$，C_{m-1}叫做模m的剩余类。

定理10 设$m>0$，C_0，$C_1,\cdots$，C_{m-1}是模m剩余类，则有

(1) 每个整数都包含在某一个剩余类C_j中，这里$0\le j\le m-1$;

(2) 两个整数x，y属于同一类的充分必要条件是

$$x\equiv y\ (\mathrm{mod}\, m)。$$

2.2 剩余类和完全剩余系(续)

定理10证明.

(1) 设a是任一整数，则有$a = qm + r, 0 \le r < m$。

故$a \in C_r$。

(2) $\rightarrow \because x$，y为同一剩余类。$\therefore x = q_1 m + r$，$y = q_2 m + r$。

$\therefore m \mid x - y = (q_1 - q_2)m$。$\therefore x \equiv y \pmod{m}$。

$\leftarrow$由同余定义1立得x和y同在某一个C_r中。

2.2 剩余类和完全剩余系(续)

定义3 在模m的剩余类C_0，$C_1,\cdots$，C_{m-1}中各取一个数$a_j \in C_j$，$j=0,1,\cdots$，$m-1$，此m个数a_0，$a_1,\cdots$，a_{m-1}称为模m的一组完全剩余系。

由定义立即得到：

定理11 m个整数成为模m的完系的充要条件为两两对模m不同余。

定理11证明.

根据定义显然成立。

#常用的完全剩余系$0,1,\cdots$，$m-1$，称为模m的非负最小完全剩余。

2 剩余类和完全剩余系(续)

定理12 设$(k,m)=1$，而a_0，$a_1,\cdots$，a_{m-1}是模m的一组完系则ka_0，$ka_1,\cdots$，ka_{m-1}也是模m的一组完系。

定理12证明.

如果不是完系，则由定 理11存在

$$ka_i \equiv ka_j \pmod m，\quad 0 \le i < j \le m-1。$$

则$m \mid k(a_i - a_j)$。又$(k,m)=1$，由上一讲定理 5，知$m \mid a_i - a_j$。矛盾。

2 剩余类和完全剩余系(续)

定理13 设$m_1 > 0$，$m_2 > 0, (m_1, m_2) = 1$，而x_1，x_2分别通过模m_1，m_2的完系，则$m_2x_1 + m_1x_2$通过模m_1m_2的完系。

定理13证明.

x_1，x_2分别有m_1，m_2个整数，因此，$m_2x_1 + m_1x_2$有m_1m_2个整数。剩下只需要证明它们对模m_1m_2两两不同余即可。

假定：$m_2x_1' + m_1x_2' \equiv m_2x_1'' + m_1x_2'' \pmod{m_1m_2}$，　　　(5)

则$m_2x_1' \equiv m_2x_1'' \pmod{m_1}$，$m_1x_2' \equiv m_1x_2'' \pmod{m_2}$。

由于$(m_1, m_2) = 1, \therefore x_1' \equiv x_1'' \pmod{m_1}$，$x_2' \equiv x_2'' \pmod{m_2}$。

又由于x_1'，x_1''同取自模m_1的完全剩余系，由此可得：

$x_1' = x_1''$。同理$x_2' = x_2''$。因此，若(x_1', x_2')与(x_1'', x_2'')不同，则(5)式不能成立。

谢谢！