第 2 章　数论初步

数论是一个古老的数学分支.在本章中我们主要介绍初等数论中的基本知识,它包括整除性、同余式、原根与指数等内容,为第5章以后学习群、环、域的知识提供一个现实模型,也为今后学习保密通讯、密码体制作必要的准备.

2.1　整除性

在现实世界的数量关系中,人们首先认识到$1, 2, 3, \cdots$这些正整数,在正整数之间可以做加法运算.为了能做减法运算又扩充到负整数和零.全体正整数构成了自然数集合$\mathbf{N}$.全体正负整数和零构成了整数集合$\mathbf{Z}$.整数集合和自然数集合是初等数论研究的对象.

在整数集合$\mathbf{Z}$中可以进行加、减、乘运算,并且满足一些规律(例如,加法的交换律和结合律,乘法对加法的分配律等).一般不能做除法运算,所以,研究整数间能否相除是揭示整数特性的一个重要手段.

2.1.1　整除关系及其性质

定义 2.1. a, b是整数,a**整除**b当且仅当存在整数d,使得$ad = b$,并记为$a \mid b$,也称a 是b的一个**因子**.

整除性反映了两个整数之间的一种关系,如$-3 \mid 6, 3 \mid -6, 4 \nmid 6$.

定理 2.1. 设$a, b, c, x, y \in \mathbf{Z}$.整除关系具有如下一些性质:

1°　对任何a均有$a \mid a$;

2°　若$a \mid b$且$b \mid a$,则$a = \pm b$;

3°　若$a \mid b$且$b \mid c$,则$a \mid c$;

4°　若$a \mid b$,则$a \mid (bc)$;

5°　若$a \mid b$且$a \mid c$,则$a \mid (bx + cy)$;

6°　若$a, b > 0$且$a \mid b$,则$a \leqslant b$;

证明　$1^\circ, 3^\circ, 4^\circ, 5^\circ$利用整除定义可以证明.这里只证明$2^\circ$和$6^\circ$.

证明2° 由$a \mid b$和$b \mid a$,知存在$x, y \in \mathbf{Z}$,使得$ax = b, by = a$.将它们的左边、右边分别相乘得到$abxy = ab$,推出$xy = 1$.从而只能有两种情况$x = y = 1$或$x = y = -1$,即$a = b$或$a = -b$.

证明6° $a, b > 0$且$a \mid b$,必有$x \in \mathbf{N}$使$ax = b$.这里$x \geqslant 1$, 得出$a \leqslant b$.

更一般地,若$a, b \in \mathbf{Z}$,且$a, b \neq 0, a \mid b$,那么$|a| \mid |b|$.由6°推出$|a| \leqslant |b|$,即$-|b| \leqslant a \leq |b|$.这表明非零的整数$b$只有有限多个因子.由于任何$x \in \mathbf{Z}, x \cdot 0 = 0$,从而0有无限多个因子.

2.1.2 最大公因子

有了整除的概念就可以定义两个整数的最大公因子.

定义 2.2. a, b是两个不同时为零的整数,a, b的**最大公因子**$d = (a, b)$满足:

1° $d \mid a, d \mid b$,即d是a与b的公共因子;

2° 若$c \mid a, c \mid b$,则$c \leqslant d$,即d是a与b的所有公共因子中最大的一个.

类似地可以定义$(a_1, a_2, \cdots, a_n)$.

除了1以外的整数至少有两个因子:1和自身.两个整数至少有一个公因子1.前面已经分析过,每个非零整数只有有限多个因子.从而当a, b不全为零时,它们的公因子也只有有限多个.d则是最大的那个公因子.显然$d = (a, b) \geqslant 1$.例如,$(-3, -6) = 3, (-3, 6) = 3, (2, 3) = 1$.如果两个整数的最大公因子为1,则称这两个整数是互素的.

为了考察是否存在整数x, y,使得a与b的最大公因子$d = ax + by$.也就是a, b的最大公因子d是否能用a与b线性表示出来.为此,我们先扩大范围研究集合

$$S = \{ax + by \mid x, y \in \mathbf{Z}\}.$$

该集合有如下性质:

1° 若$m, n \in S$,则$m \pm n \in S$;

2° 若$n \in S, c \in \mathbf{Z}$,则$cn \in S$;

3° 记S中最小正整数为d,那么S中每个数都是d的倍数.反过来,d的每个倍数也必属于S.

上面的性质1°和2°是显然的.现证明性质3°.因为a,b不全为零,$\pm a,\pm b$显然属于集合S.也就是说,集合S中有正元素,所以S中一定存在着一个最小的正整数d.任取$c\in S$,有$c=qd+r$,其中q和r分别为c除以d得到的商和非负余数,$0\leqslant r<d$.因为$d\in S$,由性质2°知$q\cdot d\in S$.又因$c\in S$,由性质1°知$r=c-q\cdot d\in S$.由于d是S中最小的正整数,从而必有$r=0$,即$c=q\cdot d$,故

$$S=\{ax+by\mid x,y\in\mathbf{Z}\}=\{k\cdot d\mid k\in\mathbf{Z}\}.$$

下面证明S的最小正整数d就是a与b的最大公因子.由于$d\in S$,存在$x_0,y_0\in\mathbf{Z}$,使得$d=ax_0+by_0$.因为$(a,b)\mid a$, $(a,b)\mid b$,于是$(a,b)\mid d$.由整除的性质6°,知$(a,b)\leqslant d$.另一方面,因为$a\in S,b\in S$,那么存在$k_1,k_2\in\mathbf{Z}$,使得$a=k_1d,b=k_2d$,从而d是a与b的公因子.而(a,b)是a与b的最大公因子,所以$d\leq(a,b)$. 综上知$d=(a,b)$.

从上面的讨论看出,若a,b是不全为零的整数,那么一定存在整数x,y使$ax+by=(a,b)$.另外,整数n可以表示成$ax+by$形式的充要条件是$(a,b)\mid n$.显然,当a与b互素时,任何整数n都可以表示成$ax+by$的形式,由此得到:

定理 2.2. *设a,b是不为零的整数,那么*

1° *(a,b)是集合$S=\{ax+by\mid x,y\in\mathbf{Z}\}$中最小的正整数;*

2° *整数n可以表示成$ax+by$形式的充要条件是$(a,b)\mid n$.*

利用定理2.2可以得到关于最大公因子的一些有用的性质.

推论 2.1. *若m为正整数,则$(ma,mb)=m\,(a,b)$.*

证明

$$\begin{aligned}(ma,mb)&=\text{形如 }max+mby\text{ 的最小正整数}\\&=m\cdot\text{形如 }ax+by\text{ 的最小正整数}\\&=m\cdot(a,b)\,.\end{aligned}$$

特别有:

1° 若$(a,b)=d$,则$d=(a,b)=d\left(\frac{a}{d},\frac{b}{d}\right)$.两边除以$d$,得到$\left(\frac{a}{d},\frac{b}{d}\right)=1$.

2° 若m是a与b的公因子,$a=ma_1,b=mb_1$. $(a,b)=m\,(a_1,b_1)$,所以$m\mid(a,b)$,即a与b的公因子是最大公因子的因子.

推论 2.2. 若$(a,m)=(b,m)=1$,则$(ab,m)=1$.

证明 由$(a,m)=(b,m)=1$知存在$x_0,y_0,x_1,y_1\in\mathbf{Z}$,使得$ax_0+my_0=1$,$bx_1+my_1=1$.将这两个式子左右两边分别相乘,得到

$$abx_0x_1+m\left(ax_0y_1+bx_1y_0+my_0y_1\right)=1.$$

从而$(ab,m)=1$.

推论 2.3. a,b是不全为零的整数,对任意整数x有$(a,b)=(a,b+ax)$.

证明 令$g=(a,b)\,,h=(a,b+ax)$.由$g\mid a,g\mid b$知$g\mid(b+ax)$,即g是a与$b+ax$的公因子.从推论2.1中的2°知$g\mid h$.另一方面$h\mid a,h\mid(b+ax)$,推出$h\mid b$.从而h是a与b的公因子.同理$h\mid g$.由定理2.1中2°和$h,g>0$,得出$h=g$,即$(a,b)=(a,b+ax)$.

推论 2.4. 若$c\mid ab$且$(c,b)=1$,则$c\mid a$.

证明 由$c\mid ab,c\mid ac$,根据推论2.1中的2°知$c\mid(ab,ac)$.而从推论2.1知$(ab,ac)=a\,(b,c)=a\cdot 1=a$.于是$c\mid a$.

上面的证明(a,b)可以表示成$ax+by$形式的过程中,没有给出一种可行的方法求出x 和y.我们利用推论2.3,可以得到求解$ax+by=(a,b)$的欧几里得算法.由于$(a,b)=(|a|\,,|b|)$,我们这里不妨假设$a\geqslant b>0$.

定理 2.3. a,b为正整数,有下列关系式:

$$\begin{aligned}
a&=bq_0+r_0,0<r_0<b,\\
b&=r_0q_1+r_1,0<r_1<r_0,\\
r_0&=r_1q_2+r_2,0<r_2<r_1,\\
&\cdots\cdots\cdots\cdots\\
r_i&=r_{i+1}q_{i+2}+r_{i+2},0<r_{i+2}<r_{i+1},\\
r_{i+1}&=r_{i+2}q_{i+3},
\end{aligned}$$

则$(a,b)=r_{i+2}$.

证明 在上述辗转相除的一系列关系式中,$b > r_0 > r_1 > \cdots r_{i+1} > r_{i+2} \geqslant 0$是一个非负的递减序列.因此经过数次相除以后所得到的余数必为0.我们这里假设$r_{i+3} = 0$.根据推论2.3有

$$\begin{aligned}(a,b) &= (b,r_0) = (r_0,r_1) = \cdots = (r_i,r_{i+1}) \\ &= (r_{i+1},r_{i+2}) = r_{i+2}.\end{aligned}$$

由上述辗转相除算法,不仅可以得到(a,b),利用这些关系式反推回去,就可以得到$(a,b) = ax + by$中的x, y的值.

例 2.1. 计算$(963, 657)$.

解 按定理2.3提供的辗转相除算法得到关系式:

$$\begin{aligned}963 &= 657 \cdot 1 + 306, \\ 657 &= 306 \cdot 2 + 45, \\ 306 &= 45 \cdot 6 + 36, \\ 45 &= 36 \cdot 1 + 9, \\ 36 &= 9 \cdot 4,\end{aligned}$$

于是$(963, 657) = 9$.

又有

$$\begin{aligned}9 &= 45 - 36 \cdot 1 = 45 - (306 - 45 \cdot 6) = 45 \cdot 7 - 306 \\ &= (657 - 306 \cdot 2) \cdot 7 - 306 = 657 \cdot 7 - 306 \cdot 15 \\ &= 657 \cdot 7 - (963 - 657 \cdot 1) \cdot 15 = 657 \cdot 22 - 963 \cdot 15,\end{aligned}$$

方程$963x + 657y = 9$的解为$x = -15, y = 22$.

2.1.3 最小公倍数

定义 2.3. a, b为整数,a与b的**最小公倍数**$c = [a,b]$满足:

1° $a \mid c, b \mid c$,且$c > 0$;

2° 若$a \mid e, b \mid e$,则$c \leqslant |e|$.

类似可以定义$[a_1, a_2, \cdots, a_n]$.

任何两个整数a, b存在着正公倍数,如$|ab|$.我们知道,若u是a与b的公倍数,则对于任何正整数x,ux也是a与b的公倍数.所以a与b不存在最大公倍数.显然a与b有最小正公倍数c.我们称c为a与b的最小公倍数.

对于两个非零整数的最小公倍数也有类似于最大公因子的结论.

定理 2.4. *a, b为非零整数,a与b的每个公倍数均是最小公倍数的倍数.*

证明 考虑集合$S' = \{a与b的所有公倍数\}$.该集合有如下性质:

1° 若$m, n \in S'$,则$m \pm n \in S'$;

2° 若$n \in S', c \in \mathbf{Z}$,则$cn \in S'$;

3° S'中有最小正整数u,那么S'中每个元素均是u的倍数.反过来u的任意倍数必属于S'.显然u就是a与b的最小公倍数.

$1^\circ, 2^\circ$是显然的.因S'是由a与b的所有公倍数组成的,$\pm ab \in S'$,即S' 中有正数,从而S'中存在最小正整数u.任取$v \in S', v = qu + r, 0 \leqslant r < u$. 由于$v, u \in S', q \in \mathbf{Z}$,所以$r = v - qu \in S'$.$u$是$S'$中的最小正整数,因此必有$r = 0$,即$v = qu$.由$a$与$b$的最小公倍数的定义知$u = [a, b]$.$S' = \{ku | k \in \mathbf{Z}\}$.这说明非零整数$a, b$的每个公倍数都是最小公倍数的倍数.

利用定理2.4可以得到关于最小公倍数的一些有用的性质.

推论 2.5. *m为正整数,则$[ma, mb] = m\,[a, b]$.*

证明 由$a \mid [a, b]\,, b \mid [a, b]$,知$ma \mid m\,[a, b]\,, mb \mid m\,[a, b]$,即$m\,[a, b]$是$ma$与$mb$ 的公倍数,从而$[ma, mb] \mid m\,[a, b]$.另一方面,若l是ma与mb的公倍数,必有$m \mid l$.不妨令$l = l'm$,那么l'是a与b的公倍数,从而$[a, b] \mid l'$.由此推出$m\,[a, b] \mid l$,现取$l = [ma, mb]$,得到$m\,[a, b] \mid [ma, mb]$.由定理2.1中2°以及$m\,[a, b] > 0$, $[ma, mb] > 0$,最后得出

$$[ma, mb] = m\,[a, b].$$

推论 2.6. *若a,b为正整数,则$[a, b]\,(a, b) = ab$.*

证明 首先讨论$(a, b) = 1$的情况,$[a, b]$是a与b的最小公倍数,存在m_1使得$[a, b] = m_1 a$.由$b \mid [a, b]$,知$b \mid m_1 a$.而$(a, b) = 1$,由推论2.4得出$b \mid m_1$.m_1应该是满足此关系的最小正整数,所以$m_1 = b$,即$[a, b] = ab$.

当$(a,b)=d$时,由推论2.1中的1°知$\left(\frac{a}{d},\frac{b}{d}\right)=1$.从上面的结论,有$\left[\frac{a}{d},\frac{b}{d}\right]=\frac{1}{d^2}ab$.根据推论2.1和推论2.5,

$$(a,b)\,[a,b]=d^2\left(\frac{a}{d},\frac{b}{d}\right)\left[\frac{a}{d},\frac{b}{d}\right]=d^2\cdot 1\cdot\frac{1}{d^2}\cdot ab=ab.$$

这正是所要的结论.

2.1.4 素因子分解唯一性定理

a是b的因子当且仅当$a\mid b$.如果正整数b只有1和b为其因子,则称b为素数.例如$2,3,5,7,11,13,17,19,\cdots$,每个大于1的整数都可以被一个素数整除,从而得到该整数的素因子分解式.例如$60=2^2\cdot 3\cdot 5$.如果不考虑因子出现的次序,那么这种分解形式是唯一的.我们只叙述素因子分解唯一性定理,而不加以证明.

定理 2.5. (素因子分解唯一性定理)

任意正整数都能用一种方式且只有一种方式写成素数的乘积.

我们可以用加法作为构造自然数的手段,任何正整数$n=\underbrace{1+1+\cdots+1}_{n}$,其基本元素就是1.当用乘法作为构造自然数的手段时,其基本元素是全体素数.这个结论是素因子分解唯一性定理告诉我们的.

那么有多少个素数呢?结论是:存在着无限多个素数.可用反证法证明这一结论.假若只有有限多个素数$p_1,p_2,\cdots,p_k$.令$n=p_1p_2\cdots p_k+1$.n是自然数,存在一个素数p_i使$p_i\mid n$,推出$p_i\mid 1$.产生矛盾,故不可.所以有无限多个素数.

一般来说,对给定的整数进行素因子分解是很困难的.首先遇到的问题是没有一种“可行性算法”来确定所给的整数是否是素数.奥地利天文学家用厄氏筛法花了20年时间得到了10^8 以内的素数.20 世纪60年代美国宣布他们的计算机内存放着前5×10^8个素数.1985年9月美国在CRAY X-MP超级计算机上计算的最大素数为$2^{216091}-1>10^{65050}$.这是目前人们知道的最大素数.

2.2 线性不定方程

限制在某类数中(如正整数、有理数等)求解的方程叫丢番图方程,最简单的丢番图方程就是线性不定方程

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = n.$$

求其整数解.

早在1400多年前,隋朝《张丘健算径》一书中最后一问是世界著名的百鸡问题.问题是:鸡翁一,值钱五,鸡母一,值钱三,鸡仔三,值钱一,百钱买百鸡,问鸡翁、鸡母、鸡仔各几何?设鸡翁x只,鸡母y 只,鸡仔$3z$只.由题意列出方程

$$\begin{cases} 5x + 3y + z = 100 \\ x + y + 3z = 100. \end{cases}$$

消去z,得到$7x + 4y = 100$.这时多元线性不定方程化为二元线性不定方程.

以下我们只讨论二元线性不定方程.

定理 2.6. a,b,n为整数.$ax+by = n$有解当且仅当$(a, b) \mid n$.如果x_0,y_0是$ax+by = n$的一组解,则通解为

$$x = x_0 + \tfrac{b}{(a,b)}t, \quad y = y_0 - \tfrac{a}{(a,b)}t,$$

其中t为整数.

证明 由上节定理2.2对集合$S = \{ax + by \mid x, y \in \mathbf{Z}\}$的讨论知$ax + by = n$有解当且仅当$(a, b) \mid n$.

如果x_0,y_0是$ax + by = n$的一组解,即$ax_0 + by_0 = n$.由于

$$a\left(x_0 + \tfrac{b}{(a,b)}t\right) + b\left(y_0 - \tfrac{a}{(a,b)}t\right) = n.$$

所以$x = x_0 + \frac{b}{(a,b)}t$,$y = y_0 - \frac{a}{(a,b)}t$是$ax + by = n$的解.反过来,若$x$,$y$是方程$ax + by = n$的解,则

$$a(x - x_0) + b(y - y_0) = 0.$$

由此得出$b \mid a\,(x - x_0)$,即$\frac{b}{(a,b)} \mid \frac{a}{(a,b)}\,(x - x_0)$.而$\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$,于是$\frac{b}{(a,b)} \mid (x - x_0)$,即$x = x_0 + \frac{b}{(a,b)}t$,其中$t$为一个整数,将$x$的表达式代入$a\,(x - x_0) + b\,(y - y_0) = 0$,解出$y = y_0 - \frac{a}{(a,b)}t$.由此可知该方程的通解为

$$x = x_0 + \tfrac{b}{(a,b)}t, \quad y = y_0 - \tfrac{a}{(a,b)}t.$$

例 2.2. 前面的百鸡问题$7x+4y=100$.因$(7,4)=1$,所以方程有解,$x_0=0,y_0=25$是一组特解.通解为$x=4t,y=25-7t$.为保证x,y为正整数,t只能取值$0,1,2,3$.故该方程的解共有四组.它们是

$$\begin{cases}x=0\\y=25\\3z=75,\end{cases}\quad\begin{cases}x=4\\y=18\\3z=78,\end{cases}\quad\begin{cases}x=8\\y=11\\3z=81,\end{cases}\quad\begin{cases}x=12\\y=4\\3z=84.\end{cases}$$

2.3 同余式与线性同余方程

2.3.1 同余式及其性质

在2.1节中我们讲到整除性.整数a除以整数b,如果余数为0,称$b\mid a$.当$b\nmid a$时,余数有各种可能性.为了区分它们,我们引入同余的概念.

定义 2.4. 设$a,b,m\in\mathbf{Z}$,$m\neq 0$,a与b**模**m**同余**当且仅当$m\mid(a-b)$,并记为$a\equiv b\pmod m$.

显然$a\equiv b\pmod m$与$a\equiv b\pmod{-m}$等价.所以,以后假设$m>0$.

同余式有许多与通常等式相类似的性质.我们列举如下(设$a,b,c,x,y\in\mathbf{Z}$):

1° $a\equiv a\pmod m$;

2° 若$a\equiv b\pmod m$,则$b\equiv a\pmod m$;

3° 若$a\equiv b\pmod m$,$b\equiv c\pmod m$,则$a\equiv c\pmod m$;

4° 若$a\equiv b\pmod m$,$c\equiv d\pmod m$,则

$$a+c\equiv b+d\pmod m,\quad ac\equiv bd\pmod m;$$

5° 若$a\equiv b\pmod m$且$d\mid m$,则$a\equiv b\pmod d$;

6° 若$a\equiv b\pmod m$,则$ax\equiv bx\pmod m$;

7° $ax\equiv ay\pmod{am}$当且仅当$x\equiv y\pmod m$;

8° 若$ax\equiv ay\pmod m$且$(a,m)=1$,则$x\equiv y\pmod m$;

9° $x \equiv y \pmod{m_i}$,$1 \leqslant i \leqslant r$当且仅当$x \equiv y \pmod{[m_1, m_2, \ldots, m_r]}$.

以上诸性质都可以由同余定义直接得到.证明从略.

2.3.2 线性同余方程

a, b为整数,我们要求线性同余方程$ax \equiv b \pmod{m}$的解.先看一个特殊情况.

定理 2.7. 设$(a, m) = 1$.对于每个整数b,同余方程$ax \equiv b \pmod{m}$有模m唯一解.

证明 因为$(a, m) = 1$,对于每个整数b都存在着$x, y \in \mathbf{Z}$,使得$ax + my = b$,即$ax \equiv b \pmod{m}$,x就是该同余方程的解.

下面证明解是模m唯一的.若x_1, x_2都是$ax \equiv b \pmod{m}$的解,即$ax_1 \equiv ax_2 \equiv b \pmod{m}$.由于$(a, m) = 1$,得到$x_1 \equiv x_2 \pmod{m}$.这说明方程的任意两个解是模$m$同余的,即解模$m$唯一.

定理 2.8. 同余方程$ax \equiv b \pmod{m}$有解当且仅当$(a, m) \mid b$.当条件满足时,该同余方程有(a, m)个模m不同余的解:

$$x = x_0 + \frac{m}{(a, m)} t \pmod{m}, \quad 0 \leqslant t \leqslant (a, m) - 1.$$

其中x_0是同余方程

$$\frac{a}{(a, m)} x \equiv \frac{b}{(a, m)} \left(\mathrm{mod}\ \frac{m}{(a, m)} \right)$$

的解.

证明 设x_0是同余方程$ax \equiv b \pmod{m}$的解.即$m \mid (ax_0 - b)$.由于$(a, m) \mid m$,显然有$(a, m) \mid (ax_0 - b)$.又由$(a, m) \mid a$,推出$(a, m) \mid b$.反过来,当$(a, m) \mid b$时,存在$x_1, y_1 \in \mathbf{Z}$, 使$ax_1 + my_1 = b$,即$ax_1 \equiv b \pmod{m}$.这表明x_1就是同余方程$ax \equiv b \pmod{m}$的一个解.

当满足同余方程有解的条件$(a,m)\mid b$时,$ax\equiv b\,(\mathrm{mod}\ m)$可以化成等价的同余方程

$$\frac{a}{(a,m)}x\equiv\frac{b}{(a,m)}\left(\mathrm{mod}\ \frac{m}{(a,m)}\right).$$

由于$\left(\frac{a}{(a,m)},\frac{m}{(a,m)}\right)=1$,该方程有模$\frac{m}{(a,m)}$唯一解$x\equiv x_0\left(\mathrm{mod}\ \frac{m}{(a,m)}\right)$.这里不妨取$0\leqslant x_0<\frac{m}{(a,m)}$.这个$x_0$也是$ax\equiv b\,(\mathrm{mod}\ m)$的一个解.下面证明$x_0+i\frac{m}{(a,m)},0\leqslant i\leqslant(a,m)-1$也是$ax\equiv b\,(\mathrm{mod}\ m)$的解.把它们代入方程

$$a\left(x_0+i\frac{m}{(a,m)}\right)=ax_0+\frac{a}{(a,m)}im\equiv b\,(\mathrm{mod}\ m)\,.$$

而

$$0\leqslant x_0+i\frac{m}{(a,m)}<\frac{m}{(a,m)}+((a,m)-1)\frac{m}{(a,m)}=m,$$

所以$x_0+i\frac{m}{(a,m)},0\leqslant i\leqslant(a,m)-1$是$(a,m)$个模$m$不同余的解.反过来,假设$y$是$ax\equiv b\,(\mathrm{mod}\ m)$ 的一个解.必有$ax_0\equiv ay\equiv b\,(\mathrm{mod}\ m)$,推出$x_0\equiv y\left(\mathrm{mod}\ \frac{m}{(a,m)}\right)$,即$y=x_0+k\frac{m}{(a,m)}$.令$i$表示$k$除以$(a,m)$的非负余数,那么$y\equiv x_0+i\frac{m}{(a,m)}\,(\mathrm{mod}\ m)$.这说明$ax\equiv b\,(\mathrm{mod}\ m)$除上述$(a,m)$个解之外没有其他形式的解.

例 2.3. 解$14x\equiv 27\,(\mathrm{mod}\ 31)$.

解 因$(14,31)=1,14x\equiv 27\,(\mathrm{mod}\ 31)$.有模31唯一解,

$$14x\equiv 27\equiv 58\,(\mathrm{mod}\ 31)\,.$$

因$(2,31)=1$,利用同余式性质8°得到

$$7x\equiv 29\,(\mathrm{mod}\ 31)\,.$$

又由$7x\equiv 29\equiv 91\,(\mathrm{mod}\ 31)$,且$(7,31)=1$,解出$x\equiv 13\,(\mathrm{mod}\ 31)$.

例 2.4. 解$6x\equiv 30\,(\mathrm{mod}\ 33)$.

解 $(6,33)=3$且$3\mid 30$,由定理2.8知该同余方程有3个模33不同余的解.

与$6x\equiv 30\,(\mathrm{mod}\ 33)$等价的同余方程$2x\equiv 10\,(\mathrm{mod}\ 11)$中$(2,11)=1,x\equiv 5\,(\mathrm{mod}\ 11)$是它的模11唯一解.$x\equiv 5+11t\,(\mathrm{mod}\ 33)\,,0\leqslant t\leqslant 2$是同余方程$6x\equiv 30\,(\mathrm{mod}\ 33)$的三个模33不同余的解,即该同余方程的解为

$$x\equiv 5,16,27\,(\mathrm{mod}\ 33)\,.$$

2.3.3 求解线性同余方程组

我国古代数学著作《孙子算经》中“物有不知其数”一问:“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?”用数学语言来描述就是(设其数为x)

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7. \end{cases}$$

这一问题的古代算法在程大位的《算法统宗》中总结成:

“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.”

意思是以$70, 21, 15$分别乘该数除以$3, 5, 7$所得的余数$2, 3, 2$,将结果相加再模105. 即

$$x \equiv 70 \cdot 2 + 21 \cdot 3 + 15 \cdot 2 = 233 \equiv 23 (\bmod\ 105).$$

国外数论文献中把这个算法称之为中国剩余定理.在下面定理中将给出证明.

定理 2.9. 设自然数$m_1, m_2, \cdots, m_r$,两两互素,对任意整数$a_1, a_2, \cdots, a_r$,线性同余方程组$x \equiv a_i (\bmod\ m_i)$,$1 \leqslant i \leqslant r$均有解,并且解是模$m_1 m_2 \cdots m_r$唯一的.

证明 令$M = m_1 m_2 \cdots m_r, M_i = \frac{M}{m_i}, (M_i, m_i) = 1, 1 \leqslant i \leqslant r$.对每个$i, M_i b_i \equiv 1 (\bmod\ m_i)$有解并且当$j \neq i$时,$M_i b_i \equiv 0 (\bmod\ m_i)$.现令$y = \sum_{j=1}^{r} M_j b_j a_j$,显然

$$y = M_i b_i a_i \equiv a_i (\bmod\ m_i), 1 \leqslant i \leqslant r,$$

从而y是同余方程组的解.同时与y模$m_1 m_2 \cdots m_r$同余的数也是该同余方程组的解.

令y_1, y_2都是同余方程组的解,那么$y_1 - y_2 \equiv 0(\mathrm{mod}\ m_i), 1 \leqslant i \leqslant r$.也就是说$y_1-y_2$是$m_1, m_2, \cdots, m_r$的公倍数,从而$[m_1, m_2, \cdots, m_r] \mid (y_1-y_2)$.而$m_1, m_2, \cdots, m_r$ 两两互素,$[m_1, m_2, \cdots, m_r] = m_1 m_2 \cdots m_r$. 最后得出

$$y_1 \equiv y_2(\mathrm{mod}\ m_1 m_2 \cdots m_r).$$

该定理的证明是构造性的,它已指明解线性同余方程组的具体步骤.

例 2.5. 解同余方程组

$$\begin{cases} x \equiv 2(\mathrm{mod}\ 3) \\ x \equiv 3(\mathrm{mod}\ 5) \\ x \equiv 2(\mathrm{mod}\ 7). \end{cases}$$

解 本题中$M = 3 \cdot 5 \cdot 7 = 105, M_1 = 35, M_2 = 21, M_3 = 15$.由$35 b_1 \equiv 1(\mathrm{mod}\ 3), 21 b_2 \equiv 1(\mathrm{mod}\ 5), 15 b_3 \equiv 1(\mathrm{mod}\ 7)$分别解出$b_1 = 2, b_2 = 1, b_3 = 1$.从而

$$\begin{aligned} y &= 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 \\ &= 70 \cdot 2 + 21 \cdot 3 + 15 \cdot 2 = 233. \end{aligned}$$

$y \equiv 23(\mathrm{mod}\ 105)$是该同余方程组的解.

定理 2.10. 线性同余方程组$x \equiv a_i(\mathrm{mod}\ m_i), i = 1, 2$,有解的充要条件是$(m_1, m_2) \mid (a_1 - a_2)$.在条件满足时,该方程的解模$[m_1, m_2]$唯一.

证明 该方程有解就是存在着整数s, t,使$x = m_1 t + a_1$且$x = m_2 s + a_2$,即$m_1 t - m_2 s = a_2 - a_1$.从定理2.6知该方程有解当且仅当$(m_1, m_2) \mid (a_2 - a_1)$.所以线性同余方程组有解的充要条件是$(m_1, m_2) \mid (a_1 - a_2)$.

若当条件满足时,x_1和x_2都是该方程组的解,则

$$\begin{cases} x_1 - x_2 \equiv 0(\mathrm{mod}\ m_1) \\ x_1 - x_2 \equiv 0(\mathrm{mod}\ m_2). \end{cases}$$

x_1-x_2是m_1, m_2的公倍数.于是$[m_1, m_2] \mid (x_1-x_2)$,即$x_1 \equiv x_2(\ \mathrm{mod}\ [m_1, m_2])$.它说明该方程的解模$[m_1, m_2]$唯一.

例 2.6. 求解

$$\begin{cases} x \equiv 2 (\bmod 4) \\ x \equiv 0 (\bmod 6). \end{cases}$$

解 因$(4,6) \mid (2-0)$,该方程组有解并且解模12唯一.下面就求它的解.由$x \equiv 2(\bmod 4)$,知$x = 2+4k_1$,将其代入$x \equiv 0(\bmod 6)$, 得到$4k_1 \equiv 4(\bmod 6)$,化简后为$k_1 \equiv 1(\bmod 3)$.于是$k_1 = 1+3k_2$.再代入$x = 2+4k_1$,得到$x = 6+12k_2$.从而解为

$$x \equiv 6(\bmod 12).$$

2.4 欧拉定理及欧拉函数

2.4.1 完系与缩系

对于给定的整数m,每个整数都与且仅与集合$\{0,1,\cdots,m-1\}$中一个数模m同余.一般地,

定义 2.5. 整数集合$\{x_1,x_2,\cdots,x_m\}$,如果每个整数都与且仅与该集合中一个x_i模m同余,则称$\{x_1,x_2,\cdots,x_m\}$为模m的**完系**.

显然$\{0,1,2,3,4\}$是模5 的完系,$\{10,21,27,38,-1\}$也是模5 的完系.不难看出, 模m的完系有两个特征, 首先它是由m个元素组成的,其次这些元素相互不模m同余.

我们把模m的同余类表示成$A_i = \{x|x \in \mathbf{Z}, x \equiv i(\bmod m)\}, 0 \leqslant i \leqslant m-1$.每个整数都与$\{0,1,\cdots,m-1\}$中一个数同余,所以每个整数只属于$A_0,A_1,\cdots,A_{m-1}$ 中的一个.若$x \in A_i$且$(x,m) = 1$,那么A_i中的任意元素y都必有$(y,m) = 1$,这是因为$x,y \in A_i, x \equiv y(\bmod m)$,即$x = y+km$, 如果$(y,m) = d$,则必有$d \mid x$.再由$d \mid m$知$d \mid (x,m)$.而$(x,m) = 1$,从而$(y,m) = d = 1$.

若$x \in A_i$且$(x,m) = 1$,则称A_i是与m互素的同余类,与m互素的同余类个数记为$\phi(m)$,称为**欧拉函数**.

定义 2.6. 在每个与m互素的同余类中取一个元素作为代表放在一起构成的集合$\{r_1,r_2,\cdots,r_{\phi(m)}\}$叫做模$m$的**缩系**.

例 2.7. $\{0,1,2,3,4,5\}$是模6的完系,六个同余类$A_i=\{6k+i|k\in Z\}, 0\leqslant i\leqslant 5$中$A_1, A_5$是与6互素的同余类,故$\phi(6)=2.\{1,5\},\{7,-1\}$都是模6 的缩系.

实际上,把$\{1,2,\cdots,m-1\}$中与m互素的数放在一起恰好是模m的一个缩系.$\phi(m)$就是不超过m且与m互素的正整数个数.不难验证$\phi(2)=1,\phi(3)=\phi(4)=\phi(6)=2,\phi(5)=\phi(8)=4,\phi(7)=6$.我们规定$\phi(1)=1$.显然对于素数$p$, $\phi(p)=p-1$.

引理 2.1. 已知$(a,m)=1$.若$\{x_1,x_2,\cdots,x_m\}$是模m的完系,则$\{ax_1,ax_2,\cdots,ax_m\}$也是模$m$的完系,若$\{r_1,r_2,\cdots,r_{\phi(m)}\}$是模$m$的缩系,则$\{ar_1,ar_2,\cdots,ar_{\phi(m)}\}$也是模$m$的缩系.

证明 $\{x_1,x_2,\cdots,x_m\}$是模m的完系,由其定义$i\neq j, x_i\neq x_j(\mathrm{mod}\ m)$. 如果$ax_i\equiv ax_j(\mathrm{mod}\ m)$,由于$(a,m)=1$,推出必有$x_i\equiv x_j(\mathrm{mod}\ m)$.这与$\{x_1,x_2,\cdots,x_m\}$ 是模m的完系矛盾. 由此得出$ax_1,ax_2,\cdots,ax_m$是两两模m 互不同余的m个元素, 它们正好构成一个模m的完系.

$\{r_1,r_2,\cdots,r_{\phi(m)}\}$是模$m$的缩系,由其定义知$(r_i,m)=1, 1\leqslant i\leqslant\phi(m)$,并且$i\neq j, r_i\not\equiv r_j(\mathrm{mod}\ m)$.从$(r_i,m)=1$和$(a,m)=1$,根据推论2.2 知$(ar_i,m)=1$.前面已经证明过$i\neq j, ar_i\not\equiv ar_j(\bmod m)$.$ar_1,ar_2,\cdots,ar_{\phi(m)}$恰是$\phi(m)$个与$m$互素且两两模$m$ 不同余的元素.它们恰好构成模m的一个缩系.

2.4.2 欧拉定理与费马定理

定理 2.11. (欧拉定理)
如果$(a,m)=1$,则$a^{\phi(m)}\equiv 1(\mathrm{mod}\ m)$.

证明 取一个模m的缩系$\{r_1,r_2,\cdots,r_{\phi(m)}\}$.当$(a,m)=1$时,$\{ar_1,ar_2,\cdots,ar_{\phi(m)}\}$也是模$m$的缩系.任选一个$r_i$,必存在一个$r_j$使$r_i\equiv ar_j(\bmod m)$,并且不同的下标$i$对应不同的下标$j$.由此得出

$$\begin{aligned}r_1r_2\cdots r_{\phi(m)}&\equiv ar_{j_1}\cdot ar_{j_2}\cdots ar_{j_{\phi(m)}}\\&=a^{\phi(m)}\cdot r_1r_2\cdots r_{\phi(m)}(\mathrm{mod}\ m).\end{aligned}$$

由于$(r_i,m)=1,1\leqslant i\leqslant\phi(m)$,根据推论2.2知

$$(r_1r_2\cdots r_{\phi(m)},m)=1,$$

从前式立即推出

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

在定理2.11中取m为素数p,$(a,p)=1$就是$p\nmid a$,$\phi(p)=p-1$, 从而得到费马定理: p为素数且$p\nmid a$,则

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

若$p|a$,$a\equiv 0(\bmod\ p)$,则显然成立$a^p\equiv a(\bmod\ p)$.而当$p\nmid a$时,从费马定理知$a^{p-1}\equiv 1(\bmod\ p)$.再由同余式性质6°,仍成立$a^p\equiv a(\bmod\ p)$.所以,对于任何$a$都有$a^p\equiv a(\bmod\ p)$,其中$p$是素数.

2.4.3 计算欧拉函数

引理 2.2. p为素数,对一切正整数n,$\phi(p^n)=p^{n-1}(p-1)$.

证明 小于等于p^n的数共有p^n个, 其中与p^n有公因子p的数是$p,2p,\cdots,p^{n-1}p$,一共有p^{n-1}个.那么与p^n无公因子p的, 即与p^n互素的数共有$p^n-p^{n-1}=p^{n-1}(p-1)$个.

定理 2.12. 当$(m,n)=1$时,$\phi(mn)=\phi(m)\cdot\phi(n)$.

证明 $\phi(mn)$是小于等于mn且与mn互素的正整数个数,下面把所有小于等于mn的正整数列成一个方针

$$\begin{array}{ccccc}
1 & m+1 & 2m+1 & \cdots & (n-1)m+1\\
2 & m+2 & 2m+2 & \cdots & (n-1)m+2\\
3 & m+3 & 2m+3 & \cdots & (n-1)m+3\\
\vdots & \vdots & \vdots & & \vdots\\
m & m+m & 2m+m & \cdots & (n-1)m+m
\end{array}$$

若$(m,r)=d>1$,那么r所在行的全部元素$r,m+r,2m+r,\cdots,(n-1)m+r$均与$mn$有公因子$d$,由此可知,与$mn$互素的数只能在$(m,r)=1$的$\phi(m)$中寻

找,而当$(m,r)=1$ 时,$\{r,m+r,2m+r,\cdots,(n-1)m+r\}$是$n$元集合,并且两两模$n$不同余.它是模$n$的完系.在一个模$n$的完系中有$\phi(n)$个数与$n$互素.而该完系中每个数均与$m$互素,从而它里面有$\phi(n)$个数与$mn$互素.

从上分析得到$\phi(mn)=\phi(m)\cdot\phi(n)$.

若$(m,n)=1$,满足$f(mn)=f(m)f(n)$的函数f成为**积性函数**.欧拉函数ϕ是积性函数.从定理2.12不难看出.若n的素因子分解式为$n=p_1^{l_1}p_2^{l_2}\cdots p_k^{l_k}$,则

$$\phi(n)=p_1^{l_1-1}(p_1-1)\cdots p_k^{l_k-1}(p_k-1)=n(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_k}).$$

例 2.8. 求2^{340}除以341的余数.

解 $341=11\cdot 31$.由欧拉定理$2^{10}\equiv 1(\mathrm{mod}\ 11),2^{30}\equiv 1(\mathrm{mod}\ 31)$.

$$2^{340}=(2^{10})^{34}\equiv 1(\mathrm{mod}\ 11),$$
$$2^{340}=(2^{30})^{11}\cdot 2^{10}\equiv 2^{10}=(2^5)^2\equiv 1(\mathrm{mod}\ 31),$$

即2^{340}是下面线性同余方程组的解:

$$\begin{cases} x\equiv 1(\mathrm{mod}\ 11)\\ x\equiv 1(\mathrm{mod}\ 31). \end{cases}$$

解得$x\equiv 1(\mathrm{mod}\ 341)$,即$2^{340}\equiv 1(\mathrm{mod}\ 341)$.

本例说明费马定理的逆定理不成立,$2^{340}\equiv 1(\mathrm{mod}\ 341)$,但是341不是素数.

例 2.9. 解$9x\equiv 7(\mathrm{mod}\ 13)$.

解 13是素数.由费马定理知$3^{12}\equiv 1(\mathrm{mod}\ 13)$.

$$x\equiv 3^{12}\cdot x\equiv 3^{10}\cdot 9x\equiv 3^{10}\cdot 7\equiv(13-4)^5\cdot 7\equiv(-4)^5\cdot 7$$
$$\equiv(13+3)^2(-28)\equiv 9\cdot(-2)\equiv 8(\mathrm{mod}\ 13)$$

$x\equiv 8(\mathrm{mod}\ 13)$是该方程的解.

2.4.4 威尔逊定理

威尔逊定理给出了判定素数的充要条件.为此先给出两个引理.

引理 2.3. $x^2 \equiv 1 (\bmod p)$恰好有两个解$x \equiv 1, p-1 (\bmod p)$.

证明 $x^2 \equiv 1 (\bmod p)$是二次同余方程.设r是其解,$r^2 - 1 \equiv 0 (\bmod p)$,即$p \mid (r+1)(r-1)$.这里有两种可能:若$p \mid (r+1)$,则$r \equiv p-1 (\bmod p)$;若$p \mid (r-1)$,则$r \equiv 1 (\bmod p)$.

引理 2.4. p为奇素数,a'表示线性同余方程$ax \equiv 1 (\bmod p)$的解,这里a可以取值$1, 2, \cdots, p-1$.当$a \not\equiv b (\bmod p)$时,$a' \not\equiv b' (\bmod p)$.若$a' \equiv a (\bmod p)$, 则$a = 1$或$p-1$.

证明 由于a取值$\{1, 2, \cdots, p-1\}$, $(a, p) = 1$.方程$ax \equiv 1 (\bmod p)$恰好有一个解a'.假若$a' \equiv b' (\bmod p)$,在同余式两边同乘ab,$aa'b \equiv ab'b (\bmod p)$.因$aa' \equiv 1 (\bmod p)$, $bb' \equiv 1 (\bmod p)$,推出$a \equiv b (\bmod p)$.从而当$a \not\equiv b (\bmod p)$ 时,必有$a' \not\equiv b' (\bmod p)$.又若$a' \equiv a (\bmod p)$,同余式两边同乘$a$,有$a^2 \equiv 1 (\bmod p)$.从引理2.3 知$a \equiv 1 (\bmod p)$或$a \equiv p-1 (\bmod p)$.

定理 2.13. (**威尔逊定理**) p为素数当且仅当$(p-1)! \equiv -1 (\bmod p)$.

证明 p是素数.当$p = 2$时,显然$(2-1)! \equiv -1 (\bmod 2)$.当$p > 2$时.由引理2.4知$a$取值于集合$\{2, 3, \cdots, p-2\}$时,存在$a' \neq a$且$aa' \equiv 1 (\bmod p)$.当$a$取值不同时相应的$a'$也是不同的,从而$2, 3, \cdots, p-2$这$p-3$个数可以把$a$ 与a'组成一对,即

$$2 \cdot 3 \cdots (p-2) \equiv 1 (\bmod p);$$
$$(p-1)! = (p-1) \cdot 2 \cdot 3 \cdots (p-2) \equiv p-1 \equiv -1 (\bmod p)$$

反过来,已知$(n-1)! \equiv -1 (\bmod n)$.令$a$是$n$的因子且$a \neq n$.由$n \mid ((n-1)! + 1)$,得到$a \mid ((n-1)! + 1)$.显然$a \mid (n-1)!$,于是$a \mid 1$.由此推出$a = 1$. 这说明$n$除了自身之外只有因子$1, n$是素数.

2.5 整数的因子及完全数

n为正整数,$d(n)$表示n的正因子数,$\sigma(n)$表示n的正因子之和.显然

$$d(n)=\sum_{d|n}1,\sigma(n)=\sum_{d|n}d.$$

若$n=p_1^{l_1}p_2^{l_2}\cdots p_k^{l_k}$,那么$p_1^{f_1}p_2^{f_2}\cdots p_k^{f_k}(0\leqslant f_i\leqslant l_i,1\leqslant i\leqslant k)$是$n$的正因子.每个$f_i$ 有l_i+1种不同的取值,从而n有$(l_1+1)(l_2+1)\cdots(l_k+1)$个正因子,即

$$\begin{aligned}
d(n)&=(l_1+1)\,(l_2+1)\cdots(l_k+1)\,,\\
\sigma(n)&=\sum_{\substack{0\leqslant f_i\leqslant l_i\\1\leqslant i\leqslant k}}p_1^{f_1}p_2^{f_2}\cdots p_k^{f_k}\\
&=\sum_{\substack{0\leqslant f_i\leqslant l_i\\1\leqslant i\leqslant k-1}}p_1^{f_1}p_2^{f_2}\cdots p_{k-1}^{f_{k-1}}\left(\sum_{f_k=0}^{l_k}p_k^{f_k}\right)\\
&=\sum_{\substack{0\leqslant f_i\leqslant l_i\\1\leqslant i\leqslant k-1}}p_1^{f_1}p_2^{f_2}\cdots p_{k-1}^{f_{k-1}}\left(\frac{p_k^{l_k+1}-1}{p_k-1}\right)\\
&\cdots\cdots\cdots\cdots\\
&=\frac{p_1^{l_1+1}-1}{p_1-1}\bullet\frac{p_2^{l_2+1}-1}{p_2-1}\cdots\cdots\frac{p_k^{l_k+1}-1}{p_k-1}.
\end{aligned}$$

不难看出,当$(m,n)=1$时,$\sigma(mn)=\sigma(m)\bullet\sigma(n)$,$d(mn)=d(m)\bullet d(n)$,即$d$和$\sigma$均是积性函数.

定义 2.7. 正整数n为**完全数**当且仅当n等于除自身之外的正因子之和,即$\sigma(n)=2n$.

例如$6=1+2+3$,$28=1+2+4+7+14$,6与28是完全数.对于完全数已经得到了很好的结果.

定理 2.14. p为素数.如果2^p-1也是素数,则$2^{p-1}(2^p-1)$是完全数.

证明 p与2^p-1都是素数,由$2^{p-1}<2^p-1$知,$(2^{p-1},2^p-1)=1$.σ是积性函数且

$$\sigma\left(2^{p-1}\right)=\frac{2^p-1}{2-1}=2^p-1,\quad \sigma\left(2^p-1\right)=\left(2^p-1\right)+1=2^p,$$

$$\begin{aligned}\sigma(n)&=\sigma\left(2^{p-1}\left(2^p-1\right)\right)=\sigma\left(2^{p-1}\right)\sigma\left(2^p-1\right)\\&=\left(2^p-1\right)\cdot 2^p=2n.\end{aligned}$$

它说明$2^{p-1}(2^p-1)$是完全数.

定理 2.15. n是一个偶完全数,必有$n=2^{p-1}\cdot(2^p-1)$,其中p和2^p-1均为素数.

证明 n为偶完全数,可以表示成$n=2^k\cdot m$,其中$2\nmid m$,$k\geqslant 1$.根据完全数的定义$\sigma(n)=2n$,即

$$2^{k+1}\cdot m=\sigma\left(2^k\cdot m\right)=\sigma\left(2^k\right)\sigma(m)=\left(2^{k+1}-1\right)\cdot(m+l).$$

解出$m=(2^{k+1}-1)\cdot l$,这里l是m的小于m的因子之和并且l本身也是m的因子.所以只能$l=1$.从而$m=2^{k+1}-1$,$\sigma(m)=m+1$.这说明m是素数.假设$k+1$不是素数,$k+1=c\cdot d$, $m=2^{k+1}-1=2^{c\cdot d}-1=\left(2^c-1\right)\left(2^{c(d-1)}+2^{c(d-2)}+\cdots+1\right)$,这与$m$是素数矛盾,故不可能.所以,$k+1$为素数$p$. 综上分析知$n=2^{p-1}\left(2^p-1\right)$,其中$p$和$2^p-1$均为素数.

形如2^p-1的素数叫作Mersenne数,截至1985年找到的最大Mersenne数为$2^{216091}-1$.目前仅发现51个梅森素数,最大的是$2^{82589933}-1$,有24862048位。

2.6 原根与指数

本节我们要解同余方程$x^n\equiv c(\bmod m)$.当$(c,m)=1$时,x_0是$x^n\equiv c(\bmod m)$的一个特解,而y是$x^n\equiv 1(\bmod m)$的解,则$x\equiv yx_0(\bmod m)$是$x^n\equiv c(\bmod m)$的解.反过来$x^n\equiv c(\bmod m)$的每个解都可以写成yx_0形式,其中y是$x^n\equiv 1(\bmod m)$的解.所以,解同余方程$x^n\equiv c(\bmod m)$,只要找到一个特解x_0,并用x_0乘以$x^n\equiv 1(\bmod m)$的全部解就得到了$x^n\equiv c(\bmod m)$的全部解.

下面我们就来研究$x^n\equiv 1(\bmod m)$的解.为此引进阶、原根及指数的概念.

2.6.1 a模m的阶

当$(a,m)=1$时,考虑集合

$$A=\{n\mid n\in\mathbf{Z}\text{且}a^n\equiv 1(\bmod m)\},$$

由欧拉定理知$\phi(m)\in A$且$\phi(m)>0$.那么集合A中一定存在最小正整数l.集合A显然有如下性质:

1° 若$n_1,n_2\in A$,则$n_1\pm n_2\in A$;

2° 若$n\in A,c\in\mathbf{Z}$则$cn\in A$;

3° 集合A是由l的整数倍数组成的,并且只由这些整数倍数组成,即$A=\{k\cdot l\mid k\in\mathbf{Z}\}$.

我们称l为a模m的阶.由集合A的性质知,当$(a,m)=1$时,a模m的阶为l,那么对每个满足$a^n\equiv 1(\bmod m)$的整数n均有$l\mid n$.特别地,$l\mid\phi(m)$.不难看出$a^{n_1}\equiv a^{n_2}(\bmod m)$当且仅当$n_1\equiv n_2(\bmod l)$.

推论 2.7. 若$(a,m)=1$,l为a模m的阶,则a^k模m的阶为$\frac{l}{(l,k)}$.

证明 首先看满足$\left(a^k\right)^j\equiv 1(\bmod m)$的$j$应具有什么性质.从集合$A$的性质知$l\mid k\cdot j$,即

$$\frac{l}{(l,k)}\mid\frac{k}{(l,k)}\cdot j,$$

由于$\left(\frac{l}{(l,k)},\frac{k}{(l,k)}\right)=1$,得到$\frac{l}{(l,k)}\mid j$,$a^k$的阶应是满足该性质最小的正整数,故$a^k$的阶为$\frac{l}{(l,k)}$.

2.6.2 原根

定义 2.8. 若$(g,m)=1$且g模m的阶为$\phi(m)$,则称g为模m的**原根**.

例如,2是模5的原根,$\phi(5)=4,2^4\equiv 1(\bmod 5)$.3是模7的原根,$\phi(7)=6$, $3^6\equiv 1(\bmod 7)$.但并不是所有m都有原根.例如$m=8,\phi(8)=\phi\left(2^3\right)=4$. $\{1,3,5,7\}$ 是模8的缩系,而1模8的阶为1;3,5,7模8的阶为2.任何与8互素的数均与且仅与$\{1,3,5,7\}$中的一个元素模8 同余,故其模8的阶与该元素相同.由此可知正整数8无原根.

取$0 \leqslant i, j \leqslant \phi(m)-1, i \neq j$,显然$g^i \not\equiv g^j (\bmod m)$, $\left\{g^0, g^1, \cdots, g^{\phi(m)-1}\right\}$构成模$m$的缩系.也就是说,$g$是模$m$的原根,每个与$m$互素的$a$均与且仅与某个$g^i$模$m$同余,其中$0 \leqslant i \leqslant \phi(m)-1$.模$m$的原根都在$\left\{g^0, g^1, \cdots, g^{\phi(m)-1}\right\}$中.若$(l, \phi(m))=1$,则$g^l$也是模$m$的原根.

下面接下去讨论哪些数有原根,其结论是所有的素数p都有原根,原根个数为$\phi(p-1)$.为此先给出两个引理.

引理 2.5. *若$f(x)$是n次整系数多项式,$f(x) \equiv 0(\bmod p)$至多有n个解.*

证明 $f(x)$是n次整系数多项式,$f(x)=a_n x^n+a_{n-1} x^{n-1}+\cdots+a_0$,其中$a_n \not\equiv 0(\bmod p)$.对$f(x)$的次数$n$进行归纳证明.

当$n=1$时,$a_1 x+a_0 \equiv 0(\bmod p)$且$a_1 \not\equiv 0(\bmod p)$,由定理2.7 知该线性同余方程有唯一解.命题成立.

假设$n=k$时,$a_k x^k+a_{k-1} x^{k-1}+\cdots+a_0 \equiv 0(\bmod p)$至多有$k$个解.现$n=k+1$.如果$f(x) \equiv 0(\bmod p)$无解,显然命题成立.如果$f(x) \equiv 0(\bmod p)$至少有一个解$r$,即$f(r) \equiv 0(\bmod p)$.

$$
\begin{aligned}
f(x) & \equiv f(x)-f(r) \\
& =a_{k+1}\left(x^{k+1}-r^{k+1}\right)+a_k\left(x^k-r^k\right)+\cdots+a_1(x-r) \\
& =(x-r) g(x)(\bmod p),
\end{aligned}
$$

其中$a_{k+1} \not\equiv 0(\bmod p)$, $g(x)$是k次整系数多项式.$f(x) \equiv(x-r) g(x) \equiv 0(\bmod p)$的任意解$s$使$(s-r) g(s)=0(\bmod p)$,即$s \equiv r(\bmod p)$或$g(s)=0(\bmod p)$,也就是说$s$或是$r$或是$g(s) \equiv 0(\bmod p)$的解.由归纳假设知后者至多有$k$个解,所以$f(x)$至多有$k+1$个解.命题对$n=k+1$也成立.

引理 2.6. *若$n \geqslant 1$,则$\sum_{d \mid n} \phi(d)=n$.*

证明 由$d \mid n$知$\frac{n}{d} \mid n$.故$\sum_{d \mid n} \phi(d)=\sum_{d \mid n} \phi\left(\frac{n}{d}\right)$.
考虑集合C_d,其中d是n的因子.

$$
\begin{aligned}
C_d & =\{m \mid 1 \leqslant m \leqslant n \text { 且}(m, n)=d\} \\
& =\left\{m \mid 1 \leqslant m \leqslant n \text { 且}\left(\frac{m}{d}, \frac{n}{d}\right)=1\right\},
\end{aligned}
$$

显然$|C_d| = \phi\left(\frac{n}{d}\right)$.$\{1, 2, \cdots, n\}$中每个元素均在且仅在一个$C_d$中,从而

$$n = \sum_{d|n} |C_d| = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d).$$

例如$n = 6$,n的因子分别为$1, 2, 3, 6$.集合$C_1 = \{1, 5\}$,$C_2 = \{2, 4\}$,$C_3 = \{3\}$,$C_6 = \{6\}$.

定理 2.16. *p为素数,$l \mid (p-1)$.那么模p阶为l的数恰好有$\phi(l)$个.*

证明 对于每个$l \mid (p-1)$,令模p阶为l的元素个数为$\psi(l)$.如果对某个l不存在模p阶为l的元素,那么$\psi(l) = 0$.如果存在a,a与p互素且a模p阶为l,即$a^l \equiv 1 (\bmod p)$.在集合$\{a^0, a^1, \cdots, a^{l-1}\}$中,由于各个元素的指数模$l$不同余,所以这些元素均模$p$不同余.而对于$0 \leqslant i \leqslant l-1$,

$$\left(a^i\right)^l = \left(a^l\right)^i \equiv 1 (\bmod p),$$

$a^0, a^1, \cdots, a^{l-1}$均是$x^l \equiv 1 (\bmod p)$的解.根据引理2.5,该同余方程至多有$l$个解.这说明$a^0, a^1, \cdots, a^{l-1}$是它的全部解,从推论2.7知$a^k$ 模p阶为l当且仅当$(k, l) = 1$.$\{0, 1, \cdots, l-1\}$中有$\phi(l)$个与l互素的数,所以$\{a^0, a^1, \cdots, a^{l-1}\}$中有$\phi(l)$个模$p$阶为$l$的数,即$\psi(l) = \phi(l)$.综上知,对任何$l \mid (p-1)$均成立$\psi(l) \leqslant \phi(l)$.

另一方面,根据费马定理$(a, p) = 1$,$a^{p-1} \equiv 1 (\bmod p)$.若$a$模$p$的阶为$t$,则必有$t \mid (p-1)$.满足该条件的$a$至少有$p-1$个.由前面假设$\psi(l)$是模$p$阶为$l$ 的元素个数.再由引理2.6得到

$$\sum_{l|(p-1)} \psi(l) \geqslant p - 1 = \sum_{l|(p-1)} \phi(l).$$

并推出$\psi(l) \geqslant \phi(l)$.

最后得到$\psi(l) = \phi(l)$,即模p阶为l的数恰好有$\phi(l)$个.

特别取$l = \phi(p)$,模p阶为$\phi(p)$的元素个数为$\phi(\phi(p)) = \phi(p-1)$.这说明有$\phi(p-1)$个模$p$的原根.例如37是素数,它的原根数为

$$\begin{aligned}\phi(\phi(37)) = \phi(36) &= \phi\left(2^2\right)\phi\left(3^2\right) \\ &= 2^1 \cdot (2-1) \cdot 3^1(3-1) = 12.\end{aligned}$$

通过简单计算知1是2的原根,3是4的原根,可以证明:m有原根当且仅当$m = 2$, 4, p^k, $2 \cdot p^k$,其中p是奇素数,k为正整数.再次说明8没有原根.

2.6.3 指数

设g为模p的原根,$\{g^0, g^1, \cdots, g^{p-2}\}$为模$p$的缩系.对每个整数$n$,若$(n,p)=1$,则存在$m, 0 \leqslant m \leqslant p-2$,使得$n \equiv g^m (\mathrm{mod}\ p)$成立.我们称$m$为$n$(对于原根$g$)的模$p$指数,并记为$\mathrm{ind}_g\, n$.

若有l使$n \equiv g^l (\mathrm{mod}\ p)$,而$n \equiv g^{\mathrm{ind}\ g^n} (\mathrm{mod}\ p)$,所以$l \equiv \mathrm{ind}_g\, n (\mathrm{mod}\ p-1)$.

模p指数有如下性质:

1° $p \nmid ab, \mathrm{ind}_g\, ab \equiv \mathrm{ind}_g\, a + \mathrm{ind}_g\, b (\mathrm{mod}\ p-1)$;

2° $p \nmid a, \mathrm{ind}_g\, a^l \equiv l \cdot ind_g a\, (\mathrm{mod}\ p-1)$.

这些性质从指数的定义很容易证出.不难看出模p指数与对数函数有相类似的性质.

定理 2.17. 若$(n,p)=1, g$为模p的原根,则同余方程$x^k \equiv n\, (\mathrm{mod}\ p)$有解当且仅当$(k, p-1) \mid \mathrm{ind}_g\, n$.当条件满足时,该方程有$(k, p-1)$个解.

证明 令$y = \mathrm{ind}_g\, x, x \equiv g^y\, (\mathrm{mod}\ p)$ 代入$x^k \equiv n\, (\mathrm{mod}\ p)$得到$g^{yk} \equiv g^{\mathrm{ind}_g n}\, (\mathrm{mod}\ p)$,即$yk \equiv \mathrm{ind}_g\, n\, (\mathrm{mod}\ p-1)$. 该方程有解$y$当且仅当$(k, p-1) \mid ind_g n$,并且条件满足时有$(k, p-1)$个解.它们是

$$y \equiv y_1, y_2, \cdots, y_{(k,p-1)}\, (\mathrm{mod}\ p-1).$$

那么$x \equiv g^{y_1}, g^{y_2}, \cdots, g^{y_{(k,p-1)}}\, (\mathrm{mod}\ p)$是$x^k \equiv n\, (\mathrm{mod}\ p)$的解.

例 2.10. 解同余方程$x^8 \equiv 3\, (\mathrm{mod}\ 11)$.

解 查原根指数表知11的最小原根是2, 3对于原根2的模11指数是8,令$y = \mathrm{ind}_2\, x$,先解$8 \cdot y = \mathrm{ind}_2\, 3 = 8\, (\mathrm{mod}\ 10)$.因$(8,10)=2$,该线性同余方程有2个模10不同余的解,它们是

$$y \equiv 1, 6\, (\mathrm{mod}\ 10),$$

由此得到$x \equiv 2^1, 2^6 \equiv 2, 9\, (\mathrm{mod}\ 11)$,它们是$x^8 \equiv 3\, (\mathrm{mod}\ 11)$的解.

例 2.11. 解线性同余方程$5x \equiv 7\, (\mathrm{mod}\ 11)$.

解 由$5x \equiv 7\, (\mathrm{mod}\ 11)$,以及11的最小原根为2知

$$\mathrm{ind}_2 5 + \mathrm{ind}_2 x \equiv \mathrm{ind}_2 7 \pmod{10}.$$

从原根指数表知$\mathrm{ind}_2 5 = 4, \mathrm{ind}_2 7 = 7$,代入上式得到$\mathrm{ind}_2 x \equiv 3 \pmod{10}$,故$x \equiv 8 \pmod{11}$是原同余方程的解.

例 2.12. 解同余方程$x^8 \equiv 3 \pmod{143}$.

解 因$143 = 11 \cdot 13$.要解$x^8 \equiv 3 \pmod{143}$就是要解同余方程组

$$\begin{cases} x^8 \equiv 3 \pmod{11} \\ x^8 \equiv 3 \pmod{13}. \end{cases}$$

由例2.10知$x^8 \equiv 3 \pmod{11}$的解为$x \equiv 2, 9 \pmod{11}$.用例2.10中的方法解出$x^8 \equiv 3 \pmod{13}$的解为$x \equiv 4, 6, 7, 9 \pmod{13}$.

下面求解

$$\begin{cases} x \equiv a \pmod{11} \\ x \equiv b \pmod{13}, \end{cases}$$

其中$a = 2, 9; b = 4, 6, 7, 9$.求解方法在2.3.4小节中已详述过,这里只给出结果$x = 13 \cdot 6 \cdot a + 11 \cdot 6 \cdot b \pmod{143}$.代入$a, b$的值,得到

$$x = \pm 9, \pm 20, \pm 35, \pm 46 \pmod{143}.$$

目前对给定素数p如何求出模p的原根尚无一般的方法.另外,给定一个整数a,它是哪些素数的原根也没有一般的方法.在使用时可在一般的数论书中查到小素数的原根及相应的指数表.表2.1给出了50以内的素数的最小原根及相应的指数.该表中第一行列出50以内的全部素数p,第一列是正整数n.素数p相应列中数值为1的元素对应的n值则是该素数的最小原根g,该列的其他元素则是$\mathrm{ind}_g n$.

表 2.1: 素数$p(\leqslant 50)$的最小原根和指数表

$\mathrm{ind}_g n$ \ p n	3	5	7	11	13	17	19	23	29	31	37	41	43	47
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	1	1	2	1	1	14	1	2	1	24	1	26	27	18
3		3	1	8	4	1	13	16	5	1	26	15	1	20
4		2	4	2	2	12	2	4	2	18	2	12	12	36
5			5	4	9	5	16	1	22	20	23	22	25	1
6			3	9	5	15	14	18	6	25	27	1	28	38
7				7	11	11	6	19	12	28	32	39	35	32
8				3	3	10	3	6	3	12	3	38	39	8
9				6	8	2	8	10	10	2	16	30	2	40
10				5	10	3	17	3	23	14	24	8	10	19
11					7	7	12	9	25	23	30	3	30	7
12					6	13	15	20	7	19	28	27	13	10
13						4	5	14	18	11	11	31	32	11
14						9	7	21	13	22	33	25	20	4
15						6	11	17	27	21	13	37	26	21
16						8	4	8	4	6	4	24	24	26
17							10	7	21	7	7	33	38	16
18							9	12	11	26	17	16	29	12
19								15	9	4	35	9	19	45
20								5	24	8	25	34	37	37
21								13	17	29	22	14	36	6
22								11	26	17	31	29	15	25
23									20	27	15	36	16	5
24									8	13	29	13	40	28
25									16	10	10	4	8	2

表 2.2: 续表2.1

$\mathrm{ind}_g\mathrm{n}$ \ p / n	3	5	7	11	13	17	19	23	29	31	37	41	43	47
26									19	5	12	17	17	29
27									15	3	6	5	3	14
28									14	16	34	11	5	22
29										9	21	7	41	35
30										15	14	23	11	39
31											9	28	34	3
32											5	10	9	44
33											20	18	31	27
34											8	19	23	34
35											19	21	18	33
36											18	2	14	30
37												32	7	42
38												35	4	17
39												6	33	31
40												20	22	9
41													6	15
42													21	24
43														13
44														43
45														41
46														23

习题

1. 证明:

(1) 若$a|b, a>0$,则$(a,b)=a$;

(2) $((a,b),b)=(a,b)$.

2. 证明:

(1) 对所有$n>0$成立$(n,n+1)=1$;

(2) 当$n>0$时,$(n,n+k)$可取什么值?

3. 求x和y使得:

(1) $314x+159y=1$;

(2) $3141x+1592y=1$.

4. 证明: 对于所有$n>0$,有$6 \mid \left(n^3-n\right)$.

5. 证明: 若对于某个m有$10 \mid (3^m+1)$,则对所有$n>0, 10 \mid \left(3^{m+4n}+1\right)$.

6. 求2345及3456两个数的素数分解式.

7. 证明: 当$n>0$时,$n(n+1)$不是一个平方数.

8. 令$n=5!+1$,证明$n+1, n+2, n+3, n+4$均为合数.

9. 求下列方程的所有整数解

(1) $x+y=2$;

(2) $2x+y=2$;

(3) $15x+16y=17$.

10. 求下列方程的负整数解:

(1) $6x-15y=51$;

(2) $6x+15y=51$.

11. 用30张票面值为5分、1角、2角5分的纸币,换5元钱.问有多少种不同的兑换方法?

12. 某人用0.99元买了苹果和桔子共12个,每只苹果比每只桔子贵3分钱,买的苹果数多于桔子数.问苹果和桔子各买多少个?

13. 若$k \equiv 1 \pmod 4$,则$6k+5$模4等于多少?

14. 证明: 每个大于3的素数模6或与1同余或与5同余.

15. 证明: 相继的两个立方数之差不能被3整除.

16. 证明: 若一个整数的各位数字之和能被3整除,那么该数也能被3整除.

17. 证明:

(1) $10^k \equiv (-1)^k \pmod{11}, k = 0, 1, 2, \cdots;$

(2) 推导出一个整数能被11整除的判别法.

18. 解下列线性同余方程:

(1) $2x \equiv 1 \pmod{17}$; (2)$3x \equiv 6 \pmod{18}$;

(3) $4x \equiv 6 \pmod{18}$; (4)$3x \equiv 1 \pmod{17}$.

19. 解下列同余方程组:

(1) $\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 1 \pmod{3} \end{cases}$ (2) $\begin{cases} x \equiv 31 \pmod{41} \\ x \equiv 59 \pmod{26} \end{cases}$

(3) $\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 1 \pmod{3} \\ x \equiv 6 \pmod{7} \end{cases}$ (3) $\begin{cases} 2x \equiv 1 \pmod{5} \\ 3x \equiv 2 \pmod{7} \\ 4x \equiv 1 \pmod{11} \end{cases}$

20. 试求同时满足如下两条要求的正整数x, y, z:

(1) 它们分别乘以$3, 5, 7$所得乘积模20的余数是公差为1的算术级数;

(2) 它们分别乘以$3, 5, 7$所得乘积除以20得到的商分别等于(1) 中的相应的余数.

21. 求满足$2 \mid n, 3 \mid (n+1), 4 \mid (n+2), 5 \mid (n+3), 6 \mid (n+4)$的最小整数$n (> 2)$.

22. 计算$\phi(42), \phi(420), \phi(4200)$.

23. 小于18且与18互素的正整数是哪些? 当$m = 18, a = 5$时,验证引理2.1.

24. p为素数,$(m, n) = p$,问$\phi(mn)$与$\phi(m)\phi(n)$之间有什么关系?

25. 证明:

(1) 如果$6 \mid n$,则$\phi(n) \leqslant \frac{n}{3}$;

(2) 如果$n-1$和$n+1$均为素数,$n > 4$,则$\phi(n) \leqslant \frac{n}{3}$.

26. (1) 验证$1+2 = \frac{2}{3}\phi(3), 1+3 = \frac{4}{2}\phi(4), 1+2+3+4 = \frac{5}{2}\phi(5), 1+5 = \frac{6}{2}\phi(6), 1+2+3+4+5+6 = \frac{7}{2}\phi(7), 1+3+5+7 = \frac{8}{2}\phi(8)$;

(2) 推想一个定理;

(3) 证明你的定理.

27. 314^{159}除以7的余数是多少?

28. 7^{355}的末位数是什么? 末两位数是什么?

29. p为素数.证明: 对非负整数k, $(k+1)^p-k^p\equiv 1\,(\bmod\ p)$,并由此推出费马定理.

30. 假设p是一个奇素数.证明:

(1) $1^{p-1}+2^{p-1}+\cdots+(p-1)^{p-1}\equiv -1\,(\bmod\ p)$;

(2) $1^p+2^p+\cdots+(p-1)^p\equiv 0\,(\bmod\ p)$.

31. 计算$d(42), d(420), d(4200), \sigma(42), \sigma(420), \sigma(4200)$.

32. 求具有60个因子的数$n\left(n<10^4\right)$.

33. 证明

$$\sum_{d\mid n}\frac{1}{d}=\frac{1}{n}\sigma(n).$$

34. 证明所有的偶完全数以6或8结尾.

35. 若n为偶完全数,$n>6$,证明$n\equiv 1\,(\bmod\ 9)$.

36. 证明

$$\sum_{p\leqslant x}\sigma(p)=\sum_{p\leqslant x}\phi(p)+\sum_{p\leqslant x}d(p).$$

37. 求$2, 4, 7, 8, 11, 13, 14$模15的阶是多少?

38. (1) 算出关于原根2的最小指数$(\bmod\ 29)$;

(2) 利用此表解$9x\equiv 2\,(\bmod\ 29)$;

(3) 利用此表解$x^9\equiv 2\,(\bmod\ 29)$.

39. $457^{911}\equiv 1\,(\bmod\ 10021)$对不对? (这里$457, 911$都是素数,$10021=11\cdot 911$.)

40. 求37的12个原根.

41. 证明: 若p, q为奇素数,$q\mid(a^p+1)$,则有$q\mid(a+1)$或$q\mid(2kp+1)$,其中k为某个整数.

42.证明: 若a模p的阶为3,则$a+1$模p的阶为6.