第四章 数论基础

“数论”是一门古老而充满现代魅力的数学学科。在编著于纪元前一世纪前后的我国数学名著《九章算术》中就讨论了整数，介绍了辗转相除法；在成书于公元四世纪的《孙子算经》中给出了被世界数学界誉为“中国剩余定理”的孙子定理。

数论是研究数的性质的学科。我国对数论的研究有许多极其光辉的成就，古代的孙子定理、商高定理(勾股数)、圆周率计算，从上个世纪三十年代开始的对解析数论、丢番图方程、一致分布研究的贡献，华罗庚先生在三角和估计与堆垒素数论研究方面的卓越成果，以及王元、潘承洞、丁夏畦、尹文霖特别是陈景润在求证哥德巴赫猜想上作出的成绩斐然的工作，陈景润的“每一充分大的偶数都是一个素数及一个不超过两个素数的乘积之和”的结果仍然是这个问题当今最好的求解结果。

在计算机的计算模型、硬件体系结构和软件的设计与实现、代数编码、计算机通信安全与密码学等方面，都有着数论知识的广泛应用。数论这门学科随着 20 世纪中期以后计算机技术的飞速发展焕发出了青春的力量。

本章介绍数论的一些基础知识，如整除性、辗转相除、因数分解及同余方程等，且约定凡述及数，若未特别说明，都指整数。

4-1 整除及辗转相除

定义 4.1.1 设 a、b 是任意整数，如果存在整数 c，使有 a=bc，则称 a 是 b 的倍数，b 是 a 的因数；亦说 a 被 b 整除，或 b 整除 a；记为 b|a .

显然，任意整数整除 0，特别 0|0，1(或-1)整除任意整数。

如果 b 不能整除 a，那么称带余除法。

定理 4.1.1 设 a、b 是任意整数且 b≠0, 则惟一存在整数 q 和 r, 使得 0≤r＜|b|, a=qb+r. 若 r＞0, 则称 q 为带余除法的不完全商, 称 r 为 b 除 a 的余数。

证明:

1) 证存在整数 q 和 r, 使得 0≤r＜|b|, a=qb+r. 考虑 b: 若 b＞0, 则 b 的倍数数可递增排列为: …,-4b,-3b,-2b,-b,0.,b,2b,3b,4b,…; 若 b＜0, 则 b 的倍数数可递增排列为: …,4b,3b,2b,b,0,-b,-2b,-3b,-4b,… .有两种情况: (1) 存在整数 q, 使得 a=qb, 此时 r =0, 问题得证。(2) 当 b＞0 时, 存在整数 q, 使得 qb≤a＜(q+1)b; 当 b＜0 时, 存在整数 q, 使得 qb≤a＜(q-1)b. 因而有 a=qb+r (*), 0≤r＜|b| .

2) 证存在的整数对q和r惟一。如果另有q'和r'满足a= q'b+r' (**), 0≤r'＜|b|, 则由式(**)-(*)得r'-r=(q - q')b, 并有|r'-r|=| q'-q|b. 鉴于|r' -r|＜|b|, |q' -q|≥0 且皆为整数, 固必有|q' -q| =0, 从而|r' -r|=0, 即q' =q, r' =r. 惟一性成立。

下面介绍求两个正整数的最大公约数的辗转相除法。

设a、b是正整数, 且a＞b. 为求a,b的最大公约数, 首先以b除a, 得: a=q_1b+r_1, 式中q_1和r_1为非负整数, 0≤r_1＜b. 若r_1=0, 则a=q_1b, a和b的最大公约数(a,b)=b; 若r_1≠0, 则 0＜r_1＜b, 以r_1除b, 得: b=$q_2$$r_1$+$r_2$, 式中$q_2$和$r_2$为非负整数, 0≤$r_2$＜$r_1$. 若$r_2$=0, 则b=$q_2$$r_1$, b和$r_1$的最大公约数(b,$r_1$)=$r_1$; 若$r_2$≠0, 则 0＜$r_2$＜$r_1$, 以$r_2$除$r_1$且得: r_1=$q_3$$r_2$+$r_3$, 式中$q_3$和$r_3$为非负整数, 0≤$r_3$＜$r_2$. 若$r_3$=0, 则($r_1$,$r_2$)=$r_2$. 从式a=$q_1$b+$r_1$, b=$q_2$$r_1$+$r_2$和$r_1$=$q_3$$r_2$+$r_3$及“若整数d可整除三个等式每个等式中的某两项, 则必可整除其第三项”知(a,b)= (b,r_1)=(r_1,r_2). 若 0＜r_3＜r_2, 则再以r_3除r_2, 并继续上述讨论, ……, 一直辗转相除下去。由于b＞r_1＞r_2＞r_3＞…和所有r_i(i=1,2,3,…)都是非负整数, 所以必存在正整数n, 使得经过n+1次辗转相除后有r_{n+1}=0, 而r_n ≠ 0. 于是(a,b)=(b,r_1)=(r_1,r_2)=…=(r_{n-1},r_n)=r_n . 显然, 由定理 4.1.1, 运用辗转相除

法可求任意两个整数的最大公约数。

例 4.1.1 求 6731 和 2809 的最大公约数。

解: 由 6731=2×2809+1113, 2809=2×1113+583, 1113=1×583+530, 583=1×530+53, 530=10×53+0 知(6731,2809)=53.

定理 4.1.2 整数 a,b 的最大公约数 d=(a,b)可以表示为 a,b 的倍数和, 即存在整数 s,t 使有 d=sa+tb.

证明: 设在求取$d(=(a,b)=r_n)$的辗转相除过程中得:

$$a=q_1b+r_1,$$
$$b=q_2r_1+r_2,$$
$$r_1=q_3r_2+r_3$$
$$\cdots\cdots\cdots\cdots$$
$$r_{i-2}=q_ir_{i-1}+r_i,$$
$$\cdots\cdots\cdots\cdots$$
$$r_{n-2}=q_nr_{n-1}+r_n,$$
$$r_{n-1}=q_{n+1}r_n.$$

为证定理, 只需证明对每个正整数$i(i=1,2,3,\ldots,n)$, 都存在整数s'和t', r_i总可以表示为$r_i=s'a+t'b$的形式。

当i=1 时, $r_1=a-q_1b=1a+(-q_1)b$.

当i=2 时, $r_2=b-q_2r_1=b-q_2(a-q_1b)=(-q_2)a+(1+q_1q_2)b$.

设对r_{i-1}, r_{i-2},$3\leqslant i\leqslant n$, 分别有整数s', t'和s'', t''使得$r_{i-1}=s'a+t'b$, $r_{i-2}=s''a+t''b$, 则r_i也可表示为同样的形式:

$r_i=-q_ir_{i-1}+r_{i-2}=-q_i(s'a+t'b)+s''a+t''b=(s''-s'q_i)a+(t'-t'q_i)b$.

由数学归纳法即知所证成立。

下面讨论如何使用矩阵知识, 构造定理 4.1.2 的结论式 d=sa+tb 中的 s 和 t.

改写并扩展定理 4.1.2 证明中的辗转相除式为:

$$\begin{pmatrix}a\\b\end{pmatrix}=\begin{pmatrix}q_1&1\\1&0\end{pmatrix}\begin{pmatrix}b\\r_1\end{pmatrix},$$

$$\begin{pmatrix} b \\ r_1 \end{pmatrix}=\begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} r_1 \\ r_2 \end{pmatrix},$$

… … … … … … … … ,

类而推之并得

$$\begin{pmatrix} a \\ b \end{pmatrix}=\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix}=A_i\begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix},$$

式中$A_i=\begin{pmatrix} T_i & V_i \\ S_i & U_i \end{pmatrix}=\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}$

且 $\begin{pmatrix} a \\ b \end{pmatrix}=\begin{pmatrix} T_i & V_i \\ S_i & U_i \end{pmatrix}\begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix}.$

考虑到 $\begin{vmatrix} q_1 & 1 \\ 1 & 0 \end{vmatrix}=\begin{vmatrix} q_2 & 1 \\ 1 & 0 \end{vmatrix}=\ldots=\begin{vmatrix} q_i & 1 \\ 1 & 0 \end{vmatrix}=-1$ 及$|A_i|=(-1)^i$知存在

$\begin{pmatrix} T_i & V_i \\ S_i & U_i \end{pmatrix}^{-1}$，且$\begin{pmatrix} T_i & V_i \\ S_i & U_i \end{pmatrix}^{-1}=\frac{A_i^*}{|A_i|}=\begin{pmatrix} (-1)^i U_i & (-1)^{i+1}V_i \\ (-1)^{i+1}S_i & (-1)^i\ T_i \end{pmatrix}$

于是有$\begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix}=\begin{pmatrix} T_i & V_i \\ S_i & U_i \end{pmatrix}^{-1}\begin{pmatrix} a \\ b \end{pmatrix}=\begin{pmatrix} (-1)^i U_i & (-1)^{i+1}V_i \\ (-1)^{i+1}S_i & (-1)^i\ T_i \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}$

并得 $r_i=(-1)^{i+1}S_ia+(-1)^iT_ib$. 特别还有$r_n=(-1)^{n+1}S_na+(-1)^nT_nb$. 即定理 4.1.2 的结论式$d=sa+tb$中的$s=(-1)^{n+1}S_n$, $t=(-1)^nT_n$.

怎样简便地计算S_i和T_i呢?

注意到 $\begin{pmatrix} T_i & V_i \\ S_i & U_i \end{pmatrix}=\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}$

$$=\begin{pmatrix} T_{i-1} & V_{i-1} \\ S_{i-1} & U_{i-1} \end{pmatrix}\begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}$$

我们有$U_i=S_{i-1}$，$V_i=T_{i-1}$，因而有$U_{i-1}=S_{i-2}$，$V_{i-1}=T_{i-2}$ $(i>2)$(*); 并且还有$S_i=q_iS_{i-1}+U_{i-1}$，$T_i=q_iT_{i-1}+V_{i-1}(i\geq 2)$(**). 将式(*)代入式(**)

得$S_i=q_iS_{i-1}+S_{i-2}$, $T_i=q_iT_{i-1}+T_{i-2}$ (i＞2)(***). 补充定义$U_1=S_0$,$V_1=T_0$, 则式(*)和式(***)对i≥2 也成立; 而且从

$$\begin{pmatrix} T_1 & V_1 \\ S_1 & U_1 \end{pmatrix}=\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix},$$

得递推公式$S_i=q_iS_{i-1}+S_{i-2}$, $T_i=q_iT_{i-1}+T_{i-2}$ (i≥2) 的初始值条件$S_0=0$, $S_1=1$; $T_0=1$, $T_1=q_1$.

例 4.1.2 将 6731 和 2809 的最大公约数表示为 6731 和 2809 的倍数和。

解: 由辗转相除法求 6731 和 2809 的最大公约数, 逐次得不完全商及余数并计算S_i和T_i列表如下:

i	0	1	2	3	4	5
r_i		1113	583	530	53	0
q_i		2	2	1	1	10
S_i	0	1	2	3	5	
T_i	1	2	5	7	12	

从表中得(6731,2809)= r_4=53, 且 53= $r_4=(-1)^{4+1}S_4a+(-1)^4T_4b=-5\times 6731+12\times 2809$.

练习 4-1

1. 求 5709 和 1331 的最大公约数并将之表示为 5709 和 1331 的倍数和。

2. 求 27090,21672 和 11352 的最大公约数。

3. 记T_i为$[q_1, q_2,\ldots, q_i]$，求证$S_i=[q_2, q_3,\ldots, q_i]$.

提示:

1. 利用例 4.1.2 的方法, 可求解如下:

i	0	1	2	3	4	5
r_i		385	176	33	11	0

q_i		4	3	2	5	3
S_i	0	1	3	7	38	
T_i	1	4	13	30	163	

因而(5709,1331)=11=$(-1)^{4+1}$38×5709+$(-1)^4$163×1331.

2. 用同样的方法, 首先求得(27090,21672)=5418, 然后再求得(5418,11352)=258, 因而知 27090, 21672 和 11352 的最大公约数是 258.

3. 从定理 4.1.2 的矩阵形式的讨论, 已有

$$\begin{pmatrix} T_i & T_{i-1} \\ S_i & S_{i-1} \end{pmatrix}=\begin{pmatrix} T_i & V_i \\ S_i & U_i \end{pmatrix}=\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix},$$

按题意, $\begin{pmatrix} T_i & T_{i-1} \\ S_i & S_{i-1} \end{pmatrix}=\begin{pmatrix} [q_1,q_2,...,q_i] & [q_1,q_2,...,q_{i-1}] \\ S_i & S_{i-1} \end{pmatrix}$

$$=\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} [q_2,q_3,...,q_i] & * \\ * & * \end{pmatrix}$$

$$=\begin{pmatrix} * & * \\ [q_2,q_3,...,q_i] & * \end{pmatrix}.$$

于是有S_i=[q_2, q_3,…, q_i].

4-2 算术基本定理

定义 4.2.1 称正整数 n 为质数(或素数), 如果 n≠1 且 n 无 1 与自身之外的其它正因数; 非 1 和非质数的正整数称合数。

若整数 a,b 除±1 外再无其它公因数, 则称 a,b 互质。显然, 质数 p 与整数 a 互质当且仅当 p 不能整除 a . 由定义，正整数 a 是合数当且仅当 a 具有大于 1 且小于自身的正因数。

引理 4.2.1 设a_1, a_2,…, a_n均为非 1 整数且质数p整除其乘积 a_1 a_2…a_n, 则p整除a_1, a_2,…, a_n之一。

证明: 事实上若质数p不能整除整数a_i, i=1,2,…,n, 则(p,

$a_i)=1$，由定理4.1.2知存在整数s_i,t_i使有$1=s_ip+t_ia_i$, i=1,2,…,n.将这n个式子的左边，右边分别相乘并整理得:$1=Sp+Ta_1a_2…a_n$，即$(p,a_1a_2…a_n)=1$.这与质数p整除$a_1a_2…a_n$矛盾，所以引理结论成立。

例 4.2.1 质数 7 整除 420=2×3×5×14，则 7 整除 2,3,5,14 中之 14 .

定理 4.2.1 (算术基本定理)若不计质因数的次序，则洽有一种方法将大于 1 的整数 n 分解成其质因数的连乘积(亦称 n 的素分解)。

证明：首先运用数学归纳法证明，大于1的整数n可以分解成它的质因数的连乘积。当 n=2 时, 2 是质数, n 分解成了质因数的乘积；设 n 小于正整数 m(≥3)时，可以分解成它的质因数的连乘积，则可证 n=m 时也能分解成其质因数的连乘积。若 m 是质数，则m=m已分解成了它的质因数的乘积；若m是合数,则m具有因数 a,1＜a＜m，且 m=ab，1＜b＜m .由于 a,b＜m，由归纳法假设 a,b 都可以分解成它的质因数的连乘积，因而 m=ab 可以分解成其质因数的连乘积。

而后证明n分解成其质因数的连乘积的分解方法惟一。如果n有质因数的连乘积分解式：$n=p_1p_2…p_k$，$n=q_1q_2…q_t$ (*)则可证k=t且当不考虑次序时$p_1p_2…p_k$和$q_1q_2…q_t$完全一样。因为$p_1p_2…p_k=q_1q_2…q_t$，所以质数$p_1|q_1q_2…q_t$，由引理 4.2.1 知p_1整除q_1，q_2,…，q_t之一，无妨记$p_1|q_1$，由于p_1,q_1都是质数，必有$p_1=q_1$；(*)式即$p_1p_2…p_k=q_1q_2…q_t$，在此等式中消去p_1和q_1得$p_2…p_k=q_2…q_t$(**)并重复上述讨论有$p_2=q_2$及$p_3…p_k=q_3…q_t$ (***)；…；注意到$p_1,p_2,…,p_k$和$q_1,q_2,…,q_t$都是质数，重复讨论到最后一步只能是$p_k=q_t$，即k=t且当不考虑次序时$p_1p_2…p_k$和$q_1q_2…q_t$完全一样。如果进一步将$p_1p_2…p_k$中的相同素数的积合并写为幂的形式，即得n的素分解的标准形式：$n=p_{i_1}^{k_1}p_{i_2}^{k_2}…p_{i_t}^{k_t}$，$0\leqslant k_i\leqslant k$, i=1,2,…,t，且$k_1+k_2+…+k_t=k$.

例 4.2.2 求整数 1996 的素分解。

解: $1996=2\times998=2\times2\times499=2^2\times499$.

例 4.2.3 质数的个数无穷。

证明: (Euclid方法)设质数的个数有n个, 可记为$p_1, p_2,\ldots, p_n$, 考虑正整数$m=p_1p_2\ldots p_n+1$, 由于$p_1, p_2,\ldots, p_n$都不能整除m, 所以m无 1 与自身以外的正因数, 因而m是质数。但m不同于$p_1, p_2,\ldots, p_n$, 这与质数只有$p_1, p_2,\ldots, p_n$等n个矛盾, 所以质数的个数无穷。

质数的个数无穷, 但它们在正整数序列中的分布情况怎样? 这是数论中一个十分有趣的问题。D.Zagier 在 1977 年 8 月给出了 50000000 以内的质数表。如果记 $\pi(n)$为 1～n 的质数个数, 从 D.Zagier 的表中可见: $\pi(100)=25, \pi(1000)=168, \pi(10000)=1229, \pi(100000)=9592$.

在正整数序列中, 人们发现了许多双生素数, 即正整数序列中差为±2 的相邻质数对。如: 3,5; 5,7; 11,13; 17,19; 29,31; 41,43; 59,61; 71,73; 101,103; … . 双生素数对的个数无限吗?我们不得而知。

Eratosthenes 给出一个求 $\pi(n)$个质数的方法:

(1) 列出 2～n 的全体整数;

(2) 对 m≤n, 找出小于等于 $\sqrt{m}$ 的全部质数;

(3) 在(1)中, 消去(2)中质数的大于 1 的倍数数;

(4) 反复执行(2)和(3), 剩下的数就是所求数。

例 4.2.4 利用 Eratosthenes 的方法, 确定 499 是质数。

解: 对 $\sqrt{499}$ 取整[$\sqrt{499}$]=22, 小于等于 22 的质数有 2,3, 5,7,11,13,17 和 19. 由于整数 499 不是这些质数的倍数, 在执行 Eratosthenes 算法后, 499 是剩下的数, 所以 499 是质数。

有时我们只关心一个整数 a 被一个正整数 m 整除时的余数 r(0≤r＜m). 例如 2004 年是农历甲申年, 121 年后是农历乙酉年。因为农历纪年法, 60 年一个循环, 60 除 121 余 1, 即 121 年

后的农历纪年是甲申年的下一年---乙酉年。

定义 4.2.2 设 a,b 是整数, m 是正整数, 若 m 分别整除 a,b 时有相同的余数 r, 则称 a 与 b 模 m 同余, 记为 $a\equiv b(\mathrm{mod}\ m)$.

显然, $a\equiv b(\mathrm{mod}\ m)$当且仅当 $m|(a-b)$.

定理 4.2.2 设 a,b 是整数, m 是正整数, 则 $a\equiv b(\mathrm{mod}\ m)$当且仅当存在整数 k, 使有 $a=b+km$.

证明: 设$a\equiv b(\mathrm{mod}\ m)$, 则存在整数$q_1$和$q_2$, 并成立$a=q_1m+r$, $b=q_2m+r$, 于是$a-b=(q_1-q_2)m=km$, 即有$a=b+km$; 反过来, 若有$a=b+km$, 则$a-b=km$, 因而$m|(a-b)$, 所以$a\equiv b(\mathrm{mod}\ m)$. 因为如果$m|(a-b)$但a与b却并不同余, 则可记$a=q_1m+r_1$, $0\leqslant r_1<m$, $b=q_2m+r_2$, $0\leqslant r_2<m$且$r_1\neq r_2$, 于是$a-b=(q_1-q_2)m+(r_1-r_2)$, $0<|r_1-r_2|<|m|$.等式中的$a-b$和$(q_1-q_2)m$可被m整除, 而r_1-r_2却不是m的倍数, 所以m不能整除a-b. 这与$m|(a-b)$矛盾, 故当$m|(a-b)$时, $a\equiv b(\mathrm{mod}\ m)$.

例 4.2.5 判断 172 与 52 是否模 6 同余。

解: 由于 $172=52+20\times 6$, 所以 172 与 52 模 6 同余。

定理 4.2.3 设 a,b,c,d 是整数, m 是正整数. 若 $a\equiv b(\mathrm{mod}\ m)$且 $c\equiv d(\mathrm{mod}\ m)$, 则$(a+c)\equiv(b+d)\ (\mathrm{mod}\ m)$, $ac\equiv bd\ (\mathrm{mod}\ m)$.

证明: 设$a\equiv b(\mathrm{mod}\ m)$且$c\equiv d(\mathrm{mod}\ m)$, 由定理 4.2.2 知存在$k_1$和$k_2$使成立$a=b+k_1m$, $c=d+k_2m$. 因而有

$$a+c=(b+d)+(k_1+k_2)m,\quad ac=bd+(bk_2+dk_1+k_1k_2)m$$

即有$(a+c)\equiv(b+d)\ (\mathrm{mod}\ m)$, $ac\equiv bd\ (\mathrm{mod}\ m)$.

例 4.2.5 证明 2004 年 1 月 1 日与 7 月 1 日同为星期四。

解: 记 2004 年 1 月 1 日为 a, 则 $a\equiv 4(\mathrm{mod}\ 7)$. 2004 年 1 月 1 日到 7 月 1 日共经历 182 天且 $182\equiv 0(\mathrm{mod}\ 7)$, 故由$(a+182)\equiv(4+0)(\mathrm{mod}\ 7)$知 2004 年 7 月 1 日是星期四。

练习 4-2

1. 运用算术基本定理, 设计求取任意两个大于 1 的正整数 m,n 的最大公约数(m,n)和最小公倍数[m,n]的方法, 并用此方法计算(51420,13310)和[30261,55020].

2. 证明: 由辗转相除法所确定的定理 4.1.2 中的s, t 即S_i和T_i互素。

3. 设 a,b,n 是正整数, 证明:

(1) $(a^n,b^n)=(a,b)^n$;

(2) (na,nb)=n(a,b) .

并以此结论求(64,216)和(6400,21600).

4. 设 a,b,c 是整数, m 是正整数, 举例说明 ac≡bc (mod m) 未必蕴涵 a≡b(mod m).

5. 记 LSSX 为离散数学。在以英文字母传输信息时, 规定以 0,1,2,…,25 分别代表 A,B,C,…,Z 等 26 个英文字母, 并约定在具体传输时, 对代表字母的数字 n 首先作 n+16 再取模 26 运算后进行。计算表示离散数学的字符串“LSSX”的传输结果(接收字)。

提示:

1. 运用算术基本定理, 求取任意两个大于 1 的正整数 m,n 的最大公约数(m,n)和最小公倍数[m,n]的方法是: 对 m,n 分别作素分解, 并记为具有相同素因子的标准形式

$$n=p_{i_1}^{k_1}p_{i_2}^{k_2}\cdots p_{i_t}^{k_t},\ m=p_{i_1}^{k_1'}p_{i_2}^{k_2'}\cdots p_{i_t}^{k_t'}$$

取$k_j''=\min\{k_j,k_j'\}$, $k_j'''=\max\{k_j,k_j'\}$, j=1,2,…,t; 则(m,n)=$p_{i_1}^{k_1''}p_{i_2}^{k_2''}\cdots p_{i_t}^{k_t''}$, [m,n]=$p_{i_1}^{k_1'''}p_{i_2}^{k_2'''}\cdots p_{i_t}^{k_t'''}$.

2. 由递推公$S_i=q_iS_{i-1}+S_{i-2}$,$T_i=q_iT_{i-1}+T_{i-2}$(i≥2)及其初始值条件$S_0=0$, $S_1=1$; $T_0=1$, $T_1=q_1$得$(S_i-S_{i-2})/S_{i-1}=q_i=(T_i-T_{i-2})/T_{i-1}$, 因而有 $S_iT_{i-1}-S_{i-1}T_i=-(S_{i-1}T_{i-2}-S_{i-2}T_{i-1})=\cdots=(-1)^{i-1}(S_1T_0-S_0T_1)=(-1)^{i-1}$. 即$1=(-1)^{i-1}T_{i-1}S_i+(-1)^iS_{i-1}T_i$. 此说$S_i$与$T_i$互素。

3. 设 a,b,n 为正整数, 则从设 $a=p_{i_1}^{k_1} p_{i_2}^{k_2} \cdots p_{i_t}^{k_t}$, $b=p_{i_1}^{k'_1} p_{i_2}^{k'_2} \cdots p_{i_t}^{k'_t}$ 以及 $a^n=(p_{i_1}^{k_1} p_{i_2}^{k_2} \cdots p_{i_t}^{k_t})^n$, $b^n=(p_{i_1}^{k'_1} p_{i_2}^{k'_2} \cdots p_{i_t}^{k'_t})^n$ 和$(a,b)=p_{i_1}^{k''_1} p_{i_2}^{k''_2} \cdots p_{i_t}^{k''_t}$, $k''_j=\min\{k_j, k'_j\}$, j=1,2,…,t 知$(a^n,b^n)=((p_{i_1}^{k_1} p_{i_2}^{k_2} \cdots p_{i_t}^{k_t})^n, (p_{i_1}^{k'_1} p_{i_2}^{k'_2} \cdots p_{i_t}^{k'_t})^n)=(p_{i_1}^{k''_1} p_{i_2}^{k''_2} \cdots p_{i_t}^{k''_t})^n=(a,b)^n$, 式中 $nk''_j=\min\{nk_j, nk'_j\}$, j=1,2,…,t; 而从 $(na,nb)=(np_{i_1}^{k_1} p_{i_2}^{k_2} \cdots p_{i_t}^{k_t}, np_{i_1}^{k'_1} p_{i_2}^{k'_2} \cdots p_{i_t}^{k'_t})=n p_{i_1}^{k''_1} p_{i_2}^{k''_2} \cdots p_{i_t}^{k''_t}$ 知$(na,nb)=n(a,b)$.

4. 设 a,b,c 是整数, m 是正整数, 若(c,m)=1, 则 ac≡bc (mod m)蕴涵 a≡b(mod m). 事实上, 由 ac≡bc(mod m)得 m|(ac-bc)即 m|(a-b)c, 而(c,m)=1, 所以 m|(a-b), 此说 a≡b(mod m). ac≡bc (mod m)未必蕴涵 a≡b(mod m)的例: 15×3≡8×3(mod 7) 蕴涵 15≡8(mod 7); 15×7≡17×7(mod 7)不蕴涵 15≡17(mod 7).

4. 对 L,S,S,X 的表示数字 11,18,18 和 23, 都加 16, 然后模 26 取余并得 1,8,8 与 13. 它们表示字母 B,I,I,N, 所以“LSSX”的传输结果是“BIIN”.

4-3 同余式

定义 4.3.1 设 a,b 为整数, m 为正整数, 若 a 与 0 关于模 m 不同余, 则称 ax+b≡0(mod m)为模 m 的一次同余式。

定理 4.3.1 设 c 是满足 ax+b≡0(mod m)的一个整数, 即成立 ac+b≡0(mod m), 则满足 x≡c(mod m)的一切整数 x 都满足 ax+b≡0(mod m). 换言之, 若 c 满足 ax+b≡0(mod m), 则 c 模 m 的同余类(满足 x≡c(mod m)的一切整数 x)满足 ax+b≡0(mod m).

证明: 由 x≡c(mod m)及定理 4.2.2 得 x=c+km, 于是 ax+b≡a(c+km)+b≡ac+b(mod m). 但 ac+b≡0(mod m), 所以 ax+b≡0(mod m).

定义 4.3.2 若 c 满足 ax+b≡0(mod m), 则称 c 模 m 的同余类为一次同余式 ax+b≡0(mod m)的解。

例 4.3.1 求 3x+5≡0(mod 7)的解。

解: 取 c=3, 则 3×3+5≡0(mod 7), 因而 3 模 7 的同余类(即满足 x≡3(mod 7)的一切整数 x){…,-18,-11,-4.3.10,17,…}为一次同余式 3x+5≡0(mod 7)的解。显然{…,-18,-11,-4.3.10,17,…}可由 3+ km(=7), k=0,±1,±2,…, 所生成。

定理 4.3.2 设(a,m)=d＞1 且 b 不是 d 的整倍数, 则一次同余式 ax+b≡0(mod m)无解。

证明: 其实, 若存在整数 c, 满足 ac+b≡0(mod m), 则由定理 4.2.2 得 ac=b+km 即 b=ac-km, 从(a,m)=d 得 d|a 且 d|m, 因而 d|b, 这与 b 不是 d 的整倍数矛盾。 所以一次同余式 ax+b≡0(mod m)无解。

例 4.3.2 求 2x+179≡0(mod 562)的解。

解: 由(2,562)=2 及 179 不是 2 的整倍数知, 一次同余式 2x+179≡0(mod 562)无解。

定理 4.3.3 若(a,m)=1,则一次同余式 ax+b≡0(mod m)有解。

证明: 因为(a,m)=1, 所以存在整数 s,t, 成立 sa+tm=1, 于是有 sab+tmb=b, 即 asb=b+(-tb)m, 这也就是说 a(sb)≡b(mod m), 即一次同余式 ax+b≡0(mod m)有解 sb 模 m 的同余类。

例 4.3.2 求 256x+179≡0(mod 337)的解。

解: 因为(256,337)=1, 所以一次同余式 256x+179≡0(mod 337)有解, 其解形为“179s模 337 的同余类”。由辗转相除法求 337 和 256 的最大公约数 1(此时 1=337s+256t, 256x+179≡0(mod 337)的解为“179t模 337 的同余类”), 逐次得不完全商及余数并计算S_i和T_i列表如下:

i	0	1	2	3	4	5
r_i		81	13	3	1	0
q_i		1	3	6	4	3
S_i	0	1	3	19	79	
T_i	1	1	4	25	104	

从表中得$t=(-1)^4T_4=104$, 因而知 256x+179≡0(mod 337)的解为

104×179=18616 模 337 的同余类, 即 81 模 337 的同余类(因为 18616≡81(mod 337)){…,-593,-256,81,418,755,…}. 这里{…,-593,-256,81,418,755,…}={81+337k| k=0,±1,±2,…}.

定理 4.3.4 设 d≠0 且 ad≡bd(mod md), 则 a≡b(mod m).

证明: 由 ad≡bd(mod md)及定理 4.2.2 知, 存在整数 k 使有 ad=bd+kmd, 但 d≠0, 所以 a=b+km, 因而 a≡b(mod m).

定理 4.3.5 设 ac≡bc(mod m)且(c,m)=d, 则 a≡b(mod m/d).

证明: 由 ac≡bc(mod m)知, m|(ac-bc)即 m|(a-b)c, 但(c,m)=d, 所以(m/d)|[(a-b)c/d], 鉴于(m/d,c/d)=1, 故有(m/d)|(a-b), 此即 a≡b(mod m).

定理 4.3.6 设(a,m)=d＞1 且 d|b, 则一次同余式 ax≡b(mod m)有 d 组解, 它们是: [x], [x+m/d], [x+2m/d], …, [x+(d-1)m/d], 式中[x]为一次同余式(a/d)x≡b/d(mod m/d)的解(0≤x＜m/d), [x+im/d], i=1,2,…,(d-1), 意指给(a/d)x≡b/d(mod m/d)的解 a/d 模 m/d 的同余类[x]中的每个整数元素加上整数 im/d.

证明: 首先证明(a/d)x≡b/d(mod m/d) 与 ax≡b(mod m)同解。由定理 4.3.5 和定理 4.3.4 知, 一次同余式 ax≡b(mod m)和一次同余式(a/d)x≡b/d(mod m/d)同解。注意到(a,m)=d＞1, 我们有(a/d,m/d)=1, 由定理 4.3.3 知, (a/d)x≡b/d(mod m/d)有解, 即 a/d 模 m/d 的同余类[x]. 若取 0≤x＜m/d, 则[x]={x+km/d| k=0,±1,±2,…}. 当然[x]={x+km/d| k=0,±1,±2,…}还是 ax≡b(mod m)的解。

鉴于[x], [x+m/d], [x+2m/d], …, [x+(d-1)m/d]都在[x]之中,而 0≤x+im/d＜m, i=1,2,…,(d-1), 且它们关于模 m 互不同余, 所以[x], [x+m/d], [x+2m/d], …, [x+(d-1)m/d]是 ax≡b(mod m)的 d 个不同的解。

下证 ax≡b(mod m)只有 [x], [x+m/d], [x+2m/d], …, [x+(d-1)m/d]这 d 个不同的解。从以上讨论知, 可设 x+tm/d 为 ax≡b(mod m)的一个解, 由于 t≡i(mod d), i∈{0,1,2,…,d-1}, 据定

理 4.3.4, 在 t≡i(mod d)两边同乘 m/d 便有 tm/d≡im/d(mod m), 这就是说, [x+tm/d]为[x], [x+m/d], [x+2m/d], …, [x+(d-1)m/d]中之一。

以上讨论了一次同余式 ax≡b(mod m)的解法, 下面介绍更为重要的同余式组:

$$x\equiv b_1 \pmod{m_1},$$
$$x\equiv b_2 \pmod{m_2},$$
$$\cdots\cdots$$
$$x\equiv b_k \pmod{m_k}.$$

的解。

在我国古代的《孙子算经》里已经提出了此类形式的问题: “今有物不知其数, 三三数之剩二, 五五数之剩三, 七七数之剩二, 问物几何?” “答曰二十三。”该问题即同余式组:

$$x\equiv 2 \pmod 3,$$
$$x\equiv 3 \pmod 5,$$
$$x\equiv 2 \pmod 7.$$

如何求解呢? 我们注意到问题中的模数 3,5,7 互素。明朝程大位的《算法统宗》里有首求解歌: “三人同行七十稀, 五树梅花廿一枝, 七子团圆整半月, 除百零五便得知。”其涵义是: 同余式组

$$x\equiv b_1 \pmod 3,$$
$$x\equiv b_2 \pmod 5,$$
$$x\equiv b_3 \pmod 7.$$

有解: $x=70b_1+21b_2+15b_3 \pmod{105}$(模数 3,5,7 互素,105=3×5×7). 此类问题的一般化求解, 由南宋秦九韶整理推广而得到。

定理 4.3.7 (秦九韶定理) 若k≥2, 正整数$m_1, m_2,\ldots, m_k$两两互素, $b_1, b_2,\ldots, b_k$是k个整数, 则同余式组

$$x\equiv b_1 \pmod{m_1},$$
$$x\equiv b_2 \pmod{m_2},$$

……

$x \equiv b_k \pmod{m_k}$

有解 $x=b_1 M_1' M_1+b_2 M_2' M_2+\ldots+ b_k M_k' M_k \pmod{M}$, 式中 $M=m_1m_2\ldots m_k=m_1M_1=m_2M_2=\ldots=m_kM_k$, 对 i=1,2,…,k, M_i' 满足一次同余式 $M_i' M_i \equiv 1 \pmod{m_i}$.

证明: 因为正整数$m_1, m_2,\ldots, m_k$两两互素, 所以当i≠j时有$(m_i, m_j)=1$, 且由于$M_i = M/ m_i$, 故成立$(m_i, M_i)=1$, i=1,2,…,k. 于是由定理 4.1.2 知, 存在整数 M_i' 和 m_i', 使得 $M_i' M_i+ m_i' m_i=1$, 即存在整数 M_i' 满足 $M_i' M_i \equiv 1 \pmod{m_i}$(*), i=1,2,…,k . 另一方面, 当i≠j时由$(m_i, m_j)=1$ 和$M_i = M/ m_i$得$m_i|M_j$, 因此有 $b_j M_j' M_j \equiv 0 \pmod{m_i}$(**), i,j=1,2,…,k . 而由(*)与(**)式得 $b_1 M_1' M_1+b_2 M_2' M_2+\ldots+ b_k M_k' M_k \equiv b_i M_i' M_i \equiv b_i \pmod{m_i}$, i=1,2,…,k. 此说 $x=b_1 M_1' M_1+b_2 M_2' M_2+\ldots+ b_k M_k' M_k \pmod{M}$是同余式组的解。

例 4.3.3 证明同余式组

$x \equiv b_1 \pmod 3$,

$x \equiv b_2 \pmod 5$,

$x \equiv b_3 \pmod 7$.

的解是$x=70b_1+21b_2+15b_3 \pmod{105}$.