第 1 章 整除

整除是数论中的基本概念．本章主要介绍与整除相关的一些基本概念及其性质．这些基本概念如整除、因子、公因子、最小公倍数、分解因子等早在高中被大家所熟悉．在这里我们将给出这些概念的严格的数学定义．通过对这些概念的数学定义及其性质的掌握，可以解决许多初等数论里与整除相关的问题．本章构成整除理论较为丰富的内容，解决问题的方法较为灵活，技巧较多．它不仅是数论的基础，而且在密码学中有很广泛的应用，如整数的素分解、欧几里德算法求最大公因子等问题在密码学中都有极其重要的应用．

§1 整除的概念

我们用集合 Z 表示全体整数组成的集合， N 表示自然数的全体． 下面给出整除的定义．

定义 1 设 $a,b\in Z$, $a\neq 0$ ，如果存在 $q\in Z$ 使得 $b=aq$ ，那么，就说 b 可被 a 整除，记作 $a\mid b$ ，称 b 是 a 的倍数， a 是 b 的因子（也可称为约数、除数）．否则就说 b 不能被 a 整除，或 a 不整除 b .

关于整除，有以下性质：

1) $a\mid b$ 且 $b\mid c\Rightarrow a\mid c$ ；

2) $a\mid b$ 且 $a\mid c\Leftrightarrow$ 对任意的 $x,y\in Z$ 有 $a\mid bx+cy$ ；

3) 设 $m\neq 0$ ，那么， $a\mid b\Leftrightarrow ma\mid mb$ ；

3) $a\mid b$ 且 $b\mid a\Rightarrow b=\pm a$ ；

4) 设 $b\neq 0$ ，那么， $a\mid b\Rightarrow |a|\leq |b|$.

证明 ⑴ 由于 $a\mid b$ ，根据整除的定义知存在 x ，使 $b=xa$ ，同样，存在 y 使得 $c=yb$ ，从而，

$$c=yb=yxa=(yx)a,$$

即 $a\mid c$.

⑵ 由（ 1 ）的证明知，存在 r,s 使得 $b=ar$ ， $c=as$ ，故对任意的 x,y ，

$$bx+cy=arx+asy=a(rx+sy),$$

所以 $a\mid bx+cy$.

⑶，⑷，（5）证明类似，读者可以自己补出证明．

显然，± 1、$\pm b$ 是 b 的因子，我们称其为 b 的显然因子； b 的其它因子称为 b 的非显然因子，或真因子. 由此我们可引出既约元的定义．

定义 2 设整数 $p\neq 0$ ，± 1. 如果它除了显然因子 ± 1、$\pm p$ 外没有其它的因子，那么 p 就称为**既约元**（常称为素数、不可约数）， 若 $a\neq\pm 1$ ，且除显然因子外还含有真因子，则称 a 为**合数**.

注 一般情况下，素数我们只取正的．

定理 1 若 a 为合数，则 a 的最小真因子为素数．

证明 由 a 为合数知，$a>2$．设 d 为 a 的最小真因子，下证 d 为素数．如果 d 不为素数，则存在 d 的真因子 d'，使 $d'\mid d$，由性质 1）知，$d'\mid a$，与 d 为最小真因子矛盾．定理得证．

定理 2 素数有无穷多个．

证明 用反证法．假设只有有限个素数，设为 $q_1,q_2,\cdots q_k$，考虑 $a=q_1q_2\cdots q_k+1$，由定理 1 知，整除 a 的最小真因子一定为素数，记为 p．由于 p 为素数，因而 p 必等于某个 q_i，所以 $p\mid a, p\mid q_1q_2\cdots q_k$，从而 $q_i\mid 1$，这与 p 是素数矛盾．因此定理得证．

将素数从小到大排列，假设 p_n 表示第 n 个素数，$\pi(x)$ 表示不超过 $x\,(x>0)$ 的素数个数．虽然我们无法知道 p_n 的确切位置，但是，我们可以得到 p_n 的弱上界估计．而对于 $\pi(x)$ 的估计，利用初等数论的内容可以推出它的主项估计--素数定理，关于素数定理，第 5 章给出一个初等证明．下面定理仅描述了 p_n 的一个非常弱的上界估计与 $\pi(x)$ 的一个弱下界估计．

定理 3 将全体素数按从小到大的顺序排列，则第 n 个素数 p_n 与 $\pi(x)$ 分别有以下结论．

（1） $p_n\le 2^{2^{n-1}}$，$n=1,2,...$；

（2）$\pi(x)>\log_2\log_2 x,\quad x\ge 2$．

证明 (1) 我们用归纳法来证明该等式成立．当 $n=1$ 时，（1）显然成立．假设对于 $n\le k$ 时（1）成立．当 $n=k+1$ 时，由定理 1 知

$$p_{k+1}\le p_1p_2\cdots p_k+1,\quad n>1,$$

所以

$$p_{k+1}\le 2^{2^0}2^{2^1}\cdots 2^{2^{k-1}}+1=2^{2^k-1}+1<2^{2^k}.$$

于是（1）得证．

（2）的证明：$\forall x\ge 2$，必存在唯一的整数 n，使得 $2^{2^{n-1}}\le x<2^{2^n}$，，从而由（1）式得

$$\pi(x)\ge\pi\left(2^{2^{n-1}}\right)\ge n>\log_2\log_2 x.$$

初等数论还有一个最基本的结论：带余除法定理，它是整除的一般情形．

定理 4 设 a,b 是两个给定的整数，$a\ne 0$．那么，一定存在唯一的一对整数 q 与 r，满足

$$b=qa+r,\quad 0\le r<a,$$

其中 r 称为 b 被 a 除后的**最小非负余数**．此外 $a\mid b$ 的充要条件是 $r=0$．

证明 唯一性： 若还有整数 q' 与 r' 满足

$$b=q'a+r',\quad 0\le r'<|a|,$$

不妨设 $r'\ge r$，则有

$$0\le r'-r<|a|,\quad r'-r=(q'-q)a,$$

因此 $r'-r=0$．所以唯一性成立．

存在性： 当 $a\mid b$ 时，可取 $q=\dfrac{b}{a},\quad r=0$．当 $a\nmid b$ 时，考虑集合

$$T=\{b-ka,k=0,\pm1,\pm2,\cdots\},$$

容易看出集合T中必有正整数（例如，取$k=\dfrac{-2|b|}{a}$），故T中必有一个最小正整数，记为

$$t_0=b-k_0a>0.$$

我们来证明必有$t_0<|a|$．因为$a\nmid b$，所以$t_0\neq|a|$．若$t_0>|a|$，则$t_1=t_0-|a|>0$．显见$t_1\in T$，$t_1<t_0$，这和t_0的最小性矛盾．取$q=k_0,r=t_0$就满足要求．显然，$a\mid b$的充要条件是$r=0$．定理得证．

设$a\geq 2$是给定的正整数，$j=0,1,\cdots,a-1$．对给定的j，被a除后余数等于j的全体整数是

$$ka+j,k=0,\pm1,\pm2,\cdots.$$

这些整数组成的集合记为$S_{a,j}$．集合$\{S_{a,j},0\leq j\leq a-1\}$满足以下两个性质：

（1）$\{S_{a,j},0\leq j\leq a-1\}$中的任两个元素两两不相交，即

$$S_{a,j}\cap S_{a,j}=\phi,\quad 0\leq j\neq j'\leq a-1;$$

（2）$\{S_{a,j},0\leq j\leq a-1\}$中所有子集的并等于$Z$，即

$$\bigcup_{0\leq j\leq a-1}S_{a,j}=Z.$$

所以全体整数按被a除后所得的最小非负余数来分类，分成了两两不相交的a个类．

例 1 x^3被9除后所得的最小非负剩余是0，1，8.

证明 由上面的讨论知，只需检验0至8之间的数即可，

$$0^3=0\times9+0;\ 1^3=0\times9+1;\ 2^3=0\times9+8;$$
$$3^3=3\times9+0;\ 4^3=7\times9+1;\ 5^3=13\times9+8;$$
$$6^3=24\times9+0;\ 7^3=38\times9+1;\ 8^3=56\times9+8.$$

得证．

例 2 设$a\geq 2$是给定的正整数．那么任一正整数n必可唯一表示为

$$n=r_ka^k+r_{k-1}a^{k-1}+\cdots+r_1a+r_0,$$

其中整数$k\geq0,0\leq r_j\leq a-1(0\leq j\leq k),r_k\neq0$．这就是正整数的$a$**进位表示.**

证明 对正整数n必有唯一的$k\geq0$，使$a^k\leq n<a^{k+1}$．由带余除法知，必有唯一的q_0,r_0满足

$$n=q_0a+r_0,\quad 0\leq r_0<a.$$

若$k=0$，则必有$q_0=0,1\leq r_0<a$，所以结论成立．

若$k=m\geq0$时结论成立．那么，当$k=m+1$时，上式中的q_0必满足

$$a^m\leq q_0<a^{m+1}.$$

由假设知

$$q_0=s_ma^m+\cdots+s_0,$$

其中$0\leq s_j\leq a-1(0\leq j\leq a-1)$，$1\leq s_m\leq a-1$．因而有

$$n=s_ma^{m+1}+\cdots+s_0a+r_0,$$

即结论对$m+1$也成立．得证．

例 3 设$a>2$是奇数．证明：

（1）一定存在正整数 $d \le a-1$，使得 $a \mid 2^d-1$；

（2）设 d_0 是满足（1）的最小正整数．那么 $a \mid 2^h-1(h \in N)$ 的充要条件是 $d_0 \mid h$．

证明（i）考虑以下 a 个数，

$$2^0, 2^1, 2^2, \cdots, 2^{a-1}.$$

由 $a \nmid 2^j (0 \le j < a)$ 及带余除法知，对每个 $j, 0 \le j < a$，

$$2^j = q_j a + r_j, 0 < r_j < a.$$

所以 a 个余数 $r_0, r_1, \cdots, r_{a-1}$ 仅可能取 $a-1$ 个值．因此其中必有两个相等，不妨设 $0 \le i < k < a$ 且 $r_i = r_k$，因而有

$$a(q_k - q_i) = 2^k - 2^i = 2^i(2^{k-i}-1).$$

由 $(a, 2)=1$，推出 $a \mid 2^{k-i}-1$．取 $d = k-i \le a-1$ 就满足要求．

（2）充分性是显然的，只要证必要性．同样由带余除法定理得

$$h = qd_0 + r, \quad 0 \le r < d_0.$$

因而有

$$2^h - 1 = 2^{qd_0+r} - 2^r + 2^r - 1 = 2^r(2^{qd_0}-1) + (2^r-1).$$

由 $a \mid 2^h-1$ 及 $a \mid 2^{qd_0}-1$，易知 $a \mid 2^r-1$．由此及 d_0 的最小性可以推出 $r=0$，即 $d_0 \mid h$．

§2 最大公因子与最小公倍数

最大公因子与最小公倍数是整除理论中两个最基本的概念．本节主要讨论最大公因子与最小公倍数的概念及其性质．

定义 1 设 a_1, a_2 是两个整数．如果 $d \mid a_1$ 且 $d \mid a_2$，那么 d 就称为是 a_1 和 a_2 的**公因子**．一般地，设 $a_1, a_2, \cdots, a_k$ 是 k 个整数．如果 $d \mid a_1, \cdots, d \mid a_k$，那么 d 就称为是 $a_1, \cdots a_k$ 的**公因子**．

定义 2 设 a_1, a_2 是两个不全为零的整数，d 是 a_1 和 a_2 的一个公因子，如果对任意的 $d' \mid a_1, d' \mid a_2$，有 $d' \mid d$，称 d 为 a_1 和 a_2 的**最大公因子**，记作 $d = (a_1, a_2)$ 或 $d = g \cdot c \cdot d(a_1, a_2)$．

一般地，设 $a_1, \cdots, a_k$ 是 k 个不全为零的整数．d 是 $a_1, \cdots, a_k$ 的一个公因子，如果对任意的 $a_1, ..., a_k$ 的公因子 d'，有 $d' \mid d$，称 d 为 $a_1, \cdots, a_k$ 的**最大公因子**，记作 $d = (a_1, ..., a_k)$ 或 $d = g \cdot c \cdot d(a_1, ..., a_k)$．

从定义 2　知，最大公因子即是公因子中最大的一个，定义 2 提供了一种证明最大公因子的方法．

性质 1 对任意整数 x，$(a_1, a_2) = (a_1, a_2 + a_1 x)$．

性质 2 设 $m > 0$，则

$$m(b_1, \cdots, b_k) = (mb_1, \cdots, mb_k).$$

性质 3 $\left(\dfrac{a_1}{(a_1, a_2)}, \dfrac{a_2}{(a_1, a_2)} \right) = 1$，更一般地，有

$$\left(\frac{a_1}{(a_1,\cdots,a_k)},\cdots,\frac{a_k}{(a_1,\cdots,a_k)}\right)=1.$$

其中性质 1 提供了一种求解最大公因子的很简单、实用的方法.

例1 对任意的整数 n 有

$$(21n+4,14n+3)=(7n+1,14n+3)=(7n+1,1)=1;$$

$$(2n-1,n-2)=(3,n-2)=\begin{cases}3, & n=3k+2,\\ 1, & n=3k\text{或}3k+1.\end{cases}$$

例 2 设 a 是奇数. 证明：必有正整数 d 使 $(2^d-3,a)=1$.

证明 由 §1 节例 3 知，必有 d 使 $a\mid 2^d-1$，再性质 1 可以推出：

$$(2^d-3,a)=(2^d-1-2,a)=(-2,a)=1.$$

例3 证明： $\left(\frac{a}{(a,c)},\frac{b}{(b,a)},\frac{c}{(c,b)}\right)=1$.

证明 显然有

$$\frac{a}{(a,c)}\Big|\frac{a}{(a,b,c)},\quad \frac{b}{(a,b)}\Big|\frac{b}{(a,b,c)},\quad \frac{c}{(b,c)}\Big|\frac{c}{(a,b,c)}.$$

于是

$$\left(\frac{a}{(a,c)},\frac{b}{(b,a)},\frac{c}{(c,b)}\right)\Big|\left(\frac{a}{(a,b,c)},\frac{b}{(a,b,c)},\frac{c}{(a,b,c,)}\right)=1.$$

故

$$\left(\frac{a}{(a,c)},\frac{b}{(b,a)},\frac{c}{(c,b)}\right)=1.$$

定义 3 a_1,a_2 是两个整数，若 $(a_1,a_2)=1$，则称 a_1 和 a_2 是**既约的**，（或者是**互素的**）. 若 $(a_1,\cdots,a_k)=1$，则称 $a_1,\cdots,a_k$ 是**既约的**，也称 $a_1,\cdots,a_k$ 是**互素的.**

定义 4 设 a_1,a_2 是两个均不等于零的整数. 如果

$$a_1\mid l,\quad a_2\mid l,$$

则称 l 是 a_1 和 a_2 的**公倍数.**

一般地，设 $a_1,a_2,\cdots,a_k$ 是 k 个均不等于零的整数. 如果

$$a_1\mid l,\cdots,a_k\mid l,$$

则称 l 是 $a_1,\cdots,a_k$ 的**公倍数.**

定义 5 设 a_1,a_2 是两个全不为零的整数，l 是 a_1 和 a_2 的一个公倍数，对 a_1,a_2 的任意公倍数 l'，有 $l\mid l'$，称 l 为 a_1 和 a_2 的**最小公倍数，**记作 $[a_1,a_2]$.

一般地，l 是 $a_1,\cdots,a_k$ 的一个公倍数，对 $a_1,\cdots,a_k$ 的任意公倍数 l'，有 $l\mid l'$，称 l 为 $a_1,\cdots,a_k$ 的**最小公倍数，**记作 $[a_1,\cdots,a_k]$.

关于最小公倍数，我们有以下结论.

性质 4 若 $a_2\mid a_1$，则 $[a_1,a_2]=\mid a_1\mid$；若 $a_j\mid a_1$，$2\le j\le k$，则 $[a_1,a_2,\cdots,a_k]=\mid a_1\mid$.

性质 5　对任意的 $d \mid a_1$，我们有

$$[a_1, a_2] = [a_1, a_2, d]，\ [a_1, a_2, \cdots, a_k] = [a_1, a_2, \cdots, a_k, d].$$

性质 6　设 $m > 0$，我们有

$$[ma_1, ma_2, \cdots, ma_k] = m[a_1, a_2, \cdots, a_k].$$

证明　设 $L = [ma_1, ma_2, \cdots, ma_k]$，$L' = [a_1, a_2, \cdots, a_k]$．由 $ma_j \mid L$，$1 \le j \le k$ 推出 $a_j \mid L/m$，$1 \le j \le k$，进而，由最小公倍数定义知 $L' \le L/m$．另一方面，由 $a_j \mid L'$，$1 \le j \le k$ 推出 $ma_j \mid mL$，$1 \le j \le k$，由最小公倍数定义知 $mL' \ge L$．从以上两方面定理得证．

关于最大公因子与最小公倍数，进一步有下列结论．

定理 1　（1）$(a_1, a_2, a_3, \cdots, a_k) = ((a_1, a_2), a_3, \cdots, a_k)$；

（2）$(a_1, \cdots, a_{k+r}) = ((a_1, \cdots, a_k), (a_{k+1}, \cdots, a_{k+r}))$．

证明　（i）设

$$d = (a_1, a_2, a_3, \cdots, a_k)，\ d' = ((a_1, a_2), a_3, \cdots, a_k)，$$

下证 $d = d'$．由

$$d \mid a_j (1 \le j \le k)，$$

则

$$d \mid (a_1, a_2), d \mid a_j (3 \le j \le k)，$$

从而 $d \mid d'$．反过来，由

$$d' \mid (a_1, a_2)，\ d' \mid a_j (3 \le j \le k)，$$

可以推出 $d' \mid a_j (1 \le j \le k)$，所以 $d' \mid d$．（i）得证．

由（i）即推出（ii），详细证明留给读者．

定理 2　设 $(m, a) = 1$，则 $(m, ab) = (m, b)$．

证明　当 $m = 0$ 时，$a = \pm 1$，结论显然成立．当 $m \ne 0$ 时，由性质 2 与定理 1 得

$$(m, b) = (m, b(m, a)) = (m, (mb, ab)) = (m, mb, ab) = (m, ab).$$

定理得证．

定理 3　设 $(m, a) = 1$．若 $m \mid ab$，则 $m \mid b$．

证明　由定理 2 得

$$|m| = (m, ab) = (m, b)，$$

这就推出 $m \mid b$．

定理 4　$[a_1, a_2](a_1, a_2) = |a_1 a_2|$．

证明　当 $(a_1, a_2) = 1$ 时．设 $l = [a_1, a_2]$，则 $l \mid a_1 a_2$．另一方面，由 $a_1 \mid l$ 知 $l = a_1 l'$．进而由 $a_2 \mid l = a_1 l'$，$(a_2, a_1) = 1$ 及定理 3 知 $a_2 \mid l'$，所以 $|a_1 a_2| \mid l$．结论得证．

当 $(a_1, a_2) \ne 1$ 时，由性质 3 知 $((a_1/(a_1, a_2), a_2/(a_1, a_2)) = 1$，从而有

$$\left[\frac{a_1}{(a_1, a_2)}, \frac{a_2}{(a_1, a_2)}\right] = \frac{|a_1 a_2|}{(a_1, a_2)^2}.$$

由性质 2 $(k = 2, m = (a_1, a_2))$ 即得结论．

例 4　设 k 是正整数，证明：

（1） $(a^k, b^k) = (a, b)^k$，

（2） 设 a, b 是整数，若 $(a, b) = 1$， $ab = c^k$．则 $a = (a, c)^k$， $b = (b, c)^k$．

证明 由性质 2，

$$(a^k, b^k) = (a, b)^k ((\frac{a}{(a,b)})^k, (\frac{b}{(a,b)})^k).$$

而

$$((\frac{a}{(a,b)}), (\frac{b}{(a,b)})) = 1,$$

故由定理 2 知，

$$((\frac{a}{(a,b)})^k, (\frac{b}{(a,b)})^k) = 1.$$

这就证明了（i）式.

由 $(a,b) = 1$ 推出 $(a^{k-1}, b) = 1$，从而

$$a = a(a^{k-1}, b) = (a^k, ab) = (a^k, c^k) = (a, c)^k.$$

同样的得到 $b = (b, c)^k$．例 4 得证.

例 5 证明：$\sqrt{7}$ 不是有理数.

证明 设 $\frac{a}{b} = \sqrt{7}$，$(a,b) = 1$，则 $a^2 / b^2 = 7$，所以 $7b^2 = a^2$，即 $7 \mid a$．$7^2 \mid a^2$ 于是 $7 \mid b$．这与 $(a,b) = 1$ 矛盾．定理得证.

§3 欧几里德算法

辗转相除法也叫 **Euclid 算法**，它在初等数论中有重要的地位．利用 Euclid 算法不仅可以求出有限个整数之间的最大公因子，而且可以求出最大公因子用这些整数表示的线性系数．Euclid 算法有许多重要得应用如可以直接用于求解一次不定方程，也可以用于元素的指数、指标的有关证明，有限群中群的阶、元素阶、子群阶等之间的关系的推导等．欧几里德算法在密码学中也有多种应用，并可用于破译或分析某些密码算法的安全性.

定理 1（**Euclid 算法**） 设 a,b 是给定的两个整数，$b \neq 0$，b 不能整除 a，重复应用带余除法得到的下面 k 个等式：

$$\begin{aligned}
a &= q_0 b + r_0, & 0 < r_0 < |b|,\\
b &= q_1 r_0 + r_1, & 0 < r_1 < r_0,\\
r_0 &= q_2 r_1 + r_2, & 0 < r_2 < r_1,\\
&\cdots\cdots\cdots\cdots & \cdots\cdots\cdots\cdots\\
r_{k-5} &= q_{k-3} r_{k-4} + r_{k-3}, & 0 < r_{k-3} < r_{k-4},\\
r_{k-4} &= q_{k-2} r_{k-3} + r_{k-2}, & 0 < r_{k-2} < r_{k-3},\\
r_{k-3} &= q_{k-1} r_{k-2}.
\end{aligned}$$

证明 对 a,b 应用带余除法，因为 b 不能整除 a 知，第一式成立．同样如果 r_0 不能整除 b，第二式成立．依次下去，就得到

$$|b| > r_0 > r_1 > \cdots > r_{j-1} > 0$$

及前面 $j-2$ 个等式成立．若 $r_{j-1} \mid r_{j-2}$，则定理对 $k = j-2$ 时成立；若 $r_{j-1} \nmid r_{j-2}$，则继续对 r_{j-2}, r_{j-1} 用带余除法．由于小于 $|b|$ 的正整数只有有限个以及1整除任一整数，所以一定会出现某个 k，要么 $1 < r_{k-2} \mid r_{k-3}$，要么 $1 = r_{k-2} \mid r_{k-3}$．定理得证．

定理 1 所描述的是余数取最小非负剩余的 Euclid 算法．本书的最后一章将给出余数取最小绝对剩余的 Euclid 算法，并给出整除步骤 k 的一个很好的上界估计，从而得到 Euclid 算法的多项式时间估计．

定理 2 在定理 1 的条件和符号下，我们有

(1) $r_{k-2} = (a, b)$, （2）

(2) 存在整数 x_0, x_1 使

$$(a,b) = x_0 a + x_1 b\,. \tag{3}$$

证明 （1）从定理 1 的最后一式开始，依次往上推，可得

$$r_{k-2} = (r_{k-2}, r_{k-3}) = \ldots\ldots = (r_1, r_0) = (r_0, b) = (a, b)$$

结论（1）成立．

（2）由 Euclid 算法中的第 k 式 (a,b) 可表成 r_{k-3} 和 r_{k-4} 的整系数线性组合，利用第 $k-1$ 式可消去通过消除 r_{k-3}，得到 (a,b) 的关于 r_{k-4} 和 r_{k-5} 的整系数线性组合．这样依次利用第 $k-2, k-3, \cdots, 2, 1$ 式，就得到 (a,b) 表为 a 和 b 的整系数线性组合．结论（2）成立．

定理 2 不但给出了求两个数的最大公约数的一个十分方便的具体算法，而且同时给出了求 x_1, x_0 的具体算法．

推论 设 $a_1, \cdots, a_k$ 是不全为零的整数，一定存在一组整数 $x_{1,0}, \cdots, x_{k,0}$，使得

$$(a_1, \cdots, a_k) = a_1 x_{1,0} + \cdots + a_k x_{k,0}\,.$$

证明留给读者．

例 1 求 42823 及 6409 的最大公因子，并将它表示成 42823 和 6409 的整系数线性组合形式．

解
$$42823 = 6 \cdot 6409 + 4369\,, \quad 6409 = 1 \cdot 4369 + 2040$$
$$4369 = 2 \cdot 2040 + 289\,, \quad 2040 = 7 \cdot 289 + 17$$
$$289 = 17 \cdot 17$$

即

$$(42823, 6409) = (6409, 4369) = (4369, 2040) = (2040, 289) = (289, 17) = 17.$$

下面是上面过程的逆过程，

$$17 = 2040 - 7 \cdot 289\,,$$
$$17 = 2040 - 7 \cdot (4369 - 2 \cdot 2040)$$
$$= -7 \cdot 4369 + 3 \cdot 2040\,,$$
$$17 = -7 \cdot 4369 + 3 \cdot (6409 - 4369)$$
$$= 3 \cdot 6409 - 10 \cdot 4369\,,$$
$$17 = 3 \cdot 6409 - 10 \cdot (42823 - 6 \cdot 6409)$$
$$= -10 \cdot 42823 + 63 \cdot 6409\,.$$

这就求出了线性组合形式：

$$(42823, 6409) = -10 \cdot 42823 + 63 \cdot 6409\,.$$

例 2 若 $(a,b) = 1$，则任一整数 n 必可表为 $n = ax + by$， x, y 是整数．

证明 由$(a,b)=1$及定理 2 知，存在x_0, y_0使$ax_0+by_0=1$．因而取

$$x=nx_0,\quad y=ny_0$$

即可．

例4 设m,n是正整数．证明：

$$(2^m-1, 2^n-1)=2^{(m,n)}-1.$$

证明 不妨设$m\geq n$．由带余除法得

$$m=q_1n+r_1,\quad 0\leq r_1<n.$$

我们有

$$2^m-1=2^{q_1n+r_1}-2^{r_1}+2^{r_1}-1=2^{r_1}(2^{q_1n}-1)+2^{r_1}-1.$$

由此及$2^n-1\mid 2^{q_1n}-1$得

$$(2^m-1, 2^n-1)=(2^{r_1}-1, 2^n-1).$$

注意到$(m, n)=(n, r_1)$，若$r_1=0$，则$(m,n)=n$，结论成立．若$r_1>0$，则继续对$(2^{r_1}-1, 2^n-1)$作同样的讨论，由辗转相除法知，结论成立．

显见，2 用任一大于1的自然数代替，结论都成立．

§4 求解一次不定方程--Euclid 算法应用之一

辗转相除法的应用十分广泛，在此介绍一个在解一次不定方程应用．

所谓的一次不定方程的一般形式是

$$a_1x_1+\cdots+a_kx_k=c \qquad (1)$$

其中 整数$k\geq 2, c, a_1,\cdots, a_k$是整数，且$a_1,\cdots,a_k$是方程的系数且不都等于零，$x_1,\cdots,x_k$是整数变数．

首先给出方程（1）有解的一个充要条件．

定理 1 不定方程（1）有解的充要条件是$(a_1,\cdots,a_k)\mid c$．当不定方程（1）有解时，它的解和不定方程

$$\frac{a_1}{d}x_1+\cdots+\frac{a_k}{d}x_k=\frac{c}{d} \qquad (2)$$

的解相同，这里$d=(a_1,\cdots,a_k)$．

证明 必要性显然．下证充分性．

若$d\mid c$，设$c=dc_1$．则必有整数$y_{1,0},\cdots,y_{k,0}$使得

$$a_1y_{1,0}+\cdots+a_ky_{k,0}=d.$$

因此

$$x_1=c_1y_{1,0},\cdots,x_k=c_1y_{k,0}$$

即为（1）的一组解，充分性成立．

由于（1）有解时必有$d\mid c$，而这时不定方程（1）和（2）是同一个方程，这就证明了后一个结论．

定理 2 设二元一次不定方程

$$a_1x_1+a_2x_2=c \qquad (3)$$

有解，若 $x_{1,0}, x_{2,0}$ 是它得一组解．那么它的所有解为

$$\begin{cases} x_1 = x_{1,0} + \dfrac{a_2}{(a_1, a_2)}t, \\ x_2 = x_{2,0} - \dfrac{a_1}{(a_1, a_2)}t, \end{cases} \quad t = 0, \pm 1, \pm 2, \cdots. \qquad (4)$$

证明 容易验证（4）给出的每一对 x_1, x_2 为（3）的解．反过来，设 x_1, x_2 是（3）的一组解，我们有

$$a_1x_1 + a_2x_2 = c = a_1x_{1,0} + a_2x_{2,0}.$$

从而有

$$a_1(x_1 - x_{1,0}) = -a_2(x_2 - x_{2,0}),$$

$$\frac{a_1}{(a_1, a_2)}(x_1 - x_{1,0}) = -\frac{a_2}{(a_1, a_2)}(x_2 - x_{2,0}).$$

又由于

$$(\frac{a_1}{(a_1, a_2)}, \quad \frac{a_2}{(a_1, a_2)}) = 1,$$

所以

$$x_1 - x_{1,0} = \frac{a_2 t}{(a_1, a_2)}, \quad x_2 - x_{2,0} = -\frac{a_1}{(a_1, a_2)}t.$$

这就证明了 x_1, x_2 可表为式（4）的形式．定理得证．

由上面的定理可得到求解二元一次不定方程的步骤：

（1） 验证 $(a_1, a_2) \mid c$ 是否成立．

（2） 若 $(a_1, a_2) \mid c$ 有解，则设法去求出一组特解 $x_{1,0}, x_{2,0}$．

下面具体举几个例子来说明．

例 1 解二元同余方程 $3x_1 + 5x_2 = 11$．

解 容易看出方程的一组特解为 $\begin{cases} x_1 = 2, \\ x_2 = 1. \end{cases}$，因为 $(3, 5) = 1$，所以方程的解为

$$\begin{cases} x_1 = 2 + 5t, \\ x_2 = 1 - 3t, \end{cases} \quad t = 0, \pm 1, \pm 2, \cdots.$$

例 2 解二元一次不定方程 $21x_1 + 35x_2 = 98$．

解 因为 $(21, 35) = 7 \mid 98$，所以方程有解．

$$x_1 = \frac{1}{21} \times (-35x_2 + 98) = -2x_2 + 5 + \frac{1}{21} \times (7x_2 - 7);$$

$$t = \frac{1}{21} \times (7x_2 - 7);$$

$$x_2 = \frac{1}{7} \times (21t + 7) = 3t + 1, \quad t = 0, \pm 1, \pm 2, \cdots;$$

$$x_1 = -2x_2 + 5 + \frac{1}{21}\times(7x_2 - 7) = -5t + 3,\ t = 0, \pm 1, \pm 2, \cdots.$$

§5 整数的素分解

整数与素数有着密切的关系，从理论上，任一整数均可分解为素数的乘积．而实际上大整数的素分解是一个困难问题，而一些特殊整数的素分解的困难性恰恰是一些公钥密码算法安全的理论根据．下面来介绍有关整数素分解的定理．

引理 设 p 是素数, $p \mid a_1 a_2$．那么 $p \mid a_1$ 或 $p \mid a_2$ 至少有一个成立，一般地，若 $p \mid a_1 \cdots a_k$，则 $p \mid a_1, \cdots, p \mid a_k$ 至少有一个成立．

证明留给读者．

定理 1（算术基本定理）设 $a > 1$，那么必有

$$a = p_1 p_2 \cdots p_s \tag{1}$$

其中 $p_j (1 \le j \le s)$ 是素数，且在不记次序的意义下，表示式（1）是唯一的．

证明 首先证明存在性，我们用数学归纳法来证．

当 $a = 2$ 时，2 是不可约数，所以结论成立．

假设当 $2 \le a < n$ 时，结论成立．

当 $a = n$ 时，若 n 是不可约数，则结论成立；若 n 是合数，则必有

$$n = n_1 n_2,\ 2 \le n_1,\ n_2 < n,$$

由假设知 n_1，n_2 都可表为不可约数的乘积

$$n_1 = p_{11} \cdots p_{1s},\ n_2 = p_{21} \cdots p_{2r}.$$

这样，就把 a 表为不可约数的乘积

$$a = n = n_1 n_2 = p_{11} \cdots p_{1s} p_{21} \cdots p_{2r}.$$

因此整数的素分解是存在的．

若有两种形式的素分解

$$a = p_1 p_2 \cdots p_s,\ p_1 \le p_2 \le \cdots \le p_s,$$

$$a = q_1 q_2 \cdots q_r,\ q_1 \le q_2 \le \cdots \le q_r,$$

这里 $p_i (1 \le i \le s)$，$q_i (1 \le i \le r)$ 是素数，我们来证明必有

$$r = s,\ p_j = q_j (1 \le j \le s).$$

不妨设 $r \ge s$，由

$$q_1 \mid a = p_1 p_2 \cdots p_s$$

知，必有某个 p_j 满足 $q_1 \mid p_j$．由于 q_1 和 p_j 是素数，所以 $q_1 = p_j$．

同样，由

$$p_1 \mid a = q_1 q_2 \cdots q_r$$

知，必有某个 q_i 满足 $p_1 \mid q_i$，因而 $p_1 = q_i$．由于 $q_1 \le q_i = p_1 \le p_j$，所以 $p_1 = q_1$．因此

$$q_2 q_3 \cdots q_r = p_2 p_3 \cdots p_s.$$

同样依次可得

$$q_2 = p_2, \cdots, q_s = p_s,\ q_{s+1}, \cdots, q_r = 1.$$

所以不存在$q_{s+1},\cdots,q_r$，即$r=s$． 定理得证．

推论 1 设$a>1$，那么，必有

$$a=p_1^{\alpha_1}\cdots p_s^{\alpha_s}\qquad p_1<p_2<\cdots<p_s \tag{2}$$

式（2）称为是a的**标准素因数分解式.**

证明是显然的，只要将分解式(1)中相同的素数合并即可．

推论 2 设$a=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$， $p_i(1\le i\le s)$是互不相同的素数，那么， d 是a的正因数的充要条件是

$$d=p_1^{e_1}\cdots p_s^{e_s}\text{，}\quad 0\le e_j\le\alpha_j\text{，}\ 1\le j\le s\text{．}$$

推论 3 设

$$a=p_1^{\alpha_1}\cdots p_s^{\alpha_s}\text{，}\ b=p_1^{\beta_1}\cdots p_s^{\beta_s}\text{，}\quad p_1<p_2<\cdots<p_s\text{，}$$

这里允许某个α_j和β_i为零，那么

$$(a,b)=p_1^{\delta_1}\cdots p_s^{\delta_s}\text{，}\ \delta_j=\min(\alpha_j,\beta_j)\text{，}\ 1\le j\le s\text{．}$$

$$[a,b]=p_1^{\gamma_1}\cdots p_s^{\gamma_s}\text{，}\ \gamma_j=\max(\alpha_j,\beta_j)\text{，}\ 1\le j\le s\text{．}$$

以及 $(a,b)[a,b]=ab$．

例1 证明： $(a,[b,c])=[(a,b),(a,c)]$．

证明 若$a=0$，等式显然成立，所以可设a,b,c是正整数，

$$a=p_1^{\alpha_1}\cdots p_s^{\alpha_s}\text{，}\ b=p_1^{\beta_1}\cdots p_s^{\beta_s}\text{，}$$

$$c=p_1^{\gamma_1}\cdots p_s^{\gamma_s}\text{，}\ p_1<p_2<\cdots<p_s\text{．}$$

由推论 3 可得

$$(a,[b,c])=p_1^{\eta_1}\cdots p_s^{\eta_s}\text{，}$$

$$\eta_j=\min(\alpha_j,\max(\beta_j,\gamma_j))\text{，}\ 1\le j\le s\text{．}$$

$$[(a,b),(a,c)]=p_1^{\tau_1}\cdots p_s^{\tau_s}\text{，}$$

$$\tau_j=\max(\min(\alpha_j,\beta_j),\min(\alpha_j,\gamma_j))\text{，}\ 1\le j\le s\text{．}$$

容易验证，无论$\alpha_j,\beta_j,\gamma_j$有怎样的大小关系，总有$\tau_j=\eta_j(1\le j\le s)$成立．结论成立．

推论 4 设a是正整数， $\tau(a)$表示a的所有正除数的个数（通常称为**除数函数**）若a有标准素因数分解式（2），则

$$\tau(a)=(a_1+1)\cdots(a_s+1)=\tau(p_1^{a_1})\cdots\tau(p_s^{a_s})\text{．}$$

推论 5 设整数$a\ge 2$．

（1）若a是合数，则必有不可约数$p\mid a$， $p\le a^{1/2}$；

（2）若a有表示式（1），则必有不可约数$p\mid a$， $p\le a^{1/s}$．

注 利用推论 5 可以推出寻找素数的一种方法，即 Eratoschenes 筛法．对于求不超过整数n的素数，只需用小于$\sqrt{n}$ 的素数分别去除每一个小于n 的整数，每次都删去可以被整除的整数，最后余下的整数即为所求的素数．

例2 利用 Eratoschenes 筛法求出小于 100 的所有素数．

最后，我们将给出素分解的一种计算公式．在讨论$n!$的素分解之前，首先讨论一个相关的数论函数$[x]$．

定义 设 x 是实数，$[x]$ 表示不超过 x 的最大整数，称为 x 的**整数部分**，即 $[x]$ 是一个整数且满足

$$[x] \le x < [x]+1.$$

记 $\{x\} = x-[x]$，称为 x 的**小数部分**．显然

$$0 \le \{x\} < 1.$$

x 是整数的充要条件是 $\{x\}=0$．

数论函数 $[x]$ 有以下性质．

定理 2 设 x, y 是实数．我们有

（1） 若 $x \le y$，则 $[x] \le [y]$；

（2） 若 $x = m+v$，m 是整数，$0 \le v < 1$，则 $m=[x]$，$v=\{x\}$．特别地，当 $0 \le x < 1$ 时，$[x]=0$，$\{x\}=x$；

（3） 对任意整数 m 有：$[x+m]=[x]+m$，$\{x+m\}=\{x\}$．$\{x\}$ 是周期为 1 的周期函数；

（4） $[x]+[y] \le [x+y] \le [x]+[y]+1$，其中等号有且仅有一个成立；

（5）

$$[-x] = \begin{cases} -[x], & x \in Z, \\ -[x]-1, & x \notin Z. \end{cases}$$

及

$$\{-x\} = \begin{cases} -\{x\}=0, & x \in Z, \\ 1-\{x\}, & x \notin Z; \end{cases}$$

（6） 对正整数 m 有 $\left[\dfrac{[x]}{m}\right] = \left[\dfrac{x}{m}\right]$；

（7） 不小于 x 的最小整数是 $-[-x]$；

（8） 设 a 和 N 是正整数．那么正整数 $1, 2, \cdots, N$ 中被 a 整除的正整数的个数是 $[N/a]$．

证明 （1）由 $[x] \le x \le y < [y]+1$ 即得．

（2）由 $m \le x < m+1$ 即得．

（3）由

$$[x]+m \le x+m < ([x]+m)+1$$

即得．

（4）由

$$x+y = [x]+[y]+\{x\}+\{y\},$$

及

$$0 \le \{x\}+\{y\} < 2.$$

当 $0 \le \{x\}+\{y\} < 1$ 时，由（2）知

$$[x+y] = [x]+[y];$$

当 $1 \le \{x\}+\{y\} < 2$ 时，

$$x+y = ([x]+[y]+1)+(\{x\}+\{y\}-1),$$

由（2）知

$$[x+y] = [x]+[y]+1.$$

（5）x为整数时显然成立，x不为整数时，

$$-x=-[x]-\{x\}=-[x]-1+1-\{x\}，\ 0\le -\{x\}+1<1，$$

由（2）知成立.

（6）带余除法知，存在整数q,r使得

$$[x]=qm+r，\ 0\le r<m，$$

即

$$[x]/m=q+r/m，\ 0\le r/m<1，$$

由此及（2）推出$[[x]/m]=\mathrm{q}$．另一方面

$$x/m=[x]/m+\{x\}/m=q+(\{x\}+r)/m$$

注意到

$$0\le(\{x\}+r)/m<1，$$

由此及（2）推出$[x/m]=\mathrm{q}$，所以（6）成立.

（7） 设不小于x的最小整数是a，即$a-1<x\le a$，因$-a\le x<-a+1$，所以$-a=[-x]$，即$a=-[-x]$.

（8） 被a整除的正整数是

$$a,2a,3a,\cdots，$$

设1，2，…，N中被a整除的正整数个数为k，那么必有

$$ka\le N<(k+1)a.$$

即$k\le N/a<(k+1)$，得证.

另外我们还将引进一个符号.

定义 2 设k是非负整数，符号$a^k\parallel b$表示b恰好被a的k次方整除，即

$$a^k\mid b，\ a^{k+1}\nmid b.$$

定理 3 设n是正整数，p是素数．再设$\alpha=\alpha(p,n)$满足$p^\alpha\parallel n!$.

那么

$$\alpha=\alpha(p,n)=\sum_{j=1}^{\infty}[\frac{n}{p^j}].\qquad(3)$$

证明 式（3）右边实际上是一有限和，因为必存在k，使

$$p^k\le n<p^{k+1}，$$

所以

$$\alpha=\sum_{j=1}^{k}[\frac{n}{p^j}]\qquad(4)$$

设j是给定的正整数，c_j表示$1,2,\cdots,n$中能被p^j整除的数的个数，d_j表示$1,2,\cdots,n$中恰被p的j次方整除的数的个数．显见，

$$d_j=c_j-c_{j+1}.$$

由定理2（8）知

$$d_j=[n/p^j]-[n/p^{j+1}].$$

容易看出，当$j>k$时，$d_j=0$.

下面将$1,2,\cdots,n$分为两两不交的k个集合，第j个集合由$1,2,\cdots,n$中

恰被 p^j 整除的数组成．这样，第 j 个集合的所有数的乘积恰被 p 的 $j\cdot d_j$ 次方整除，所以

$$\alpha = 1\cdot d_1 + 2\cdot d_2 + \cdots + k\cdot d_k$$

由此即得式（4），所以（3）式成立．定理得证．

推论 6　设 n 是正整数。我们有

$$n! = \prod_{p\le n} p^{\alpha(p,n)}\ , \qquad (5)$$

这里连乘号表示对所有不超过 n 的素数求积，$\alpha(p,n)$ 由式（3）给出．此外显然有

$$\alpha(p_1,n) \le \alpha(p_2,n),\ \ p_2 < p_1 .$$

例 4 求 80!的十进制表示中零的个数．

解 这就是要求整数 k 使 $10^k \,\|\, 80!$，因为 $80!$ 的素分解中，素数越小，则 $\alpha = \alpha(p,n)$ 越大，故即求 $80!$ 中 5 的幂次．

$$\alpha = \alpha(5,80) = \sum_{j=1}^{\infty}[\frac{80}{5^j}] = [\frac{80}{5}] + [\frac{80}{25}] = 19\ ,$$

所以 $80!$ 的十进位表示中有 19 个零．

例5 设整数 $a_j > 0$，$1 \le j \le s$，

$$n = a_1 + a_2 + \cdots + a_s\ ,$$

证明：$n!/(a_1!a_2!\cdots a_s!)$ 是整数．

证明　由定理 **5**，只需证明对任意素数 p 必有

$$\alpha(p,n) \ge \alpha(p,a_1) + \alpha(p,a_2) + \cdots + \alpha(p,a_s)\ ,$$

进而即证明

$$[\frac{n}{p^j}] \ge [\frac{a_1}{p^j}] + [\frac{a_2}{p^j}] + \cdots + [\frac{a_s}{p^j}]\ ,$$

由 $n = a_1 + a_2 + \cdots + a_s$，及定理 **2** 性质 4 知上式成立，由此可推出 $n!/(a_1!a_2!\cdots a_s!)$ 是整数．

习题

1．利用 Eratoschenes 筛法求出 200 以内的全部素数．

2．设奇数 $n>1$，证明：n 是素数的充要条件是 n 不能表为三个或三个以上连续整数的和．

3．设 a 是奇数，证明：必有正整数 d 使 $(2^d - 5, a) = 1$．

4．求满足 $(a,b,c) = 10$，[a,b,c]=100 的全部正整数组 a,b,c．

5．设 a 是正整数，$\sigma(a)$ 表示 a 的所有正除数之和．证明：$\sigma(1) = 1$，当 a 有标准素因数分解式

$$a = p_1^{\alpha_1}\cdots p_s^{\alpha_s},\ \ p_1 < p_2 < \cdots < p_s\ ,$$

则

$$\sigma(a) = \frac{p_1^{\alpha_1+1}}{p_1 - 1}\cdots\frac{p_s^{\sigma_s+1}}{p_s - 1} = \prod_{j=1}^{s}\frac{p_j^{\alpha_j+1}}{p_j - 1} = \sigma(p_1^{\alpha_1})\cdots\sigma(_s^{\alpha_s})\ .$$

6．求 198 和 252 的最大公约数，并把它表为 198 和 252 的整系数线性组合．

7．求 $117x_1 + 21x_2 = 38$ 的解．

8．求$15x_1+10x_2+6x_3=61$的全部解．

9．证明：$(a,[b,c])=[(a,b),(a,c)]$．

10．证明：当$n>1$时，$1+1/2+\cdots+1/n$不是整数．

11．证明：（1）小于x的最大整数是$-[-x]-1$；

（2）大于x的最小整数是$[x]+1$；

（3）离x最近的整数是$[x+1/2]$和$-[-x+1/2]$．当$x+1/2$是整数时，这两个不同的整数和x等距；当$x+1/2$不是整数时，它们相等．

12．设$n\geq 1$．以$\phi(n)$记正整数$1,2,\cdots,n$中与n既约的数的个数．证明：

（i）$\phi(2)=\phi(2)=1$；

（ii）当$n\geq 3$时，$2\mid\phi(n)$；

（iii）当$n=p$为素数时，$\phi(p)=p-1$．

13．设$m>1$．证明：$m\nmid 2^m-1$．

14．证明：存在无穷多个n使$n\mid 2^n+1$．

15．证明：$13\mid a^2-7b^2$的充要条件是$13\mid a$，$13\mid b$．

16．设p是奇素数，q是2^p-1的素因数．证明：$q=2kp+1$．

17．当p为素数时，$M_p=2^p-1$形式的数称为 Mersenne 数．把这种数用二进位来表示，利用辗转相除法（出现的数均用二进位表示）来直接证明：所有的 Mersenne 数两两互素．

18．整系数多项式

$$p(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0,\quad a_n\neq 0.$$

证明：必有无穷多个整数值x，使得$p(x)$是合数．