●学习指导●

整数的唯一分解定理

朱翠蓉
(华中师范大学数学系)

整数的唯一分解定理:设 $a>1$,则必有

$$a=p_1p_2\cdots p_n \quad (1)$$

其中 $p_i(1\leqslant i\leqslant n)$ 是素数,在不计素数乘积的次序的意义下,表达式(1)是唯一的。

此定理又称作算术基本定理,它是初等数论中最基本的定理之一,是整除理论的中心内容;它反映了整数的本质,数论中许多结果都依赖于它。因此,透彻理解此定理并掌握它在初等数论中的基本应用应该作为学习的基本要求,下面围绕这一点谈 3 个问题。

1　整数唯一分解定理反映了整数的本质

教材(彭敦刚等编《初等数论》,华中师范大学出版社,1995 年 10 月出版。下同)中,整数的唯一分解定理按如下理论次序建立:

定义　一个大于 1 的整数,如果它的正因数只有 1 和它本身,则称之为素数,否则称之为合数。

此定义将全体正整数分为三类:{素数},{1},{合数},而整数的唯一分解定理讨论的是大于 1 的整数。由如上定义,很容易证明下面的定理 1、定理 2 和定理 3。

定理 1　1) $a>1$ 是合数的充要条件是 $a=bc$,$1<b<a$,$1<c<a$;

2) 若 $b>1$,p 是素数且 $b|p$,则 $b=p$。

定理 2　设 $a>1$ 为整数,则 a 的除 1 外的最小正因数 q 是素数,并且当 a 是合数时,$q\leqslant\sqrt{a}$。

定理 3　若 p 是素数,a 是任一整数,则 $p|a$ 或 $(p,a)=1$。

利用定理 3 很容易证明下面的定理 4。

定理 4　若 p 是素数,且 $p|ab$,则 $p|a$ 或 $p|b$。

最后,依赖定理 1、定理 2,借助数学归纳法,证明了对于大于 1 的整数 a,(1)式总成立(即大于 1 的整数 a 能分解成素数的连乘积),依据定理 4 可以证明(1)式的唯一性(即对大于 1 的整数 a,在不计素因子次序的意义下,分解式(1)是唯一的)。

从上可以看出,素数的定义是整数唯一分解定理成立的前提,整数的唯一分解定理反映了整数的本质属性。如,把自然数集换成自然数的子集 $S=\{3k+1|k=0,1,2,\cdots\}$,在 S 中如果定义"素数"为:对 S 中的数 a,如果 a 恰有两个因子在 S 中,则称 a 为 S 中的"素数"。按如此定义,4,7,10,13,19,22,25,31,……都是 S 中的"素数",那么 S 中的数 100 就有

$$100=4\times25,\quad 100=10\times10$$

这两种分解式了。也就是说,整数的唯一分解定理的结论在 S 中不成立。

2　大于 1 的整数的标准分解式

对大于 1 的整数 a,(1)式成立。将(1)中相同的素数合并,并按素数从小到大的顺序排列,即得 a 的标准分解式:

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k},\ p_1<p_2<\cdots<p_k \quad (2)$$

其中 p_i 是素数,$\alpha_i\geqslant1$,$i=1,2,\cdots,k$。

a 的标准分解式(2)是唯一确定的,因此,任一大于 1 的整数,除了通常所用的二进制、十进制、十二进制等多项式表示法外,素因子表示方法(即标准分解式)也是常用的表

收稿日期:1996-12-28

示形式，这在后面的例题中可以体会到。

下面几个简单的判别法有助于求一个数的标准分解式：(其中的数 a 均为十进制数)

①整数 a 能被 2 整除的充要条件是 a 的末位数字是偶数。②整数 a 能被 3 整除的充要条件是 a 的各位数字之和能被 3 整除。③整数 a 能被 5 整除的充要条件是 a 的末位数字是 0 或 5。④整数 a 能被 11 整除的充要条件是 a 的奇位数字的和与偶位数字的和之差能被 11 整除。⑤将 a 写成千进制数，即 $a=a_n\cdot 1000^n+a_{n-1}\cdot 1000^{n-1}+\cdots+a_1\cdot 1000+a_0, 0\leqslant a_i<1000$，则 a 能被 7(或 11，或 13)整除的充要条件是 $(a_0+a_2+\cdots)-(a_1+a_3+\cdots)=\sum\limits_{i=0}^{n}(-1)^i a_i$ 能被 7(或 11、或 13)整除。

例 1　求 82798848 的标准分解式。

解

$$
\begin{array}{r|l}
2 & 82798848 \\ \hline
2 & 41399424 \\ \hline
2 & 20699712 \\ \hline
2 & 10349856 \\ \hline
2 & 5174928 \\ \hline
2 & 2587464 \\ \hline
2 & 1293732 \\ \hline
2 & 646866 \\ \hline
3 & 323433 \\ \hline
3 & 107811 \\ \hline
3 & 35937 \\ \hline
3 & 11979 \\ \hline
3 & 3993 \\ \hline
11 & 1331 \\ \hline
11 & 121 \\ \hline
 & 11
\end{array}
$$

所以 $82798848=2^8\cdot 3^5\cdot 11^3$。

利用高斯函数可求出 $n!$ 的标准分解式。

例 2　求 29! 的标准分解式。

解　不超过 29 的素数有 2,3,5,7,11,13,17,19,23,29。又

$$2(29!)=[\frac{29}{2}]+[\frac{29}{2^2}]+[\frac{29}{2^3}]+[\frac{29}{2^4}]$$
$$=14+7+3+1=25$$

$$3(29!)=[\frac{29}{3}]+[\frac{29}{3^2}]+[\frac{29}{3^3}]$$
$$=9+3+1=13$$

$$5(29!)=[\frac{29}{5}]+[\frac{29}{5^2}]=5+1=6$$

$$7(29!)=[\frac{29}{7}]=4, 11(29!)=[\frac{29}{11}]=2$$

$$13(29!)=[\frac{29}{13}]=2$$

$$17(29!)=19(29!)=23(29!)$$
$$=29(29!)=1$$

所以 $29!=2^{25}\cdot 3^{13}\cdot 5^6\cdot 7^4\cdot 11^2\cdot 13^2\cdot 17\cdot 19\cdot 23\cdot 29$。

有时，为了叙述方便，常常令正整数 $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_m^{\alpha_m}, p_1<p_2<\cdots<p_m, \alpha_i\geqslant 0, i=1,2,\cdots,m$，这种表示法的依据还是整数的唯一分解定理。显然，这种表示法不是唯一的，它不是 a 的标准分解式。

例 3　已知 a,b,n 均为自然数，证明：若 $a^n|b^n$，则 $a|b$。

证明　设 $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}, b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}$，其中 $p_1,p_2,\cdots,p_k$ 是不同的素数，$\alpha_i,\beta_i\geqslant 0, i=1,2,\cdots,k$，

则　$a^n=p_1^{\alpha_1 n}p_2^{\alpha_2 n}\cdots p_k^{\alpha_k n}, b^n=p_1^{\beta_1 n}p_2^{\beta_2 n}\cdots p_k^{\beta_k n}$

因为 $a^n|b^n$，所以对任何 $i, 1\leqslant i\leqslant k$，有 $p_i^{\alpha_i n}|b^n$。又当 $i\neq j$ 时，$(p_i,p_j)=1$，故 $(p_i^{\alpha_i n}, p_j^{\beta_j n})=1$，所以 $p_i^{\alpha_i n}|p_i^{\beta_i n}$，从而 $\alpha_i n\leqslant\beta_i n$。已知 $n>0$，即有 $\alpha_i\leqslant\beta_i, i=1,2,\cdots,k$，故 $a|b$。

3　应用举例

整数的标准分解式是大于 1 的整数的一种表示形式，有时利用这种表示形式会给证明或计算带来很大的方便。

例 4　求 1996! 的末尾零的个数。

分析　显然，此题不是要求算出 1996! 是多少，而是要从理论上推导出 1996! 末尾零的个数。因 $2\times 5=10$，即 1996! 的末尾的零是由素因子 2 与 5 的乘积产生的，故只需考虑 1996! 的标准分解式中因子 2 与 5 的个数，而显然 $2(1996!)>5(1996!)$，故 1996! 末尾零的个数即为 $5(1996!)$。

解　因为

$$5(1996!)=\sum_{i=1}^{\infty}[\frac{1996}{5^i}]$$

$=399+79+15+3=496$

所以 1996! 的末尾有 496 个零。

例 5　证明:对任意整数 n,$60|n(n^2-1)(n^2-4)$。

证明　因为 $60=2^2\cdot 3\cdot 5$,$n(n^2-1)(n^2-4)=(n-2)(n-1)n(n+1)(n+2)$ 是 5 个连续整数的乘积,故 $5|n(n^2-1)(n^2-4)$,$4|n(n^2-1)(n^2-4)$,$3|n(n^2-1)(n^2-4)$。而 3,4,5 两两互素,$[3,4,5]=60$,所以 $60|n(n^2-1)(n^2-4)$。

利用教材第一章中的定理 5.1,借助整数的标准分解式,可以很快地求出几个正整数的最大公因数与最小公倍数。

例 6　求 $(1008,1260,882,1134)$ 与 $[1008,1260,882,1134]$。

解　$1008=2^4\cdot 3^2\cdot 7$

$1260=2^2\cdot 3^2\cdot 5\cdot 7$

$882=2\cdot 3^2\cdot 7^2$

$1134=2\cdot 3^4\cdot 7$

故　$(1008,1260,882,1134)=2\cdot 3^2\cdot 7=126$

$[1008,1260,882,1134]=2^4\cdot 3^4\cdot 5\cdot 7^2=317520$

虽然从理论上任意一个大于 1 的整数都能写出它的标准分解式,但在实际计算时,特别当 a 很大时,由于计算量太大,常常难以办到。因此,对较大的几个整数而言,用正整数的标准分解式求最大公因数或最小公倍数并不简单,一般采用辗转相除法求其最大公因数,然后利用 $[a,b]=\dfrac{ab}{(a,b)}$ 求其最小公倍数。

例 7　设 b 是任意的正整数,试证明 b 可以唯一表作 $b=a^2k$,其中 a^2 是平方数,k 是 1 或相异素数的乘积。

分析　由题意可知,解题时用正整数的标准分解式要容易些。

证明　当 $b=1$ 时,$a^2=1$,$k=1$,显然结论成立。当 $b>1$ 时,设 b 的标准分解式为

$$b=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$$

其中 $p_1,p_2,\cdots,p_s$ 是相异的素数,且 $\alpha_i\geqslant 1$,$i=1,2,\cdots,s$。

由带余除法,$\alpha_i=2q_i+r_i$,$r_i=0$ 或 1,$i=1,2,\cdots,s$。于是

$$b=(p_1^{q_1}p_2^{q_2}\cdots p_s^{q_s})^2\cdot p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s}$$

设 $a=p_1^{q_1}p_2^{q_2}\cdots p_s^{q_s}$,$k=p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s}$,

则　$$b=a^2k$$

其中 k 是 1 或相异素数的乘积。这就证明了 b 可以表成 a^2k 的形式。下证唯一性。

设 $b=c^2t$,t 是 1 或相异素数的乘积。为叙述方便,用 $p(m)$ 表示素数 p 在 m 的标准分解式中的幂指数,如此例中,$p_i(b)=\alpha_i$,$i=1,2,\cdots,s$。则根据指数运算的性质,有

$$\alpha_i=p_i(b)=p_i(c^2t)$$
$$=p_i(c^2)+p_i(t)=2p_i(c)+p_i(t)$$

由于 t 是 1 或相异素数的乘积,故 $p_i(t)=0$ 或 1,因此,$p_i(c)$ 和 $p_i(t)$ 分别是 α_i 被 2 除所得的商和余数。由带余除法知 $p_i(c)=q_i$,$p_i(t)=r_i$。于是 $a^2=c^2$,$k=t$。

例 8　证明:在数列 5,11,17,23,…,$6n-1$,…中含有无穷个素数。

分析　换一下表述形式,即为:证明有无穷多个形如 $6n-1$ 的素数。这样,即知此题的证明可仿教材第一章 § 4 例 4 的证明。其实这一证明的理论依据也是整数的唯一分解定理。证明略。

例 9　设整数 $a>1$,求 a 的所有正因数的个数。

解　设 a 的标准分解式为

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$$

若 d 为 a 的任一正因数,则 d 有形式

$$d=p_1^{x_1}p_2^{x_2}\cdots p_k^{x_k},0\leqslant x_i\leqslant\alpha_i,i=1,2,\cdots,k\quad(*)$$

显然,具有形式(*)的数 d 均为 a 的正因数,故 a 的全部正因数由(*)式表出。用 $\sigma_0(a)$ 表示 a 的所有正因数的个数,则

$$\sigma_0(a)=\sum_{d|a}1=(\sum_{x_1=0}^{\alpha_1}\sum_{x_2=0}^{\alpha_2}\cdots\sum_{x_k=0}^{\alpha_k})1$$
$$=(\sum_{x_1=0}^{\alpha_1}1)(\sum_{x_2=0}^{\alpha_2}1)\cdots(\sum_{x_k=0}^{\alpha_k}1)$$

$$= (\alpha_1+1)(\alpha_2+1)\cdots(\alpha_k+1) = \prod_{i=1}^{k}(\alpha_i+1)$$

其中 $\sum\limits_{d|a}$ 表示对 a 的所有正因数求和，下同。

例 10　求一个正整数的所有正因数的和。

证明　若 $a=1$，则 a 的所有正因数的和为 1。若 $a>1$，则设 a 的标准分解式为 $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，由例 9 知，$a$ 的所有正因数为

$$d=p_1^{x_1}p_2^{x_2}\cdots p_k^{x_k}, 0\leqslant x_i\leqslant\alpha_i, i=1,2,\cdots,k$$

则
$$\sigma(a)=\sum_{d|a}d=\sum_{x_1=0}^{\alpha_1}\sum_{x_2=0}^{\alpha_2}\cdots\sum_{x_k=0}^{\alpha_k}p_1^{x_1}p_2^{x_2}\cdots p_k^{x_k}$$
$$=(\sum_{x_1=0}^{\alpha_1}p_1^{x_1})(\sum_{x_2=0}^{\alpha_2}p_2^{x_2})\cdots(\sum_{x_k=0}^{\alpha_k}p_k^{x_k})$$
$$=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdot\cdots\cdot\frac{p_k^{\alpha_k+1}-1}{p_k-1}=\prod_{i=1}^{k}\frac{p_i^{\alpha_i+1}-1}{p_i-1}$$

例 9、例 10 所得的两个计算公式是中学竞赛中经常用到的。

例 11　1)证明：$\varphi(1)+\varphi(p)+\varphi(p^2)+\cdots+\varphi(p^\alpha)=p^\alpha$，$p$ 为素数。

2)a 为正整数，证明 $\sum\limits_{d|a}\varphi(d)=a$。

证明　1)由教材第三章定理 3.5，

$$\varphi(1)+\varphi(p)+\varphi(p^2)+\cdots+\varphi(p^\alpha)$$
$$=1+(p-1)+(p^2-p)+\cdots+(p^\alpha-p^{\alpha-1})=p^\alpha$$

2)若 $a=1$，则 $\sum\limits_{d|1}\varphi(d)=1$，结论成立。

若 $a>1$，设 $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ 为 a 的标准分解式，则 a 的全部正因数可表为

$$d=p_1^{x_1}p_2^{x_2}\cdots p_k^{x_k}, 0\leqslant x_i\leqslant\alpha_i, i=1,2,\cdots,k$$

于是
$$\sum_{d|a}\varphi(d)=\sum_{x_1=0}^{\alpha_1}\sum_{x_2=0}^{\alpha_2}\cdots\sum_{x_k=0}^{\alpha_k}\varphi(p_1^{x_1}p_2^{x_2}\cdots p_k^{x_k})$$
$$=\sum_{x_1=0}^{\alpha_1}\sum_{x_2=0}^{\alpha_2}\cdots\sum_{x_k=0}^{\alpha_k}\varphi(p_1^{x_1})\varphi(p_2^{x_2})\cdots\varphi(p_k^{x_k})$$
$$=\sum_{x_1=0}^{\alpha_1}\varphi(p_1^{x_1})\cdot\sum_{x_2=0}^{\alpha_2}\varphi(p_2^{x_2})\cdot\cdots\cdot\sum_{x_k=0}^{\alpha_k}\varphi(p_k^{x_k})$$
$$=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}=a$$

在讨论同余问题时，常利用正整数的标准分解式以及同余的性质，将合数模的同余问题转化为素数模的同余问题来解决。

例 12　若 $20^n+16^n-3^n-1$ 能被 323 整除，求正整数 n。

解　由于 $323=17\times19$，且 $(17,19)=1$，故 $20^n+16^n-3^n-1\equiv0 \pmod{323}$ 等价于

$$\begin{cases}20^n+16^n-3^n-1\equiv0 \pmod{17}\\20^n+16^n-3^n-1\equiv0 \pmod{19}\end{cases}$$

而
$$20^n+16^n-3^n-1\equiv3^n+(-1)^n-3^n-1\equiv(-1)^n-1 \pmod{17}$$

故当 n 为偶数时，

有　$20^n+16^n-3^n-1\equiv0 \pmod{17}$

当 n 为奇数时，

有　$20^n+16^n-3^n-1\not\equiv0 \pmod{17}$

又
$$20^n+16^n-3^n-1\equiv1^n+(-3)^n-3^n-1\equiv(-3)^n-3^n \pmod{19}$$

故当 n 为偶数时，

有　$20^n+16^n-3^n-1\equiv0 \pmod{19}$

当 n 为奇数时，

有　$20^n+16^n-3^n-1\not\equiv0 \pmod{19}$

综上知，所求的正整数 n 是全体正偶数。

例 13　解同余方程 $6x^3+27x^2+17x+20\equiv0 \pmod{15}$。

解　因为 $15=3\times5$，所以

$$6x^3+27x^2+17x+20\equiv0 \pmod{15}$$
$$\Leftrightarrow\begin{cases}6x^3+27x^2+17x+20\equiv0 \pmod 3\\6x^3+27x^2+17x+20\equiv0 \pmod 5\end{cases}$$
$$\Leftrightarrow\begin{cases}2x+2\equiv0 \pmod 3\\x^3+2x^2+2x\equiv0 \pmod 5\end{cases}$$

而 $2x+2\equiv0 \pmod 3$ 的解为

$$x\equiv2 \pmod 3$$

$x^3+2x^2+2x\equiv0 \pmod 5$ 的解为

$$x\equiv0,1,2 \pmod 5$$

由孙子定理，分别解同余式组

$$\begin{cases}x\equiv2 \pmod 3,\\x\equiv0 \pmod 5,\end{cases}\quad\begin{cases}x\equiv2 \pmod 3,\\x\equiv1 \pmod 5,\end{cases}\quad\begin{cases}x\equiv2 \pmod 3\\x\equiv2 \pmod 5\end{cases}$$

得　$x\equiv5,11,2 \pmod{15}$

故原同余方程的解为

$$x\equiv2,5,11 \pmod{15}$$