

## 一对数论对偶公式的另证和推广

彭明海  
(数学系)

在文[1]中,介绍了下面两个有用的公式:设  $a, b, c \in N$ , 有

$$1^\circ \quad [(a, b), (a, c)] = (a, [b, c])$$

$$2^\circ \quad ([a, b], [a, c]) = [a, (b, c)]$$

其中, " $[x, y]$ " 表示整数  $x$  与  $y$  的最小公倍数, " $(x, y)$ " 表示整数  $x$  与  $y$  的最大公约数.

一般的证法是:将  $a, b, c$  写成质数幂的积再根据最小公倍数、最大公约数同这些幂指数的关系进行论证.

本文仅利用大家熟知的最大公约数与最小公倍数的基本性质,很自然地证明了  $1^\circ, 2^\circ$  成立.然后将它们作有趣的推广.推广后的公式在数论中是有用的.

证明  $1^\circ$

$$\therefore \text{左} = \frac{(a, b)(a, c)}{((a, b), (a, c))} = \frac{(a, b)(a, c)}{(a, b, c)}$$

$$\text{右} = (a, \frac{bc}{(b, c)})$$

$$\therefore (a, b, c)(b, c) \cdot \text{左} = (a, b)(a, c)(b, c)$$

$$(a, b, c)(b, c) \cdot \text{右} = (a, b, c)(ab, ac, bc)$$

$$\therefore \text{要证左} = \text{右} \quad \text{只需证: } (a, b)(a, c)(b, c) = (a, b, c)(ab, ac, bc)$$

$$\begin{aligned} \text{而 } (a, b)(a, c)(b, c) &= ((a, b)a, (a, b)c)(b, c) \\ &= (a^2(b, c), ab(b, c), ac(b, c), bc(b, c)) \\ &= (ab(a, b, c), ac(a, b, c), bc(a, b, c)) \\ &= (a, b, c)(ab, ac, bc) \end{aligned}$$

我们利用  $1^\circ$  证明  $2^\circ$ : 据  $1^\circ$  知

$$\begin{aligned} ([a, b], [a, c]) &= ([([a, b], a), ([a, b], c)]) \\ &= ([a, (a, b), (a, c)], (b, c)) \\ &= [a, (b, c)] \end{aligned}$$

实际上  $1^\circ$  与  $2^\circ$  是等价的, 以上据  $1^\circ$  证明了  $2^\circ$ , 我们也可以据  $2^\circ$  证明  $1^\circ$ .  $\therefore$  据  $2^\circ$  知

$$\begin{aligned} [(a, b), (a, c)] &= ([([a, b], a), ([a, b], c)]) \\ &= ([([a, a], [b, a]), ([a, c], [b, c]))) \\ &= (a, [a, b], [a, c], [b, c]) \end{aligned}$$

$$= (a, [b, c])$$

这就是我们之所以将  $1^0$  与  $2^0$  叫做对偶公式的原因。

下面我们对  $1^0$  推广如下:

$3^0$  设  $a, b_1, b_2, \dots, b_n \in N, (n \geq 2)$  则有  $(a, [b_1, b_2, \dots, b_n]) = [(a, b_1), (a, b_2), \dots, (a, b_n)]$

我们用数学归纳法证明  $3^0$ : 当  $n=2$  时, 据  $1^0$  知  $3^0$  成立。假定  $n$  时命题成立, 视  $n+1$  的情形:

$$\begin{aligned} \because (a, [b_1, b_2, \dots, b_{n+1}]) &= (a, [[b_1, b_2, \dots, b_n], b_{n+1}]) \\ &= [(a, [b_1, b_2, \dots, b_n]), (a, b_{n+1})] \\ &= [[(a, b_1), (a, b_2), \dots, (a, b_n)], (a, b_{n+1})] \\ &= [(a, b_1), (a, b_2), \dots, (a, b_n), (a, b_{n+1})] \end{aligned}$$

$\therefore n+1$  时  $3^0$  成立, 归纳证毕。

$4^0$  设  $a_1, a_2, b_1, b_2, \dots, b_n \in N (n \geq 2)$  则

$$([a_1, a_2], [b_1, b_2, \dots, b_n]) = [(a_1, b_1), (a_1, b_2), \dots, (a_1, b_n), (a_2, b_1), \dots, (a_2, b_n)]$$

证明: 据  $3^0$  知

$$\begin{aligned} ([a_1, a_2], [b_1, b_2, \dots, b_n]) &= [(a_1, [b_1, b_2, \dots, b_n]), (a_2, [b_1, b_2, \dots, b_n])] \\ &= [[(a_1, b_1), (a_1, b_2), \dots, (a_1, b_n)], (a_2, [b_1, b_2, \dots, b_n])] \\ &= [(a_1, b_1), (a_1, b_2), \dots, (a_1, b_n), (a_2, b_1), (a_2, b_2), \dots, (a_2, b_n)] \end{aligned}$$

$5^0$  设  $a_1, a_2, \dots, a_m; b_1, b_2, \dots, b_n \in N$ , 则

$$([a_1, a_2, \dots, a_m], [b_1, b_2, \dots, b_n]) = [(a_1, b_1), (a_1, b_2), \dots, (a_1, b_n), (a_2, b_1), (a_2, b_2), \dots, (a_2, b_n), \dots, (a_m, b_1), (a_m, b_2), \dots, (a_m, b_n)]$$

据  $4^0$ , 可用数学归纳法证明  $5^0$ , 这里证明从略。

我们用符号  $\prod_{\substack{1 \leq i \leq 3 \\ 1 \leq j \leq 2}} (a_i, b_j)$  表示  $2 \times 3 = 6$  个最大公约数的排列缩写。

即

$$\prod_{\substack{1 \leq i \leq 3 \\ 1 \leq j \leq 2}} (a_i, b_j) \triangleq (a_1, b_1), (a_1, b_2), (a_1, b_3), (a_2, b_1), (a_2, b_2), (a_2, b_3), \prod_{\substack{1 \leq i \leq 3 \\ 1 \leq j \leq 2}} [a_i, b_j] \text{ 同义。}$$

$6^0$  设  $a_{11}, a_{12}, \dots, a_{1s_1}; a_{21}, a_{22}, \dots, a_{2s_2}, \dots, a_{k1}, a_{k2}, \dots, a_{ks_k} \in N$ , 其中  $s_1, s_2, \dots, s_k \in N$ , 则有

$$\begin{aligned} ([a_{11}, a_{12}, \dots, a_{1s_1}], [a_{21}, a_{22}, \dots, a_{2s_2}], \dots, [a_{k1}, a_{k2}, \dots, a_{ks_k}]) \\ = \prod_{\substack{1 \leq i_1 \leq s_1 \\ 1 \leq i_2 \leq s_2 \\ \vdots \\ 1 \leq i_k \leq s_k}} (a_{1i_1}, a_{2i_2}, \dots, a_{ki_k}) \end{aligned}$$

据  $5^0$  可用数学归纳法证明  $6^0$  成立。这也略去证明 ( $\because$  当  $k=2$  时,  $6^0$  即  $5^0$ )

我们可类似地对公式  $2^0$  作如下的推广:

$$7^{\circ} [a, (b_1, b_2, \dots, b_n)] = ([a, b_1], [a, b_2], \dots, [a, b_n])$$

其中  $a, b_1, b_2, \dots, b_n \in N$

$$8^{\circ} [(a_1, a_2), (b_1, b_2, \dots, b_n)] = ([a_1, b_1], [a_1, b_2], \dots, [a_1, b_n], [a_2, b_1], \dots, [a_2, b_n])$$

其中  $a_1, a_2, b_1, b_2, \dots, b_n \in N$

$$9^{\circ} [(a_1, a_2, \dots, a_m), (b_1, b_2, \dots, b_n)] = ([a_1, b_1], \dots, [a_1, b_n], [a_2, b_1], \dots, [a_m, b_n])$$

其中  $a_1, a_2, \dots, a_m, b_1, b_2, \dots, b_n \in N$ ,

$$10^{\circ} [(a_{11}, a_{12}, \dots, a_{1i_1}), (a_{21}, a_{22}, \dots, a_{2i_2}), \dots, (a_{k1}, a_{k2}, \dots, a_{ki_k})]$$

$$= ([a_{1i_1}, a_{2i_2}, \dots, a_{ki_k}])$$

$$11^{\circ} [(a_1, a_2), (b_1, b_2)] = ([a_1, b_1, b_2], [a_2, b_1, b_2])$$

在  $11^{\circ}$  中当  $b_1=b_2$  时,就是公式  $2^{\circ}$ 。

$$12^{\circ} [(a_1, a_2), (b_1, b_2)] = [(a_1, b_1, b_2), (a_2, b_1, b_2)]$$

在  $12^{\circ}$  中当  $b_1=b_2$  时就是公式  $1^{\circ}$

从形式上看,  $11^{\circ}$  与  $12^{\circ}$  也是对偶的。从中易发现一些规律。

根据以上各条性质,运用数学归纳法易得出:

设  $a_1, a_2, b_1, b_2, \dots, b_n \in N$  时,有

$$13^{\circ} [(a_1, a_2), [b_1, b_2, \dots, b_n]] = ([a_1, b_1, b_2, \dots, b_n], [a_2, b_1, b_2, \dots, b_n])$$

$$14^{\circ} ([a_1, a_2], (b_1, b_2, \dots, b_n)) = ([a_1, b_1, b_2, \dots, b_n], (a_2, b_1, b_2, \dots, b_n))$$

对  $13^{\circ}, 14^{\circ}$  还可推广为:  $a_1, a_2, \dots, a_m, b_1, b_2, \dots, b_n \in N$ , 有

$$15^{\circ} [(a_1, a_2, \dots, a_m), [b_1, b_2, \dots, b_n]] = ([a_1, b_1, b_2, \dots, b_n], [a_2, b_1, b_2, \dots, b_n], \dots, [a_m, b_1, b_2, \dots, b_n])$$

$$16^{\circ} ([a_1, a_2, \dots, a_m], (b_1, b_2, \dots, b_n)) = ([a_1, b_1, b_2, \dots, b_n], (a_2, b_1, \dots, b_n), \dots, (a_m, b_1, b_2, \dots, b_n))$$

当然,对  $15^{\circ}$  和  $16^{\circ}$  还可推广,这里限于篇幅不再推导了,也留给读者去作。

## 参考文献

[1] 曾荣,王玉,基础数论典型题解 300 例,

[2] 华罗庚,数论导引。