

# 关于最大公因数的一个性质及证明

赵云平

(临沧师范高等专科学校 数理系, 云南 临沧 677099)

**【摘要】**最大公因数也称最大公约数,是两个或多个整数共有约数中最大的一个。本文主要讨论两个整数的最大公因数的性质,并给出具体的证明。

**【关键词】**最大公因数;辗转相除法;整除;性质

**【中图分类号】**O156.1 **【文献标志码】**A **【文章编号】**1673-1891(2015)02-0030-02

DOI:10.16104/j.cnki.xccxb.2015.02.011

## 1 预备知识

在数论里,最大公因数是一个非常重要的概念。最大公因数满足两条,一是公因数,二是最大。这个公因数到底存不存在呢?实际上这个公因数的存在性是比较容易判断的,因为1是任何整数的约数,所以公因数肯定是存在的,至少也有个1。那最大会不会存在呢?比如两个整数都取成0,而0可以被任何非零整数整除,所以它的公约数是任何的整数,要找最大,就找不到了。如果不全为0的话,有这样明显的结论,若 $a_1, a_2, \dots, a_n$ 不全为0,则它们的最大公因数是存在的。存在的话,关于最大公因数还有哪些重要的结论,这是本文研究的出发点。首先来回顾一下最大公因数的概念<sup>[1-5]</sup>。

**定义1:**若 $a_1, a_2, \dots, a_n$ 是 $n(n \geq 2)$ 个整数,整数 $d$ 是所有 $a_i$ 的因数,称 $d$ 是 $a_1, a_2, \dots, a_n$ 的公因数。整数 $a_1, a_2, \dots, a_n$ 的公因数中最大的一个,称为 $a_1, a_2, \dots, a_n$ 的最大公因数,记作 $a_1, a_2, \dots, a_n$ 。

**定理1:**若 $a_1, a_2, \dots, a_n$ 是任意个不全为零的整数,则

$$(a_1, a_2, \dots, a_n) = (|a_1|, |a_2|, \dots, |a_n|)。$$

也就是说将来在讨论最大公因数的时候,如果里边的数有负号,可以把负号去掉。

**定理2:**若 $b \neq 0, b \in \mathbb{Z}$ ,则 $(0, b) = |b|$

**定理3:**设 $a, b, c$ 是任意三个不全为0的整数,且 $a=bq+c$ ,其中 $q$ 是非零整数,则 $(a, b)=(b, c)$ 。

**证明:**设 $(a, b)=d_1, (b, c)=d_2$ ,证明这两个公因数相等即要证明 $d_1=d_2$ ,只要证明 $d_1 \leq d_2, d_2 \leq d_1$ 同时成立,那么这两个公因数相等。

i)证 $d_1 \leq d_2$ ,由已知 $(a, b)=d_1$ ,则 $d_1|a, d_1|b$ ,又 $c=a-bq$ ,则 $d_1$ 也能整除 $a, b$ 的线性组合,所以 $d_1|c$ 。由 $d_1|b, d_1|c$ ,推出 $d_1$ 是 $b, c$ 的公因数,又因为 $(b, c)=d_2$ ,所以 $d_1 \leq d_2$ 。

ii)证 $d_2 \leq d_1$ ,由已知 $(b, c)=d_2$ ,则 $d_2|b, d_2|c$ ,又 $a=bq+c$ ,

则 $d_2$ 也能整除 $b, c$ 的线性组合,所以 $d_2|a$ 。由 $d_2|a, d_2|b$ ,推出 $d_2$ 是 $a, b$ 的公因数,又因为 $(a, b)=d_1$ ,所以 $d_2 \leq d_1$ 。

综上所述, $d_1=d_2$ ,即 $(a, b)=(b, c)$ 。

定理3的好处就是在求最大公因数的时候,可以将大数化为小数来求,如此反复进行下去就是所谓的辗转相除法。

## 2 最大公因数的性质

下面针对最大公因数的一个性质,给出详细及不同证明方法。

**性质<sup>[2]</sup>:**设 $a, b$ 是任意两个不全为零的整数,则

(i)若 $m$ 是任一正整数,则 $(am, bm)=(a, b)m$ 。

(ii)若 $\delta$ 是 $a, b$ 的任一公因数,则 $(\frac{a}{\delta}, \frac{b}{\delta}) = \frac{(a, b)}{|\delta|}$ ,特别。

教科书中对于证明过程已经写得很好了,但是不够明确。

**证明:**当 $a, b$ 有一个为零时,由定理2,定理显然成立,下面设 $a, b$ 都不为零 $(\frac{a}{(a, b)}, \frac{b}{(a, b)}) = 1$

(i)证法(一),

由定理1,假定 $a, b > 0$ ,由辗转相除法,有

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b$$

$$b = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1$$

⋮

$$r_{n-2} = r_{n-1}q_n + r_n, \quad 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = r_nq_{n+1} + r_{n+1}, \quad r_{n+1} = 0$$

此时, $(a, b) = r_n$

上述式子左右两侧同乘正整数 $m$ ,

$$ma = mbq_1 + mr_1, \quad 0 \leq mr_1 < mb$$

$$mb = mr_1q_2 + mr_2, \quad 0 \leq mr_2 < mr_1$$

⋮

$$mr_{n-2} = mr_{n-1}q_n + mr_n, \quad 0 \leq mr_n < mr_{n-1}$$

$$mr_{n-1} = mr_nq_{n+1} + mr_{n+1}, \quad mr_{n+1} = 0$$

$$\text{令 } a' = ma, b' = mb, r_1' = mr_1, r_2' = mr_2, \dots, r_{n-2}' = mr_{n-2},$$

收稿日期:2015-05-03

作者简介:赵云平(1982-),女,云南临沧人,硕士,讲师,研究方向:基础数学数论应用,应用数学运筹学线性规划,数值代数。

$r_{n-1}' = mr_{n-1}, r_n' = mr_n, r_{n+1}' = mr_{n+1}$ , 有

$$a' = b'q_1 + r_1', \quad 0 \leq r_1' < b'$$

$$b' = r_1'q_2 + r_2', \quad 0 \leq r_2' < r_1'$$

⋮

$$r_{n-2}' = r_{n-1}'q_n + r_n', \quad 0 \leq r_n' < r_{n-1}'$$

$$r_{n-1}' = r_n'q_{n+1} + r_{n+1}', \quad r_{n+1}' = 0,$$

有  $(a', b') = r_n'$ ,

即  $(ma, mb) = r_n' = mr_n = m(a, b)$ 。

证法(二),

设  $(am, bm) = c_1, (a, b) = c_2$ , 下面证  $c_1 = mc_2$

由  $(am, bm) = c_1$ , 有  $c_1 | am$  且  $c_1 | bm$ ,

由整除的定义, 存在整数  $d_1, d_2$ , 使

$$am = c_1 d_1, \quad bm = c_1 d_2 \cdots \cdots (1)$$

由  $(a, b) = c_2$ , 有  $c_2 | a$  且  $c_2 | b$ ,

由整除的定义, 存在整数  $d_1', d_2'$ , 使

$$a = c_2 d_1', \quad b = c_2 d_2' \cdots \cdots (2)$$

将(2)式代入(1)式, 得

$$c_2 d_1' m = c_1 d_1, \quad c_2 d_2' m = c_1 d_2,$$

又因  $(d_1', d_2') = 1$

所以  $c_1 | c_2 m, c_1 \leq c_2 m \cdots \cdots (3)$

下证  $c_2 m \leq c_1$ ,

$$\text{又 } ma = mc_2 d_1', \quad mb = mc_2 d_2'$$

则  $mc_2$  是  $(ma, mb)$  的公约数,

所以  $c_2 m \leq c_1 \cdots \cdots (4)$

#### 注释及参考文献:

[1]陈全国,刘森.关于最大公因数和最小公倍数的一点注记[J].牡丹江大学学报,2014(10):140-141.

[2]闵嗣鹤,严士健.初等数论(第三版)[M].北京:高等教育出版社,2003.

[3]课程教材研究所.初等数论[M].北京:人民教育出版社,2006.

[4]胡典顺,徐汉文.初等数论[M].北京:科学出版社,2010.

[5]潘承洞,潘承彪.初等数论[M].北京:北京大学出版社,2002.

## One Property of the Greatest Common Factor and Its Proof

ZHAO Yun-ping

(Department of Mathematics and Science, Lincang Teachers' College, Lincang, Yunnan 677099)

**Abstract:** The greatest common factor is also called the highest common divisor, which is the highest one of the common divisors of two or more integers. The property of the greatest common factor of two integers will be mainly discussed with its concrete proof.

**Key words:** the greatest common factor; algorithm of division; divisibility; the property

由(3)(4),得  $c_1 = mc_2$

在求解最大公因数过程中,应用定理(i)可以简化计算。

(ii)由结论(i),

$$\left(\frac{a}{\delta}, \frac{b}{\delta}\right) |\delta| = \left(\frac{|a|}{|\delta|} |\delta|, \frac{|b|}{|\delta|} |\delta|\right) = (|a|, |b|) = (a, b)$$

在等式两边同除  $|\delta|$ , 得

$$\left(\frac{a}{\delta}, \frac{b}{\delta}\right) = \frac{(a, b)}{|\delta|}.$$

特别的,取  $\delta = (a, b)$ , 有

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

也就是说,  $a$  和  $b$  都除以最大公因数求它们的最大公因数是互质的。

由此就得到处理  $(a, b) = d$  的一个很好的办法:

如果  $(a, b) = d$ , 那么  $a = da_1, b = db_1$ , 且  $(a_1, b_1) = 1$ 。

反过来也是对的,  $d$  是  $a, b$  的公约数, 若  $a = da_1, b = db_1$ , 且  $(a_1, b_1) = 1$ , 那么  $(a, b) = d$ 。这是处理最大公因数的一个非常有用的方法。

### 3 结论

本文利用辗转相除法和相互整除的关系证明了两个数的最大公因数的性质(i), 从而比较容易地证明了性质(ii), 如果是多个数的公因数需要做进一步讨论。