THE TEACHING OF MATHEMATICS

2018, Vol. XXI, 2, pp. 73–79

A GREATEST COMMON DIVISOR IDENTITY

Yuanhong Zhi

Abstract. In this paper we present an identity involving the greatest common divisors of almost all possible subproducts of n nonzero integers. Then we prove this identity, with the help of the fundamental theorem of arithmetic, and an identity concerning the minimum function min. As a consequence, a new formula for the least common multiple is derived.

MathEduc Subject Classification: F64

MSC Subject Classification: 97F60

Key words and phrases: Greatest common divisor; fundamental theorem of arithmetic; least common multiple.

In this paper, we present an identity expressing the relationship between the greatest common divisors of almost all possible subproducts of n nonzero integers. This identity can be viewed as a kind of generalized version of the elementary identity (see [3] for reference)

$$\gcd(ab, ac, bc) = \frac{\gcd(a, b) \cdot \gcd(a, c) \cdot \gcd(b, c)}{\gcd(a, b, c)},$$

which is easily checked, and proved (we also give a proof at the end of this paper). Here and below, gcd denotes the greatest common divisor, and lcm the least common multiple. Sometimes we also write the gcd of a and b as (a, b), if there is no ambiguity. In the following, we first state and prove the identity, and then give a direct corollary, which represents lcm by gcd's.

1. Main result

We are going to prove the following identity.

THEOREM 1. *For all nonzero integers $a_1, \dots, a_n$, with $n \geq 3$, we have*

$$\gcd\Big(\prod_{j\neq 1} a_j, \prod_{j\neq 2} a_j, \dots, \prod_{j\neq k} a_j, \dots, \prod_{j\neq n} a_j\Big) = \begin{cases} \frac{G(2)\cdot G(4)\cdots G(n-1)}{G(3)\cdot G(5)\cdots G(n)}, & \text{if } n \text{ is odd,} \\ \frac{G(2)\cdot G(4)\cdots G(n)}{G(3)\cdot G(5)\cdots G(n-1)}, & \text{if } n \text{ is even,} \end{cases}$$

where $\prod_{j\neq k} a_j := \prod_{\substack{p=1\\ p\neq k}}^{n} a_j = a_1 \cdots \widehat{a_k} \cdots a_n$, *where the notation* $\widehat{\ }$ *means the number under it is skipped, and*

$$\begin{aligned} G(2) &:= \prod_{1\le i<j\le n} \gcd(a_i, a_j),\\ G(3) &:= \prod_{1\le i<j<k\le n} \gcd(a_i, a_j, a_k),\\ &\cdots\\ G(k) &:= \prod_{1\le \sigma_1<\sigma_2<\cdots<\sigma_k\le n} \gcd(a_{\sigma_1}, a_{\sigma_2}, \ldots, a_{\sigma_k}),\\ &\cdots\\ G(n) &:= \gcd(a_1, \ldots, a_n). \end{aligned}$$

Particularly, for every three nonzero integers a, b, c,

$$\gcd(ab, bc, ca) = \frac{\gcd(a,b)\cdot\gcd(b,c)\cdot\gcd(c,a)}{\gcd(a,b,c)}; \tag{1}$$

and for four nonzero integers a, b, c, d,

$$\begin{aligned} \gcd(abc, abd, acd, bcd) &= \frac{(a,b)\cdot(a,c)\cdot(a,d)\cdot(b,c)\cdot(b,d)\cdot(c,d)\cdot(a,b,c,d)}{(a,b,c)\cdot(a,b,d)\cdot(a,c,d)\cdot(b,c,d)}\\ &= \frac{G_2\cdot G_4}{G_3}, \end{aligned}$$

where

$$\begin{aligned} &G_2 := \gcd(a,b)\cdot\gcd(a,c)\cdot\gcd(a,d)\cdot\gcd(b,c)\cdot\gcd(b,d)\cdot\gcd(c,d),\\ &G_3 := \gcd(a,b,c)\cdot\gcd(a,b,d)\cdot\gcd(a,c,d)\cdot\gcd(b,c,d), \quad G_4 := \gcd(a,b,c,d). \end{aligned}$$

In order to prove Theorem 1, we need the following lemma.

Lemma 1. *Let* n *be an integer with* $n \ge 3$. *Suppose* $a_1, \ldots, a_n$ *are real numbers. Then we have the following identities:*

(a) *If* n *is odd, then*

(2)

$$\begin{aligned} &\min\{a_1, a_2\} + \min\{a_1, a_3\} + \cdots + \min\{a_{n-1}, a_n\}\\ &\qquad + \min\{a_1, a_2, a_3, a_4\} + \cdots + \min\{a_{n-3}, a_{n-2}, a_{n-1}, a_n\}\\ &\qquad + \min\{a_1, a_2, \ldots, a_6\} + \cdots + \min\{a_{n-5}, a_{n-4}, a_{n-3}, a_{n-2}, a_{n-1}, a_n\}\\ &\qquad + \cdots + \min\{a_1, \ldots, a_{n-1}\} + \cdots + \min\{a_2, a_3, \ldots, a_n\}\\ &\quad = \min\{a_{\sigma_1} + a_{\sigma_2} + \cdots + a_{\sigma_{n-1}} \mid 1 \le \sigma_1 < \sigma_2 < \cdots < \sigma_{n-1} \le n\}\\ &\qquad + \min\{a_1, a_2, a_3\} + \min\{a_1, a_2, a_4\} + \cdots + \min\{a_{n-2}, a_{n-1}, a_n\}\\ &\qquad + \min\{a_1, a_2, a_3, a_4, a_5\} + \cdots + \min\{a_{n-4}, a_{n-3}, a_{n-2}, a_{n-1}, a_n\}\\ &\qquad + \cdots + \min\{a_1, \ldots, a_n\}; \end{aligned}$$

(b) *if n is even, then*

$$\begin{aligned}
&\min\{a_1,a_2\}+\min\{a_1,a_3\}+\cdots+\min\{a_{n-1},a_n\}\\
&\qquad+\min\{a_1,a_2,a_3,a_4\}+\cdots+\min\{a_{n-3},a_{n-2},a_{n-1},a_n\}\\
&\qquad+\min\{a_1,a_2,\ldots,a_6\}+\cdots+\min\{a_{n-5},a_{n-4},a_{n-3},a_{n-2},a_{n-1},a_n\}\\
&\qquad+\cdots+\min\{a_1,\ldots,a_n\}\\
&\quad=\min\{a_{\sigma_1}+a_{\sigma_2}+\cdots+a_{\sigma_{n-1}}\mid 1\le\sigma_1<\sigma_2<\cdots<\sigma_{n-1}\le n\}\\
&\qquad+\min\{a_1,a_2,a_3\}+\min\{a_1,a_2,a_4\}+\cdots+\min\{a_{n-2},a_{n-1},a_n\}\\
&\qquad+\min\{a_1,a_2,a_3,a_4,a_5\}+\cdots+\min\{a_{n-4},a_{n-3},a_{n-2},a_{n-1},a_n\}\\
&\qquad+\cdots+\min\{a_1,\ldots,a_{n-1}\}+\cdots+\min\{a_2,a_3,\ldots,a_n\}.
\end{aligned}$$

Proof. We shall prove just the case when n is odd, for the proof of the case when n is even is similar. Let n be a positive odd integer with $n \ge 3$. Since the desired identity is transpositionally, and cyclically symmetrical, it suffices to consider the case of $a_1 \le a_2 \le \cdots \le a_n$. Then the left-hand side of (2) equals

$$\sum_{k=1}^{\frac{n-1}{2}}\sum_{j=1}^{n-2k+1} a_j\binom{n-j}{2k-1},$$

while its right-hand side is

$$\sum_{j=1}^{n-1} a_j+\sum_{l=1}^{\frac{n-1}{2}}\sum_{j=1}^{n-2l} a_j\binom{n-j}{2l}.$$

Hence, it suffices to show

$$\sum_{k=1}^{\frac{n-1}{2}}\sum_{j=1}^{n-2k+1} a_j\binom{n-j}{2k-1}=\sum_{j=1}^{n-1} a_j+\sum_{l=1}^{\frac{n-1}{2}}\sum_{j=1}^{n-2l} a_j\binom{n-j}{2l}. \tag{3}$$

Indeed, since for every positive integer m, by the binomial theorem,

$$\begin{aligned}
0^m&=\bigl(1+(-1)\bigr)^m=\sum_{j=0}^{m}\binom{m}{j}(-1)^j\\
&=\binom{m}{0}-\binom{m}{1}+\binom{m}{2}-\binom{m}{3}+\cdots+(-1)^m\binom{m}{m},
\end{aligned}$$

it follows that

$$\begin{aligned}
&\binom{m}{0}+\binom{m}{2}+\binom{m}{4}+\cdots+\binom{m}{m}\\
&\qquad=\binom{m}{1}+\binom{m}{3}+\binom{m}{5}+\cdots+\binom{m}{m-1},
\end{aligned}\tag{4}$$

if m is even, and

$$\binom{m}{0}+\binom{m}{2}+\binom{m}{4}+\cdots+\binom{m}{m-1} = \binom{m}{1}+\binom{m}{3}+\binom{m}{5}+\cdots+\binom{m}{m}, \tag{5}$$

if m is odd. Also, we have

$$\begin{aligned}\sum_{k=1}^{\frac{n-1}{2}}\sum_{j=1}^{n-2k+1} a_j\binom{n-j}{2k-1} &= \left(\binom{n-1}{1}+\binom{n-1}{3}+\cdots+\binom{n-1}{n-2}\right)a_1\\ &+\left(\binom{n-2}{1}+\binom{n-2}{3}+\cdots+\binom{n-2}{n-2}\right)a_2\\ &+\cdots+\binom{n-(n-2)}{1}a_{n-2}+\binom{n-(n-1)}{1}a_{n-1},\end{aligned} \tag{6}$$

while

$$\begin{aligned}\sum_{j=1}^{n-1} a_j+\sum_{l=1}^{\frac{n-1}{2}}\sum_{j=1}^{n-2l} a_j\binom{n-j}{2l} &= \left(1+\binom{n-1}{2}+\binom{n-1}{4}+\cdots+\binom{n-1}{n-1}\right)a_1\\ &+\left(1+\binom{n-2}{2}+\binom{n-2}{4}+\cdots+\binom{n-2}{n-3}\right)a_2\\ &+\cdots+a_{n-2}+a_{n-1}+\binom{n-(n-2)}{2}a_{n-2}.\end{aligned} \tag{7}$$

From the equations (4)–(7), we obtain (3), as desired. Therefore the identity (2) follows. ■

Now we proceed to prove Theorem 1.

Proof of Theorem 1. Let $\mathcal{P}$ denote the set of all primes. Suppose that for each a_j, the canonical prime expansion is

$$a_j=\prod_{p\,\in\,\mathcal{P}} p^{\alpha_j(p)},$$

where $\alpha_j(p)$ is a nonnegative integer for each $p\in\mathcal{P}$. Then

$$\prod_{j\neq 1} a_j=\prod_{p\,\in\,\mathcal{P}} p^{\sum\limits_{j\neq 1}\alpha_j(p)},$$

and so, by a property of gcd (for reference, see [1], [2]),

$$\gcd\left(\prod_{j\neq 1}a_j,\prod_{j\neq 2}a_j,\ldots,\prod_{j\neq k}a_j,\ldots,\prod_{j\neq n}a_j\right) = \prod_{p\,\in\,\mathcal{P}} p^{\min\left\{\sum\limits_{j\neq 1}\alpha_j(p),\sum\limits_{j\neq 2}\alpha_j(p),\ldots,\sum\limits_{j\neq n}\alpha_j(p)\right\}},$$

where $\sum_{j\neq k} \alpha_j(p) := \sum_{\substack{j=1\\ j\neq k}}^{n} \alpha_j(p),\ k \in \{1,2,\ldots,n\}$.

Similarly,

$$G_2 = \prod_{p\in\mathcal{P}} p^{\sum_{1\le i<j\le n} \{\alpha_i(p),\alpha_j(p)\}},$$

and hence

$$G_2G_4\cdots G_{n-1} = \prod_{p\in\mathcal{P}} p^{\sum_{\text{even}}},$$

where $\sum_{\text{even}}$ denotes

$$\sum_{1\le i<j\le n} \min\{\alpha_i(p),\alpha_j(p)\} + \sum_{1\le\sigma_1<\sigma_2<\sigma_3<\sigma_4\le n} \min\{\alpha_{\sigma_1}(p),\alpha_{\sigma_2}(p),\alpha_{\sigma_3}(p),\alpha_{\sigma_4}(p)\}$$
$$+\cdots+ \sum_{1\le\sigma_1<\sigma_2<\cdots<\sigma_{n-1}\le n} \min\{\alpha_{\sigma_1}(p),\ldots,\alpha_{\sigma_{n-1}}(p)\}.$$

Moreover,

$$G_3G_5\cdots G_n = \prod_{p\in\mathcal{P}} p^{\sum_{\text{odd}}},$$

where $\sum_{\text{odd}}$ denotes

$$\sum_{1\le\sigma_1<\sigma_2<\sigma_3\le n} \min\{\alpha_{\sigma_1}(p),\alpha_{\sigma_2}(p),\alpha_{\sigma_3}(p)\}$$
$$+ \sum_{1\le\sigma_1<\sigma_2<\sigma_3<\sigma_4<\sigma_5\le n} \min\{\alpha_{\sigma_1}(p),\alpha_{\sigma_2}(p),\alpha_{\sigma_3}(p),\alpha_{\sigma_4}(p),\alpha_{\sigma_5}(p)\}$$
$$+\cdots+\min\{\alpha_1(p),\ldots,\alpha_n(p)\}.$$

Since we have assumed that n is odd, the identity we are proving is equivalent to

$$\gcd\Big(\prod_{j\neq 1} a_j, \prod_{j\neq 2} a_j, \ldots, \prod_{j\neq k} a_j, \ldots, \prod_{j\neq n} a_j\Big)\cdot G(3)\cdot G(5)\cdots G(n) = G(2)\cdot G(4)\cdots G(n-1). \tag{8}$$

Clearly, we obtain

$$\gcd\Big(\prod_{j\neq 1} a_j, \prod_{j\neq 2} a_j, \ldots, \prod_{j\neq k} a_j, \ldots, \prod_{j\neq n} a_j\Big)\cdot G(3)\cdot G(5)\cdots G(n)$$
$$= \prod_{p\in\mathcal{P}} p^{\min\left\{\sum_{j\neq 1}\alpha_j(p),\sum_{j\neq 2}\alpha_j(p),\ldots,\sum_{j\neq n}\alpha_j(p)\right\}} \cdot \prod_{p\in\mathcal{P}} p^{\sum_{\text{odd}}}$$

$$= \prod_{p\in\mathcal{P}} p^{\min\left\{\sum_{j\neq 1}\alpha_j(p),\sum_{j\neq 2}\alpha_j(p),\dots,\sum_{j\neq n}\alpha_j(p)\right\}+\sum_{\text{odd}}},$$

where

$$\begin{aligned}
&\min\left\{\sum_{j\neq 1}\alpha_j(p),\sum_{j\neq 2}\alpha_j(p),\dots,\sum_{j\neq n}\alpha_j(p)\right\}+\sum_{\text{odd}}\\
&\quad=\min\left\{\sum_{j\neq 1}\alpha_j(p),\sum_{j\neq 2}\alpha_j(p),\dots,\sum_{j\neq n}\alpha_j(p)\right\}\\
&\qquad+\sum_{1\le\sigma_1<\sigma_2<\sigma_3\le n}\min\{\alpha_{\sigma_1}(p),\alpha_{\sigma_2}(p),\alpha_{\sigma_3}(p)\}\\
&\qquad+\sum_{1\le\sigma_1<\sigma_2<\sigma_3<\sigma_4<\sigma_5\le n}\min\{\alpha_{\sigma_1}(p),\alpha_{\sigma_2}(p),\alpha_{\sigma_3}(p),\alpha_{\sigma_4}(p),\alpha_{\sigma_5}(p)\}\\
&\qquad+\cdots+\min\{\alpha_1(p),\dots,\alpha_n(p)\}.
\end{aligned}$$

Now, from Lemma 1 it follows that

$$\min\left\{\sum_{j\neq 1}\alpha_j(p),\sum_{j\neq 2}\alpha_j(p),\dots,\sum_{j\neq n}\alpha_j(p)\right\}+\sum_{\text{odd}}=\sum_{\text{even}},$$

which implies that (8) holds. Hence the proof of Theorem 1 is completed. ∎

2. An application of our result

Since we can easily show that (for the case of two integers, see Theorem 1.13 in [2], and for the case of three integers, see [3])

$$\frac{|a_1\cdot a_2\cdots a_n|}{\operatorname{lcm}(a_1,a_2,\dots,a_n)}=\gcd\left(\prod_{j\neq 1}a_j,\ \prod_{j\neq 2}a_j,\ \dots,\ \prod_{j\neq k}a_j,\ \dots,\ \prod_{j\neq n}a_j\right),$$

where lcm denotes the least common multiple, by Theorem 1, the following corollary is apparent.

Corollary 1. *For all nonzero integers $a_1,\dots,a_n$, with $n\ge 3$, we have*

$$\operatorname{lcm}(a_1,a_2,\dots,a_n)=\begin{cases}\frac{G(3)\cdot G(5)\cdots G(n)}{G(2)\cdot G(4)\cdots G(n-1)}\cdot|a_1\cdot a_2\cdots a_n|, & \text{if } n \text{ is odd},\\ \frac{G(3)\cdot G(5)\cdots G(n-1)}{G(2)\cdot G(4)\cdots G(n)}\cdot|a_1\cdot a_2\cdots a_n|, & \text{if } n \text{ is even}.\end{cases}$$

Remark. Actually, for the case of three nonzero integers, we can prove Theorem 1, that is, identity (1), as follows.

$$\begin{aligned}
&(a,b)(b,c)(c,a)\\
&\quad=\big((a,b)b,(a,b)c\big)(c,a) \qquad \text{(Th1.6)}
\end{aligned}$$

$$
\begin{aligned}
&= \big((ab,b^2),(ac,bc)\big)(c,a) = (ab,b^2,ac,bc)(c,a) \qquad \text{(associativity)}\\
&= \big((ab,b^2,ac,bc)c,(ab,b^2,ac,bc)a\big) \qquad \text{(Th1.6)}\\
&= \big((abc,b^2c,ac^2,bc^2),(a^2b,ab^2,a^2c,abc)\big) \qquad \text{(Th1.6)}\\
&= (abc,b^2c,ac^2,bc^2,a^2b,ab^2,a^2c,abc) \qquad \text{(associativity)}\\
&= (abc,b^2c,bc^2,ac^2,a^2c,a^2b,ab^2,abc) \qquad \text{(commutativity)}\\
&= (abc,b^2c,bc^2,abc,ac^2,a^2c,a^2b,ab^2,abc) \qquad \text{(idempotency)}\\
&= \big((abc,b^2c,bc^2),(abc,ac^2,a^2c),(a^2b,ab^2,abc)\big) \qquad \text{(associativity)}\\
&= \big(bc(a,b,c),ac(b,c,a),ab(a,b,c)\big)\\
&= \big(bc(a,b,c),ac(a,b,c),ab(a,b,c)\big)\\
&= (a,b,c)(bc,ac,ab) = (a,b,c)(ab,bc,ca),
\end{aligned}
$$

where Th1.6 refers to the Theorem 1.6 of [2]. But for the general case, this method is inapplicable.

REFERENCES

[1] G. E. Andrews, *Number Theory*, W. B. Saunders Company, 1971.

[2] I. Niven, H. S. Zuckerman, H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th Ed., New York: John Wiley & Sons, Inc, 1991.

[3] Chengdong Pan, Chengbiao Pan, *Elementary Number Theory*, 3rd Ed. (In Chinese), Beijing: Peking University Press, 2013.

School of Mathematics and Statistics, Yunnan University, Kunming, PR. China

E-mail: `rougenuage@126.com`