K

keenonscience

GCD and LCM: the Fundamental Relationship and Its Generalization to N Numbers

Nihil sub sole novum

From the case of two numbers to canonical factorization,
up to the generalization to N naturals

A Number Theory in-depth note

written by **Nicola Maglione** – keenonscience

@keenonmaths

August 2026

Contents

Introduction 3

1 The Case of Two Numbers 3

2 Canonical Factorization: GCD and LCM via Exponents 4

3 The Generalization to N Numbers 4

4 Observations and Special Cases 5

Bibliography 6

Introduction

Given two non-zero natural numbers n and m, it is a well-known fact that their product equals the product of their least common multiple and their greatest common divisor:

$$n \cdot m = \mathrm{GCD}(n, m) \cdot \mathrm{LCM}(n, m).$$

This relationship is as elementary as it is useful: in computer science, for instance, efficient algorithms exist for computing the GCD (starting with Euclid's algorithm), and this identity lets us get the LCM "for free":

$$\mathrm{LCM}(n, m) = \frac{n \cdot m}{\mathrm{GCD}(n, m)}.$$

A natural question is whether this relationship, valid for two numbers, generalizes to a set of N natural numbers. The answer is yes, but not in the most obvious way one might imagine: naively replacing the GCD and LCM of two numbers with the GCD and LCM of N numbers does not work, as we will see with an explicit counterexample in Section 4.

The path of this note is as follows. Section 1 recalls the classical $N = 2$ case, with three numerical examples and a direct proof. Section 2 introduces a more powerful tool – canonical factorization via maximum and minimum exponents – which yields a second, purely algebraic proof of the same $N = 2$ case. Section 3 uses this tool to prove the generalization to N numbers. Section 4, finally, collects some observations: why the naive generalization fails, and why the assumption that the numbers are non-zero naturals is not merely decorative.

1. The Case of Two Numbers

Theorem 1. *Given two non-zero naturals n, m,*

$$n \cdot m = \mathrm{GCD}(n, m) \cdot \mathrm{LCM}(n, m),$$

from which the two immediate corollaries follow: $\mathrm{LCM}(n, m) = \dfrac{nm}{\mathrm{GCD}(n, m)}$ *and* $\mathrm{GCD}(n, m) = \dfrac{nm}{\mathrm{LCM}(n, m)}$.

Example 1.1. $n = 3, m = 4$ *(coprime).* $\mathrm{LCM}(3, 4) = 12$, $\mathrm{GCD}(3, 4) = 1$, *hence* $3 \cdot 4 = 12 \cdot 1$.

Example 1.2. $n = 12, m = 90$. $\mathrm{LCM}(12, 90) = 180$, $\mathrm{GCD}(12, 90) = 6$, *hence* $12 \cdot 90 = 180 \cdot 6$.

Example 1.3. $n = 24, m = 30$. *The factorizations are* $24 = 2^3 \cdot 3$ *and* $30 = 2 \cdot 3 \cdot 5$. *For the* LCM*, each prime factor is taken with its maximum exponent:* $\mathrm{LCM}(24, 30) = 2^{\max(3,1)} \cdot 3 \cdot 5 = 120$. *For the* GCD*, only the common factors are taken, with the minimum exponent:* $\mathrm{GCD}(24, 30) = 2^{\min(3,1)} \cdot 3 = 6$. *Check:* $120 \cdot 6 = 24 \cdot 30 = 720$. *This example concretely anticipates the max/min mechanism that we will formalize in Section 2.*

Proof. Let $D = \mathrm{GCD}(n, m)$ and $G = \mathrm{LCM}(n, m)$; the claim $n \cdot m = G \cdot D$ is equivalent to $G = \dfrac{nm}{D}$. We show that G, so defined, satisfies the definition of least common multiple, i.e. (a) it is a multiple of both n and m, and (b) no smaller common multiple exists.

For (a): since D divides both n and m, there exist naturals k, h with $n = kD$ and $m = hD$. Then $G = \dfrac{nm}{D} = \dfrac{kDm}{D} = km$, a multiple of m; and similarly $G = \dfrac{nm}{D} = \dfrac{nhD}{D} = hn$, a multiple of n.

For (b): suppose, for contradiction, that there exists $G' < G$ that is a common multiple of n and m, i.e. $G' = h'n = k'm$. Setting $D' = \dfrac{nm}{G'}$, one checks that D' divides both n and m (so it is a common divisor), and that $G' < G \Rightarrow D' > D$ – contradicting the maximality of D as the GCD. This contradiction proves that G is the LCM(n, m), completing the proof. ■

2. Canonical Factorization: GCD and LCM via Exponents

We now introduce the tool we will use for the generalization, presenting it already in its general form for N numbers.

Given N non-zero naturals $a_1, \ldots, a_N$, each factors uniquely into primes. Let $F = \{f_1, \ldots, f_K\}$ be the set of *all* prime factors appearing in at least one of the factorizations (shared and unshared alike). Each a_i can then be written uniquely as

$$a_i = \prod_{j=1}^{K} f_j^{e_{ij}}, \qquad i = 1, \ldots, N,$$

where some exponents e_{ij} may be zero (the factor f_j does not appear in the factorization of a_i). From this, the GCD and LCM of N numbers can be conveniently defined as

$$\mathrm{LCM}(a_1, \ldots, a_N) = \prod_{j=1}^{K} f_j^{\max_{i=1,\ldots,N}(e_{ij})}, \qquad \mathrm{GCD}(a_1, \ldots, a_N) = \prod_{j=1}^{K} f_j^{\min_{i=1,\ldots,N}(e_{ij})}.$$

Observation 2.1. If a factor f_j is not shared by all the a_i, its minimum exponent is 0: it therefore does not appear in the factorization of the GCD – exactly the textbook criterion "the GCD is computed only from the shared factors". This max/min definition is thus equivalent to the elementary one, only more convenient to manipulate algebraically, since it treats all factors uniformly rather than requiring a case-by-case distinction.

Using these definitions with $N = 2$, we can re-prove Theorem 1 in a purely algebraic way. Let $c_1, \ldots, c_k$ be the factors shared by n and m (with exponents e_{n_α} and e_{m_α}), and let $u_{n_1}, \ldots$ and $u_{m_1}, \ldots$ be the factors unique to n and to m respectively. Then

$$\mathrm{GCD}(n, m) = \prod_{\alpha=1}^{k} c_\alpha^{\min(e_{n_\alpha}, e_{m_\alpha})}, \qquad \mathrm{LCM}(n, m) = \prod_{\alpha=1}^{k} c_\alpha^{\max(e_{n_\alpha}, e_{m_\alpha})} \cdot \prod_{\beta} u_{n_\beta}^{e'_{n_\beta}} \cdot \prod_{\gamma} u_{m_\gamma}^{e'_{m_\gamma}}.$$

Alternative proof of Theorem 1. Multiplying the two expressions above and using the identity $\min(x, y) + \max(x, y) = x + y$ on each shared exponent, we directly obtain $\mathrm{LCM}(n, m) \cdot \mathrm{GCD}(n, m) = n \cdot m$ – the same result as in Section 1, now obtained by purely algebraic means. The two proofs are independent and mutually consistent. ■

3. The Generalization to N Numbers

Theorem 2. *Given N non-zero naturals $a_1, \ldots, a_N$,*

$$\prod_{i=1}^{N} a_i = \mathrm{LCM}(a_1, \ldots, a_N) \cdot \mathrm{GCD}\left(\frac{1}{a_1} \prod_{i=1}^{N} a_i,\ \ldots,\ \frac{1}{a_N} \prod_{i=1}^{N} a_i \right).$$

Observation 3.1. The GCD on the right-hand side is not the GCD of the a_i themselves, but of the N "co-products" $\frac{1}{a_m}\prod_i a_i$ – the product of all the a_i except the m-th one. For $N = 2$, $\frac{1}{a_1}(a_1a_2) = a_2$ and $\frac{1}{a_2}(a_1a_2) = a_1$: the GCD of the two co-products is simply $\mathrm{GCD}(a_1, a_2)$, and the formula reduces exactly to Theorem 1. For $N > 2$ this is no longer true, and it is precisely this difference that makes the generalization non-trivial (Section 4).

Proof. Using the definitions from Section 2, we compute the GCD on the right-hand side. The m-th co-product factors as

$$\frac{1}{a_m}\prod_{i=1}^{N} a_i = \prod_{j=1}^{K} f_j^{\sum_{i=1}^{N} e_{ij} - e_{mj}}.$$

Since the GCD selects the minimum exponent over $m = 1, \ldots, N$, and minimizing $\sum_i e_{ij} - e_{mj}$ over m is equivalent to maximizing e_{mj} (the sum $\sum_i e_{ij}$ does not depend on m), the exponent of the factor f_j in the GCD of the co-products is $\sum_{i=1}^{N} e_{ij} - \max_i(e_{ij})$. Hence

$$\mathrm{GCD}\left(\frac{1}{a_1}\prod_i a_i, \ldots, \frac{1}{a_N}\prod_i a_i\right) = \prod_{j=1}^{K} f_j^{\sum_{i=1}^{N} e_{ij} - \max_i(e_{ij})}.$$

The left-hand side of the claim is $\prod_i a_i = \prod_{j=1}^{K} f_j^{\sum_{i=1}^{N} e_{ij}}$, which is exactly the product of $\mathrm{LCM}(a_1, \ldots, a_N) = \prod_j f_j^{\max_i(e_{ij})}$ and the expression just found: an identity of exponents that is trivially verified. ■

Setting $N = 2$ in the general formula recovers $a_1a_2 = \mathrm{LCM}(a_1, a_2) \cdot \mathrm{GCD}(a_2, a_1) = \mathrm{LCM}(a_1, a_2) \cdot \mathrm{GCD}(a_1, a_2)$, i.e. exactly Theorem 1: the generalization contains the classical case as a special instance.

4. Observations and Special Cases

Counterexample 1 (why naive generalization is not enough). *Let us check that the formula* $\prod_i a_i = \mathrm{LCM}(a_1, \ldots, a_N) \cdot \mathrm{GCD}(a_1, \ldots, a_N)$ *– which naively substitutes the* GCD *of the* a_i *for the* GCD *of the co-products – is* ***false*** *in general for* $N \geq 3$*. Take* $a_1 = 4, a_2 = 6, a_3 = 9$*: we have* $\mathrm{LCM}(4, 6, 9) = 36$ *and* $\mathrm{GCD}(4, 6, 9) = 1$ *(no prime factor is shared by all three), so* $\mathrm{LCM} \cdot \mathrm{GCD} = 36$*, while* $\prod_i a_i = 4 \cdot 6 \cdot 9 = 216 \neq 36$*. The correct formula from Theorem 2, on the other hand, does work: the co-products are* $216/4 = 54$*,* $216/6 = 36$*,* $216/9 = 24$*;* $\mathrm{GCD}(54, 36, 24) = 6$*; and indeed* $\mathrm{LCM}(4, 6, 9) \cdot \mathrm{GCD}(54, 36, 24) = 36 \cdot 6 = 216 = \prod_i a_i$*.* ✓

Observation 4.1. Why is the GCD of the co-products needed instead of the GCD of the a_i? For $N = 2$, the GCD "captures" the factors shared by the two numbers. For $N \geq 3$, a factor can be shared by two of the a_i without being shared by all N: information that the "total" $\mathrm{GCD}(a_1, \ldots, a_N)$ (which requires sharing across *all* of them) loses, but which the GCD of the co-products correctly recovers, because each co-product "sees" $N - 1$ of the factors – a factor shared by $N - 1$ numbers still appears in the GCD of the co-products even if it is not shared by all N.

△ **Delicate case 1.** *The assumption "*$a_1, \ldots, a_N$ *non-zero naturals" is not decorative. If some* $a_i = 0$*, unique prime factorization is not defined, and the entire apparatus of Section 2 (exponents* e_{ij}*) collapses. With the usual conventions* $\mathrm{LCM}(0, a) = 0$ *and* $\mathrm{GCD}(0, a) = a$*, Theorem 1 still holds in the degenerate case* $n = 0$ *(*$n \cdot m = 0 = \mathrm{LCM}(0, m) \cdot \mathrm{GCD}(0, m)$*), but only thanks to the convention* $\mathrm{LCM}(0, \cdot) = 0$ *that trivializes everything; for* $N \geq 3$ *with*

several zeros or mixed combinations, the behaviour is not guaranteed to be equally clean. For this reason the note restricts itself, as stated, to strictly positive naturals.

In summary: for $N = 2$, the classical relationship lets us compute the LCM from an efficient GCD algorithm (for instance, Euclid's algorithm). For general N, the same idea works, but it requires the GCD of the co-products – not of the a_i themselves – as shown by Theorem 2 and clarified by this section's counterexample.

Bibliography

[1] G.H. Hardy, E.M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press. (The classic reference for elementary number theory; treats GCD, LCM, and unique factorization as the foundations of the whole theory.)

[2] I. Niven, H.S. Zuckerman, H.L. Montgomery, *An Introduction to the Theory of Numbers*, Wiley. (Contains exercises and extensions on the properties of GCD and LCM for more than two numbers, useful for exploring further the generalization to N numbers treated here.)

[3] T.M. Apostol, *Introduction to Analytic Number Theory*, Springer. (For readers who want to see GCD and LCM framed within the broader context of multiplicative arithmetic functions.)

keenonscience – @keenonmaths – a Number Theory in-depth note, published on keenonmaths.org.

About the author. Nicola Maglione is an electronic engineer (M.Sc. in Electronic Engineering, University of Naples, 2001), with over twenty years of experience in the semiconductor industry as a design and program manager, specializing in NAND Flash memories and high-speed interfaces, and holder of several patents in memory architectures. Alongside his professional activity, he has always cultivated a passion for mathematics – in particular Analysis, Abstract Algebra, and Number Theory – and for physics, which he shares through keenonscience, his science-outreach page, and on the site keenonmaths.org.

© 2026 Nicola Maglione. Distributed under a Creative Commons Attribution – NonCommercial – NoDerivatives 4.0 International licence (CC BY-NC-ND 4.0): sharing is permitted with attribution to the source; commercial use and derivative works are not permitted.
creativecommons.org/licenses/by-nc-nd/4.0