The least common multiple of several numbers in terms of greatest common divisors

Antonella Perucca

Abstract

We show a general formula expressing the least common multiple of several positive integers in terms of various greatest common divisors. This generalizes the well-known formula which states that the least common multiple of two positive integers equals their product divided by their greatest common divisor. The proof is based on the inclusion-exclusion principle for multisets, which is also proved in this note.

Formulas for the least common multiple

Consider two positive integers a and b: it is well-known that we can express their least common multiple through their greatest common divisor as follows:

$$\operatorname{lcm}(a,b) = \frac{a \cdot b}{\gcd(a,b)}\,.$$

For three positive integers a, b, c we have a similar formula:

$$\operatorname{lcm}(a,b,c) = \frac{a \cdot b \cdot c \cdot \gcd(a,b,c)}{\gcd(a,b) \cdot \gcd(a,c) \cdot \gcd(b,c)}\,.$$

For n positive integers $a_1, \dots, a_n$ we have a general formula for their least common multiple expressed through various greatest common divisors. To ease notation we define the $\gcd$ of a single positive integer to be the number itself and the $\gcd$ of an empty set of numbers as 1. If I is any subset of $\{1, \dots, n\}$, we then write $\gcd(I)$ for the greatest common divisor of the elements a_i with $i \in I$. We thus have the formula

$$\operatorname{lcm}(a_1, \dots, a_n) = \prod_{I \subseteq \{1,\dots,n\}} \gcd(I)^{(-1)^{\#I}} \tag{1}$$

which can be rewritten as

$$\operatorname{lcm}(a_1, \dots, a_n) = \frac{\prod_{\substack{I \subseteq \{1,\dots,n\} \\ \#I \text{odd}}} \gcd(I)}{\prod_{\substack{I \subseteq \{1,\dots,n\} \\ \#I \text{ even}}} \gcd(I)}\,.$$

In this last formula we have a quotient with as many factors in the numerator as in the denominator because a set has as many subsets with odd cardinality as with even cardinality. Notice that we recover the two initial formulas with our new notation:

$$\operatorname{lcm}(a,b) = \frac{\gcd(a) \cdot \gcd(b)}{\gcd() \cdot \gcd(a,b)}$$

$$\operatorname{lcm}(a,b,c) = \frac{\gcd(a) \cdot \gcd(b) \cdot \gcd(c) \cdot \gcd(a,b,c)}{\gcd() \cdot \gcd(a,b) \cdot \gcd(a,c) \cdot \gcd(b,c)}$$

We prove the general formula (1) by making use of the inclusion-exclusion principle for multisets.

Inclusion-Exclusion Principle for Multisets

Multisets are like sets, but the elements can be repeated: the number of times that an element appears in a multiset is its *multiplicity* (if an element does not appear, then its multiplicity is zero). An *equality* between two multisets means that the elements are the same, and they appear with the same multiplicity. One similarly defines the *inclusion* between two multisets, where we have an inequality between the two multiplicities.
The *union* $A \cup B$ of two multisets A and B is the smallest multiset containing both A and B, and one similarly defines the *intersection* $A \cap B$. Notice that the multiplicity of an element in the union is the maximum between the two multiplicities in A and in B, and for the intersection we have the minimum instead. We also have the *sum* $A + B$ which is obtained by putting together the elements of A and of B: the multiplicity for an element in $A + B$ is the sum of the two multiplicities in A and in B. Moreover, if $B \subseteq A$ we define the *difference* $A - B$ as the multiset C such that $A = B + C$ (the multiplicities in C are the difference of the multiplicities in A and B). Notice that we can immediately generalize the operations of union, intersection, and sum to finitely many multisets.

The inclusion-exclusion principle for two multisets A, B states that we have

$$A \cup B = A + B - (A \cap B)\,.$$

For three multisets A, B, C, we have the identity

$$A \cup B \cup C = A + B + C + (A \cap B \cap C) - (A \cap B) - (A \cap C) - (B \cap C)\,.$$

Finally, the general formula of the *inclusion-exclusion principle* for $n \geqslant 2$ multisets A_1 to A_n is the identity

$$\bigcup_{i=1}^{n} A_i = \sum_{\substack{I \subseteq \{1,2,\dots,n\} \\ \#I \text{ odd}}} \bigcap_{i \in I} A_i \quad - \sum_{\substack{I \subseteq \{1,2,\dots,n\} \\ \#I \text{ even}, I \neq \emptyset}} \bigcap_{i \in I} A_i\,. \tag{2}$$

To prove the inclusion-exclusion principle it suffices to show that the multiplicity for an element in $\bigcup_{i=1}^{n} A_i$ is the same as its multiplicity in the multiset on the right-hand side of (2). Writing m_i for the multiplicity of the element in A_i we have to show that

$$\max_{i \in \{1,\dots,n\}} m_i = \sum_{\substack{I \subseteq \{1,2,\dots,n\} \\ \#I \text{ odd}}} \min_{i \in I} m_i \quad - \sum_{\substack{I \subseteq \{1,2,\dots,n\} \\ \#I \text{ even}, I \neq \emptyset}} \min_{i \in I} m_i\,. \tag{3}$$

Without loss of generality suppose that m_n is the maximum of the multiplicities. Then for all sets $I \neq \{n\}$ we have $\min_{i \in I} m_i = \min_{i \in I \setminus \{n\}} m_i$. We deduce that the above formula is equivalent to

$$m_n = m_n + \sum_{\substack{I \subseteq \{1,2,\dots,n\} \\ \#I \text{ odd}, I \neq \{n\}}} \min_{i \in I \setminus \{n\}} m_i \quad - \sum_{\substack{I \subseteq \{1,2,\dots,n\} \\ \#I \text{ even}, I \neq \emptyset}} \min_{i \in I \setminus \{n\}} m_i\,. \tag{4}$$

The above equality is true because the subsets of $\{1, 2, \dots, n-1\}$ with odd (respectively, even) cardinality correspond to the subsets of $\{1, 2, \dots, n\}$ of even (respectively, odd) cardinality containing n and hence the two sums cancel out.

Proof of the formula for the least common multiple

The fundamental theorem of arithmetic states that every positive integer is a product of prime numbers, and this in a unique way up to rearranging the prime factors (prime numbers are considered to be products with just one factor, and the number 1 is the empty product). To any positive integer we may then associate the multiset of its prime factors, and we have a very elegant correspondence between the positive integers and the finite multisets of prime numbers.

Several arithmetic notions related to divisibility translate to basic notions for multisets, because the divisibility between two positive integers corresponds to an inclusion between their multisets of prime factors. We deduce that the least common multiple corresponds to the union of the multisets of prime factors, while the greatest common divisor corresponds to the intersection of the multisets of prime factors. Moreover, the product of positive integers corresponds to the sum of the multisets of prime factors, and a quotient (between a multiple and a divisor) corresponds to the difference of the multisets of prime factors.

With this correspondence, the formula in (1) immediately translates to the identity in (2), which we have proven. One detail: notice that $\prod_{I\subseteq\{1,\dots,n\},\#I \text{ even}} \gcd(I)$ is a divisor of $\prod_{I\subseteq\{1,\dots,n\},\#I \text{ odd}} \gcd(I)$ because, as it is clear from the inclusion-exclusion principle for multisets, we have the inclusion

$$\sum_{\substack{I\subseteq\{1,2,\dots,n\}\\ \#I \text{ even},\, I\neq\emptyset}} \bigcap_{i\in I} A_i \subseteq \sum_{\substack{I\subseteq\{1,2,\dots,n\}\\ \#I \text{ odd}}} \bigcap_{i\in I} A_i\,.$$

As a concluding remark, the formulas which we have shown imply that all which is done in terms of the least common multiple can be described through the greatest common divisor.