Commutativity of Multiplication in Euclid's Arithmetic

David Pierce

Draft of May 5, 2015

Mathematics Department
Mimar Sinan Fine Arts University
Istanbul
http://mat.msgsu.edu.tr/~dpierce/

Contents

1 Introduction

In Euclid's *Elements* [1, 2], the arithmetical books—Books VII, VIII, and IX—rely on no explicit postulates. Nonetheless, I contend that, on the basis of some plausible assumptions about numbers, Propositions 1, 2, 4, 5, 6, 12, and 15 of Book VII provide us with a valid nontrivial proof that multiplication of numbers is commutative. The proof relies on a theory of *proportion,* developed by means of the so-called Euclidean Algorithm.

The commutativity of multiplication of numbers might be taken as a plausible assumption itself, if numbers are thought of as rows of dots, as in Figure 1. However, if numbers are thought of as bounded straight lines, as in Euclid's diagrams and as in Figure 2, then the commutativity of multiplication is not obvious.

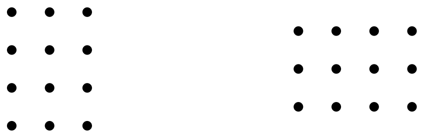

Figure 1: Multiplication of rows of dots

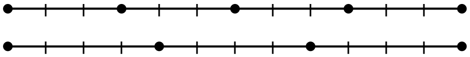

Figure 2: Multiplication of bounded straight lines

I make a more detailed analysis of Euclid's arithmetic elsewhere [6]. Here I try to cast Euclid's proof of the commutativity of multiplication in modern terms, without giving a full account of why (or to what extent) the result really *is* Euclid's proof. In one sense, the modern proof cannot be Euclid's proof, since the modern proof is written out symbolically.

In §4 below, I give a list of axioms that I think Euclid uses implicitly. There are some redundancies, as worked out in §5; but I have seen no reason to think that Euclid recognized these redundancies. Some axioms allow us to prove results that Euclid may have taken as axiomatic; see §6.

Thus the list of axioms is not entirely obvious. I have tried to be explicit about the use or at least the *first* use of an axiom in a given proof. Axioms are thus named both in the main text, and in the margin. This technique allowed me to make corrections and improvements to the list of axioms. This work of correcting and improving may turn out not to have been finished.

2 Outline of Euclid's Argument

Multiplication is defined by

$$a \cdot b = \underbrace{a + \cdots + a}_{b}.$$

If the Euclidean algorithm has the same steps for a and b that it does for c and d, this means

$$a : b :: c : d.$$

Then in particular

$$1 : a :: b : b \cdot a. \tag{1}$$

Also

$$a : b :: c : d \implies a : b :: a + c : b + d. \tag{2}$$

Therefore, in particular, since $1 : a :: 1 : a$, also

$$1 : a :: \underbrace{1 + \cdots + 1}_{b} : \underbrace{a + \cdots + a}_{b}, \tag{3}$$

that is,

$$1 : a :: b : a \cdot b,$$

and consequently, because of (1),

$$b \cdot a = a \cdot b.$$

A different proof in this style seems possible. The proof of (2) uses the distribution axiom

$$(a + b) \cdot c = a \cdot c + b \cdot c,$$

for which Euclid gives intuitive justification. The way he generalizes (2) to get (3), he might generalize the distribution axiom to get

$$(\underbrace{a + \cdots + a}_{b}) \cdot c = \underbrace{a \cdot c + \cdots + a \cdot c}_{b},$$

that is,

$$(a \cdot b) \cdot c = (a \cdot c) \cdot b.$$

Letting a be unity yields commutativity of multiplication. This second proof may seem simpler; but then we are using symbolism that Euclid does not. At this stage, he may prefer to avoid talking about products of three (or more) factors.

3 Euclid's Arithmetical Structure

In his arithmetical books, Euclid can be seen as working in a structure

$$(\mathbb{N}, 1, +, \times, <).$$

Here 1 is **unity,** or the **unit,** in the sense of Definition 1 of Book VII of the *Elements.* (However, this definition itself may be a later addition to the *Elements*; see [6, §3.1, p. 54].) Then elements of $\mathbb{N}$ are **numbers,** that is, multitudes of units in the sense of Definition

2. Thus, for Euclid, there are many units. They are all equal to one another, however: this is noted explicitly in the proof of Proposition VII.15. For Euclid, equality is not identity: for example, in an isosceles triangle, by definition two sides (and not just their "lengths") are equal. Today we do treat equality as identity: this should not cause us any problem in the present work.

The binary operation + of **addition** is undefined, though it has been used in the *Elements* since the beginning: at the head of Book I, Common Notion 2 is,

> If equals be added to equals, the wholes are equal.

We can read the expression $a+b$ in the conventional way, as a **plus** b, meaning a with the addition of b. For Euclid, this will be the same as $b+a$; it is the **sum** of a and b, or b and a. In Proposition I.35, two parallelograms on the same base and in the same parallels are equal to one another, because one of the parallelograms can be cut up into pieces that can be *added* back together in a different way to form the other parallelogram.

The binary operation × of **multiplication** is defined, after a fashion: Definition VII.15 reads (in my translation),

> A number is said to **multiply** a number when, however many units are in it, so many times is the multiplicand composed, and some number comes to be.

As usual, when in use between two numbers, our symbol × will become a dot. Suppose then

$$a \cdot b = c.$$

Let us understand this to mean that when a is the multiplicand, and b the multiplier, then c is produced. We may write the equation also as

$$\underbrace{a + \cdots + a}_{b} = c,$$

meaning c is the sum of b copies of a. In Euclid's terminology, a **measures** $a \cdot b$. Measuring is an undefined notion in the text of the

Elements as we have it; but by Definitions VII.3 and 5, there are two more ways to express it:

- a is **part** of $a \cdot b$,
- $a \cdot b$ is a **multiple** of a.

We might also say

- b **divides** $a \cdot b$ (into parts, each of which is equal to a),
- $a \cdot b$ is b **times** a (or a, b times).
- $a \cdot b$ is the **product** of a when multiplied by b.

The main point is that multiplication is initially presented in an asymmetrical way. I have chosen to write b times a as $a \cdot b$, rather than $b \cdot a$, because the former is the way that *ordinal* multiplication is conventionally written today.

In Euclid, the status of unity as a number is ambiguous. For example, by Definition VII.11,

> A **prime number** is [a number] measured only by unity;

and yet in the proof of Proposition VII.2, it is noted that a number measures itself. We may refer to the elements of $\mathbb{N}$ other than 1 as **proper** numbers.

The binary relation $<$ is of course the (undefined) notion of being **less than.** There is the converse relation $>$ of being **greater than,** which may be more common in the *Elements*: Common Notion 5 (in Heath's numbering) is

> The whole is greater than the part,

although the geometric sense of "part" meant here is not the more precise arithmetical sense given above.

I propose now that, for Euclid, the structure $(\mathbb{N}, 1, +, \times, <)$ is tacitly understood to be isomorphic to some structure

$$(\alpha \smallsetminus 1, 1, +, \times, \in),$$

where in the latter structure, $1 = \{0\}$, and $+$ and $\times$ are *ordinal* operations, and α is a nonzero ordinal that is closed under these operations. In particular, $\alpha = \omega^{\omega^{\beta}}$ for some ordinal β, as will be shown below. Then Euclid makes additional assumptions ensuring that $\beta = 0$, so $\alpha = \omega$, and, in particular, multiplication must be commutative.

4 Euclid's Implicit Axioms

Presumably Euclid is not actually thinking in terms of our ordinals. But his work suggests that he understands the following axioms to be true in the structure $(\mathbb{N}, 1, +, \times, <)$:

1. The less-than relation is a linear ordering.

2. Every non-empty subset has a least element.

3. 1 is the least element of the whole set: $1 \leqslant a$.

4. Addition is associative: $a + (b + c) = (a + b) + c$.

5. Addition makes greater: $a + b > a$.

6. Being greater is achieved by addition: if $b > a$, then the equation
$$b = a + x$$
is soluble.

7. To multiply by a sum is to add the multiples:
$$c \cdot (a + b) = c \cdot a + c \cdot b.$$

8. Multiplication by unity is identical: $x \cdot 1 = x$.

9. Division with remainder is always possible: if $b \geqslant a$, then either the equation
$$b = a \cdot x$$

is soluble, or else the system

$$b = a \cdot x + y \;\;\&\;\; a > x$$

is soluble.

10. Multiplication is associative: $c \cdot (b \cdot a) = (c \cdot b) \cdot a$.
11. Multiplication by a proper number makes greater:

$$b > 1 \implies a \cdot b > a.$$

12. The multiple of unity by a number is the number: $1 \cdot x = x$.
13. A multiple of a sum is the sum of the multiples:

$$(a + b) \cdot c = a \cdot c + b \cdot c.$$

14. Addition is commutative: $b + a = a + b$.

Axiom 13

Axiom 9

All of these axioms but number 2 belong to first-order logic. Most of the axioms would seem to be “obvious” properties of numbers. Axiom 13 is a modern interpretation of Euclid’s Proposition VII.5; this proposition then should be understood as an “intuitive” argument for why the axiom is true. Axiom 9 is used implicitly in the Euclidean Algorithm. We shall see below how the other axioms arise in Euclid’s work.

5 Modern Analysis of the Axioms

Meanwhile, let us note that the first twelve axioms are indeed true in $(\omega^{\omega^{\beta}} \smallsetminus 1, 1, +, \times, \in)$ as suggested above (see for example [4, Ch. IV]). It is a straightforward exercise to show that the converse is true as well:

Theorem 1. *If a structure $(A, 1, \oplus, \otimes, <)$ satisfies the first nine axioms above, then it is isomorphic to some structure $(\alpha \smallsetminus 1, 1, +, \times, \in)$, where $\alpha = \omega^{\omega^{\beta}}$ for some ordinal β, and $+$ and $\times$ are the ordinal operations.*

xiom 1
xiom 2

Proof. Since $(A, <)$ is a well-ordered set by Axioms 1 and 2, we may assume from the start that it is a nonempty ordinal with 0 removed, and $<$ is $\in$. Showing that $\oplus$ and $\otimes$ are then the ordinal operations means showing the following, for all α and β in A:

1. 1 is the least element of A.

2. $\alpha \oplus 1$ is the successor α' of α with respect to $<$.

3. $\alpha \oplus \beta' = (\alpha \oplus \beta)'$.

4. If β is a limit ordinal, then $\alpha \oplus \beta = \sup_{\xi<\beta}(\alpha \oplus \beta)$.

5. $\alpha \otimes 1 = \alpha$.

6. $\alpha \otimes \beta' = (\alpha \otimes \beta) \oplus \alpha$.

7. If β is a limit, then $\alpha \otimes \beta = \sup_{\xi<\beta}(\alpha \otimes \xi)$.

An important part of the argument will be showing that the operations $\xi \mapsto \alpha \oplus \xi$ and $\xi \mapsto \alpha \otimes \xi$ are strictly increasing. Details are as follows.

1. Minimality of 1 is Axiom 3. Axiom 3

2. Suppose $\alpha < \beta$ in A. By Axiom 6, for some γ in A, Axiom 6

$$\alpha \oplus \gamma = \beta,$$

and therefore, by Axioms 5 and 4, for all δ in A, Axiom 5

Axiom 4

$$\delta \oplus \alpha < (\delta \oplus \alpha) \oplus \gamma = \delta \oplus (\alpha \oplus \gamma) = \delta \oplus \beta.$$

Thus the operation

$$\xi \mapsto \delta \oplus \xi$$

on A is strictly increasing. If also $\beta < \alpha \oplus 1$, this means $\alpha \oplus \gamma < \alpha \oplus 1$, so $\gamma < 1$, which is absurd. Thus $\alpha \oplus 1$ is the successor, α', of α.

3. $\alpha \oplus \beta' = \alpha \oplus (\beta \oplus 1) = (\alpha \oplus \beta) \oplus 1 = (\alpha \oplus \beta)'$.

4. Now suppose β is a limit ordinal in A. Then $\alpha \oplus \beta$ is an upper bound of $\{\alpha \oplus \xi \colon \xi < \beta\}$. Let γ be the least upper bound. Then for some δ in A, $\alpha \oplus \delta = \gamma$. We must have $\delta \leqslant \beta$. If $\delta < \beta$, then $\delta' < \beta$, so $\alpha \oplus \delta' \leqslant \gamma = \alpha \oplus \delta < \alpha \oplus \delta'$, which is absurd. Therefore $\delta = \beta$. Thus

$$\alpha \oplus \beta = \sup_{\xi < \beta}(\alpha \oplus \xi).$$

Therefore $\oplus$ is indeed the usual ordinal addition, $+$.

Axiom 8 5. $\alpha \otimes 1 = \alpha$ by Axiom 8.

Axiom 7 6. By Axiom 7, $\alpha \otimes \beta' = \alpha \otimes (\beta + 1) = \alpha \otimes \beta + \alpha \otimes 1 = \alpha \otimes \beta + \alpha$.

7. Also, the operation

$$\xi \mapsto \delta \otimes \xi$$

is strictly increasing: for if again $\alpha < \beta$ in A, so that $\alpha + \gamma = \beta$ for some γ, then

$$\delta \otimes \alpha < \delta \otimes \alpha + \delta \otimes \gamma = \delta \otimes (\alpha + \gamma) = \delta \otimes \beta.$$

Now suppose again β is a limit ordinal in A, so $\alpha \otimes \beta$ is an upper bound of $\{\alpha \otimes \xi \colon \xi < \beta\}$. Let γ be the least upper bound. By Axiom 9, for some δ and θ, we have either $\alpha \otimes \delta = \gamma$ or $\alpha \otimes \delta + \theta = \gamma$, where $\theta < \alpha$. As before, δ must be β, and there is no θ, that is, Axiom 9

$$\alpha \otimes \beta = \sup_{\xi < \beta}(\alpha \otimes \beta).$$

Thus $\otimes$ is ordinal multiplication, $\times$.

Finally, the ordinal $A \cup 1$ has a Cantor normal form

$$\omega^{\alpha_0} \cdot b_0 + \cdots + \omega^{\alpha_n} \cdot b_n,$$

where $\alpha_0 > \cdots > \alpha_n$ and $\{b_0, \dots, b_n\} \subseteq \omega \smallsetminus 1$. If $n > 0$, then A contains $\omega^{\alpha_0} \cdot b_0$, but not its double, $\omega^{\alpha_0} \cdot b_0 + \omega^{\alpha_0} \cdot b_0$ or $\omega^{\alpha_0} \cdot (b_0 \cdot 2)$: this is absurd, since A is closed under addition. Thus $n = 0$, and we may write $A \cup 1 = \omega^{\alpha} \cdot b$. If $b > 1$, then $b = c'$ for some c in $\omega \smallsetminus 1$, and A contains $\omega^{\alpha} \cdot c$, but not its double, which again is absurd. Thus $b = 1$, and $A \cup 1 = \omega^{\alpha}$. Since A is closed under multiplication, α must be closed under addition, so as before, α must be ω^{β} for some β. □

Corollary 1. *The first nine axioms entail the next three.*

Corollary 2. *With the first nine axioms, either of Axioms 13 and 14* Axiom 13
entails Axiom 14

$$(\omega \smallsetminus 1, +, \times, \in) \cong (\mathbb{N}, 1, +, \times, <),$$

and therefore × *on* $\mathbb{N}$ *is commutative.*

Proof. In the statement of Theorem 1, if $\beta > 0$, so $\alpha > \omega$, then α contains $\omega + 1$; but

$$\begin{aligned} (\omega + 1) \cdot \omega = \omega \cdot \omega &< \omega \cdot \omega + 1 \cdot \omega, \\ 1 + \omega = \omega &< \omega + 1. \end{aligned}$$ □

Of course Euclid's argument does not proceed as above. Meanwhile, there is a more economical approach:

Theorem 2. *The first six axioms, along with Axiom 14, entail*

$$(\omega \smallsetminus 1, 1, {}', \in) \cong (\mathbb{N}, 1, x \mapsto x + 1, <).$$

Proof. Without the use of any axioms about $\mathbb{N}$ at all, there is a unique homomorphism from $(\omega \smallsetminus 1, 1, {}')$ to $(\mathbb{N}, 1, x \mapsto x + 1)$. Showing that it is an isomorphism is equivalent to establishing the so-called Peano Axioms:

1. $(\mathbb{N}, 1, x \mapsto x + 1)$ allows proof by induction.
2. The operation $x \mapsto x + 1$ on $\mathbb{N}$ is not surjective.
3. The operation $x \mapsto x + 1$ on $\mathbb{N}$ is injective.

(See for example [5, Thm 2].)

1. In $\mathbb{N}$, if $a \neq 1$, then $a > 1$ by Axiom 3, so $a = 1 + b$ for some b Axiom 3
by Axiom 6, and then $a = b + 1$ by Axiom 14, so $b < a$ by Axiom 5. Axiom 6
Therefore $(\mathbb{N}, 1, x \mapsto x + 1)$ allows proof by induction by the standard Axiom 14
argument: if $B \subseteq \mathbb{N}$, and $1 \in B$, and $a + 1 \in B$ whenever $a \in B$, then Axiom 5
the complement $\mathbb{N} \smallsetminus B$ can contain no least element, so by Axiom 2 it Axiom 2
is empty.

2. Since $1 \leqslant a < a+1$, the operation $x \mapsto x+1$ on $\mathbb{N}$ is not surjective.

3. Using also Axiom 4 as in the proof of Theorem 1, if $a < b$, then Axiom

Axiom 1 we have $a+1 = 1+a < 1+b = b+1$, and so by Axiom 1, the operation $x \mapsto x+1$ on $\mathbb{N}$ is injective.

Finally, since the ordering of $\mathbb{N}$ is determined by the addition according to the rule

$$a < b \iff \exists x\ a + x = b, \tag{4}$$

and a similar rule holds for $\omega \smallsetminus 1$, we have the desired isomorphism. □

Assuming only that the structure $(\mathbb{N}, 1, x \mapsto x+1)$ allows proof by induction, Landau shows implicitly in *Foundations of Analysis* [3] that there are unique operations $+$ and $\times$ on $\mathbb{N}$ such that

$$x + (y+1) = (x+y) + 1$$

and

$$x \cdot 1 = x, \qquad\qquad x \cdot (y+1) = x \cdot y + x. \tag{5}$$

By induction too, these operations respect the remaining of the axioms above that govern the operations alone and 1. In the same way, multiplication is commutative. Under the additional assumption that $x \mapsto x+1$ is injective, but not surjective, one shows that the relation $<$ defined by (4) satisfies the remaining axioms.

6 Euclid's Argument

We now look at Euclid's argument for the commutativity of multiplication.

Axiom 12 We can understand Axiom 12 to mean

$$b = \underbrace{1 + \cdots + 1}_{b}.$$

We can understand expressions like $1 + \cdots + 1$, and more generally

Axiom 4 $a + \cdots + a$, as being justified by Axiom 4. But we can also understand the latter expression to mean simply

$$(\cdots((a+a)+a)+\cdots+a).$$

We might take the following as being obvious for numbers, as Euclid seems to; but we *can* prove it using axioms already enumerated:

Lemma 1. *In* $\mathbb{N}$*, if* $a > b$*, then the equation*

$$a = b + x$$

has a unique *solution.*

Proof. There is a solution by Axiom 6. Any two solutions are comparable, by Axiom 1. But then there cannot be two solutions, since $x \mapsto b + x$ is strictly increasing, as in the proof of Theorem 1, which uses also Axioms 5 and 4. □

Axiom 6
Axiom 1
Axiom 5
Axiom 4

The unique solution in the theorem is the **difference** of a from b, denoted by

$$a - b.$$

Lemma 2. *In* $\mathbb{N}$*, if* $a > b$*, then*

$$c \cdot (a - b) = c \cdot a - c \cdot b.$$

Proof. We have, by Axiom 7,

$$\begin{aligned} b + (c - b) &= a, \\ c \cdot \bigl(b + (c - b)\bigr) &= c \cdot a, \\ c \cdot b + c \cdot (a - b) &= c \cdot a, \\ c \cdot (a - b) &= c \cdot a - c \cdot b. \end{aligned}$$ □

Axiom 7

The **Euclidean Algorithm** is given in **Propositions 1 and 2** of Book VII. We combine these propositions into one:

Theorem 3. *If $a_1 > a_2$, there are sequences*

$$(b_1, b_2, \dots, b_n), \qquad\qquad (a_1, a_2, \dots, a_{n+1})$$

given by

$$\begin{gathered} a_1 = a_2 \cdot b_1 + a_3 \ \ \& \ \ a_2 > a_3, \\ a_2 = a_3 \cdot b_2 + a_4 \ \ \& \ \ a_3 > a_4, \\ \dots\dots\dots\dots\dots\dots, \\ a_k = a_{k+1} \cdot b_k + a_{k+2} \ \ \& \ \ a_{k+1} > a_{k+2}, \\ \dots\dots\dots\dots\dots\dots, \\ a_n = a_{n+1} \cdot b_n. \end{gathered}$$

Thus

$$a_1 > a_2 > \dots > a_n > a_{n+1}.$$

Then, a_{n+1} is a common measure of a_1 and a_2, and a_{n+1} is measured by every common measure of a_1 and a_2. Moreover, a_{n+1} is greater than every other common measure of a_1 and a_2.

Axiom 9 Axiom 2 *Proof.* By Axiom 9, from a_k and a_{k+1}, we can obtain b_k and perhaps a_{k+2}. By Axiom 2, for some n, there is no a_{n+2}. We can now compute

$$\begin{aligned} a_{n-1} &= a_n \cdot b_{n-1} + a_{n+1} \\ &= (a_{n+1} \cdot b_n) \cdot b_{n-1} + a_{n+1} \\ &= a_{n+1} \cdot (b_n \cdot b_{n-1}) + a_{n+1} && \text{[Axiom 10]} \\ &= a_{n+1} \cdot (b_n \cdot b_{n-1}) + a_{n+1} \cdot 1 && \text{[Axiom 8]} \\ &= a_{n+1} \cdot (b_n \cdot b_{n-1} + 1). && \text{[Axiom 7]} \end{aligned}$$

Axiom 10 Axiom 8 Axiom 7 Axiom 3 Continuing in this way, we obtain a_{n+1} as a common measure of a_1 and a_2. Similarly, every common measure of a_1 and a_2 measures a_3, and a_4, and so on up to a_{n+1}. Since in general $1 \leqslant b$ by Axiom 3, we have

$$a \leqslant a \cdot b$$

Axiom 11 by Axiom 11. In particular, if a measures c, then $a \leqslant c$. □

Thus a_{n+1} as in the theorem is the **greatest common measure** of a_1 and a_2. We may write

$$a_{n+1} = \mathrm{gcm}(a_1, a_2).$$

Two numbers are **prime to one another,** as in Definition 12, if their only (and therefore their greatest) common measure is unity.

As noted earlier, **Proposition 5** of Book VII is our Axiom 13. Meanwhile, though *proportion* is mentioned in Definition 4, the real meaning is suggested by **Proposition 4:** four numbers a, b, c, and d are **proportional,** and we shall write this as Axiom 13

$$a : b :: c : d, \tag{6}$$

just in case, for some e and f,

$$\begin{aligned} a &= \mathrm{gcm}(a,b) \cdot e, & c &= \mathrm{gcm}(c,d) \cdot e,\\ b &= \mathrm{gcm}(a,b) \cdot f, & d &= \mathrm{gcm}(c,d) \cdot f. \end{aligned} \tag{7}$$

Euclid seems not to make the following two lemmas explicit. Lemma 3, like Lemma 1, might be considered as axiomatic. Lemma 4 might be taken as an obvious consequence of the axioms, although writing out a proof in modern fashion is tedious.

Lemma 3. *If $a \cdot b = a \cdot c$, then $b = c$.*

Proof. If $b \neq c$, then we may assume $b < c$, by Axiom 1. But then $a \cdot b < a \cdot c$, since $x \mapsto a \cdot x$ is strictly increasing, as in the proof of Theorem 1, which uses Axioms 6, 5, and 7. □ Axiom 1 Axiom 6 Axiom 5 Axiom 7

Lemma 4. *Under the conditions (7), e and f must be prime to one another. Conversely, if this is so, and*

$$\begin{aligned} a &= g \cdot e, & c &= h \cdot e,\\ b &= g \cdot f, & d &= h \cdot f \end{aligned} \tag{8}$$

for some g and h, then (6) holds.

Proof. Given (7) and Axiom 10, we find that $\mathrm{gcm}(a,b)\cdot\mathrm{gcm}(e,f)$ is a common measure of a and b. Then

Axiom

$$\mathrm{gcm}(a,b)\cdot\mathrm{gcm}(e,f)\leqslant\mathrm{gcm}(a,b)$$

by Theorem 3; but if $\mathrm{gcm}(e,f)>1$, then

$$\mathrm{gcm}(a,b)\cdot\mathrm{gcm}(e,f)>\mathrm{gcm}(a,b)$$

Axiom 11
Axiom 1
Axiom 3

by Axiom 11; therefore $\mathrm{gcm}(e,f)=1$ by Axioms 1 and 3.

Conversely, if (8) holds, then g is a common measure of a and b, so for some k,

$$g\cdot k=\mathrm{gcm}(a,b).$$

But for some e' and f',

$$\begin{aligned} g\cdot e=a=\mathrm{gcm}(a,b)\cdot e'=(g\cdot k)\cdot e'=g\cdot(k\cdot e'),\\ g\cdot f=b=\mathrm{gcm}(a,b)\cdot f'=(g\cdot k)\cdot f'=g\cdot(k\cdot f')\end{aligned}$$

Axiom 10

by Axiom 10, so

$$e=k\cdot e',\qquad\qquad f=k\cdot f'$$

Axiom 8

by Lemma 3, and so k is a common divisor of e and f. Suppose these are prime to one another. then $g=\mathrm{gcm}(a,b)$ by Axiom 8, and likewise $h=\mathrm{gcm}(c,d)$. We thus obtain (7), and therefore (6). □

I suppose it is just possible that Euclid overlooked the need to prove the last lemma. It seems to me more likely that he would reason as follows. If e and f are prime to one another, this means applying the Euclidean Algorithm to them yields unity. But if we replace unity with g, obtaining a and b as in (7), then the same steps of the algorithm will obviously yield g.

In any case, the lemma yields the following, which is **Proposition 12** of Book VII:

Theorem 4. *If $a : b :: c : d$, then*

$$a : b :: a + c : b + d.$$

om 13 *Proof.* Suppose (6) holds, so that (7) holds. By Axiom 13,

$$\begin{aligned} a + c &= \big(\mathrm{gcm}(a, b) + \mathrm{gcm}(c, d)\big) \cdot e, \\ b + d &= \big(\mathrm{gcm}(a, b) + \mathrm{gcm}(c, d)\big) \cdot f, \end{aligned}$$

and therefore $a : b :: a + c : b + d$ by Lemma 4. □

Euclid's **Proposition 15** is that if b measures a as many times as unity measures c, then c measures a as many times as unity measures b. Since $c = 1 \cdot c$ by Axiom 12, the conclusion is Axiom 12

$$b \cdot c = a \implies c \cdot b = a,$$

or simply the following theorem, which is Euclid's Proposition 16.

Theorem 5. *In $\mathbb{N}$, multiplication is commutative:*

$$a \cdot b = b \cdot a.$$

Proof. By Theorem 3,

$$\mathrm{gcm}(a, a \cdot b) = a.$$

Since again $1 \cdot b = b$ by Axiom 12, so that $\mathrm{gcm}(1, b) = 1$, we now have Axiom 12

$$1 : b :: a : a \cdot b. \tag{9}$$

Since

$$a = \underbrace{1 + \cdots + 1}_{a}, \qquad b \cdot a = \underbrace{b + \cdots + b}_{a},$$

repeated application of Theorem 4 yields

$$1 : b :: a : b \cdot a. \tag{10}$$

Comparison with (9) yields the desired conclusion. Such, approximately, is Euclid's argument. Strictly, the comparison of two proportions is not needed, but by definition of proportion, and Axiom 8, (10) yields

Axiom

$$a = \mathrm{gcm}(a, b \cdot a) \cdot 1 = \mathrm{gcm}(a, b \cdot a),$$
$$b \cdot a = \mathrm{gcm}(a, b \cdot a) \cdot b = a \cdot b.$$

The possibility of applying Theorem 4 repeatedly to obtain (10) might be taken as an implicit rule of inference. Today we can justify (10) by induction. First, by Axiom 12,

Axiom 12

$$1 : b :: 1 : 1 \cdot b.$$

Assuming $1 : b :: c : c \cdot b$, we have

$$1 : b :: c + 1 : c \cdot b + b;$$

and $c \cdot b + b = c \cdot b + 1 \cdot b = (c + 1) \cdot b$ by Axioms 12 and 13. In the proof of Theorem 2, we used Axioms 3, 6, 14, 5, and 2 to justify proof by induction. □

Axiom 12
Axiom 13
Axiom 3
Axiom 6
Axiom 14
Axiom 5
Axiom 2

References

[1] Euclid. *Euclidis Elementa*, volume II of *Euclidis Opera Omnia.* Teubner, Leipzig, 1884. Edited with Latin interpretation by I. L. Heiberg. Books V–IX.

[2] Euclid. *The Thirteen Books of Euclid's Elements.* Dover Publications, New York, 1956. Translated from the text of Heiberg with introduction and commentary by Thomas L. Heath. In three volumes. Republication of the second edition of 1925. First edition 1908.

[3] Edmund Landau. *Foundations of Analysis. The Arithmetic of Whole, Rational, Irrational and Complex Numbers.* Chelsea Publishing Company, New York, N.Y., third edition, 1966. Translated by F. Steinhardt; first edition 1951; first German publication, 1929.

[4] Azriel Levy. *Basic set theory*. Dover Publications Inc., Mineola, NY, 2002. Reprint of the 1979 original [Springer, Berlin].

[5] David Pierce. Induction and recursion. *The De Morgan Journal*, 2(1):99–125, 2012. `http://education.lms.ac.uk/2012/04/david-pierce-induction-and-recursion/`.

[6] David Pierce. On the foundations of arithmetic in Euclid. `http://mat.msgsu.edu.tr/~dpierce/Euclid/`, April 2015. 98 pp., size A5.