


In Defense of Euclid

The Ancient Greek
Theory of Numbers

The Poetry of Euclid

 “A **unit** is that by virtue of which each of the things that exist is called one.”

» *The Elements*, book VII, definition 1.

Our Goal:

The Fundamental Theorem of Arithmetic

- The prime factorization of every positive integer is unique, save order.
- The Unique Factorization Theorem

Numbers and Operations

Positive Integers: 2, 3, 4,... and unity as defined above.

Addition

Subtraction, the smaller from the larger

Multiplication

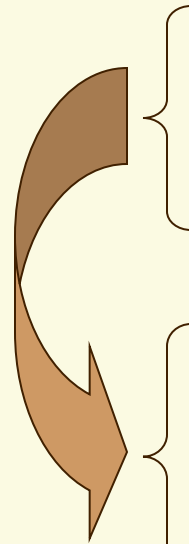


Relating Numbers

Positive integers A and B can be related as...

- A Equal to B
- A Greater Than B
- A Less Than B

Equivalent statements:




- A is measured by B
- B measures A


- B divides A
- $B|A$
- $A = k \cdot B$ for some integer k

Not Division!


No Algebraic Notation

 “If two numbers by multiplying one another make certain numbers, the numbers so produced will be equal to one another”


» Book VII, proposition 16

 $A \cdot B = B \cdot A$, the commutative property of multiplication


Generality: The Infinitude of Primes


 Euclid: “Prime numbers are more than any assigned multitude of prime numbers.”

» Book IX,
proposition 20

 Modern: There exists no greatest prime number.

Compare the Proofs

 Euclid: “Let A ,
 B , C be assigned
prime
numbers...”

 Modern: let p_1 ,
 p_2 , $p_3, \dots p_n$ be
prime...

- How are these two statements significantly different?

Is this lack of generality
damaging?

📄 Not according to Proclus:

- “This procedure is justified, since for the demonstration they use the objects set out in the diagram not as these particular figures, but as figures resembling others of the same sort”

» from *A Commentary on The First Book of Euclid's Elements* by Proclus

Generality → *Simplification*

- 📄 *The Elements* is a pedagogical text
 - a summary of elementary number theory
- 📄 loss of generality OK for simplification
 - concepts and procedures are undamaged
- 📄 Common practice in the modern classroom

Geometric Arithmetic

Integers as Line Segments

- Utilized in less than 1/4 of the propositions in book VII-IX
- Never utilized in the proof of a proposition.

Geometric Classifications of Numbers

☞ square, plane, solid, cube, etc.

☞ Pythagorean Roots

☞ Analogies by Plato's time


☞ Euclid defines the classifications in numerical terms.

☞ Square and Cubes represented linearly

Higher powers defined recursively:

$$1, A, A \cdot A, A \cdot (A \cdot A), \dots$$

An Illustrative Proof

 The Commutative Property of Multiplication:

“If two numbers by multiplying one another make certain numbers, the numbers so produced will be equal to one another”

» Book VII, proposition 16

A Sketch

Let A, B be numbers such that $A \cdot B = C$ and $B \cdot A = D$.

We must show that $C = D$

Since $A \cdot B = C$, A divides C , B times

Also, since $B \cdot A = D$, A divides D , B times

Thus C must equal D since A divides them both B times.

Q.E.D.

Is this Proof Geometric?

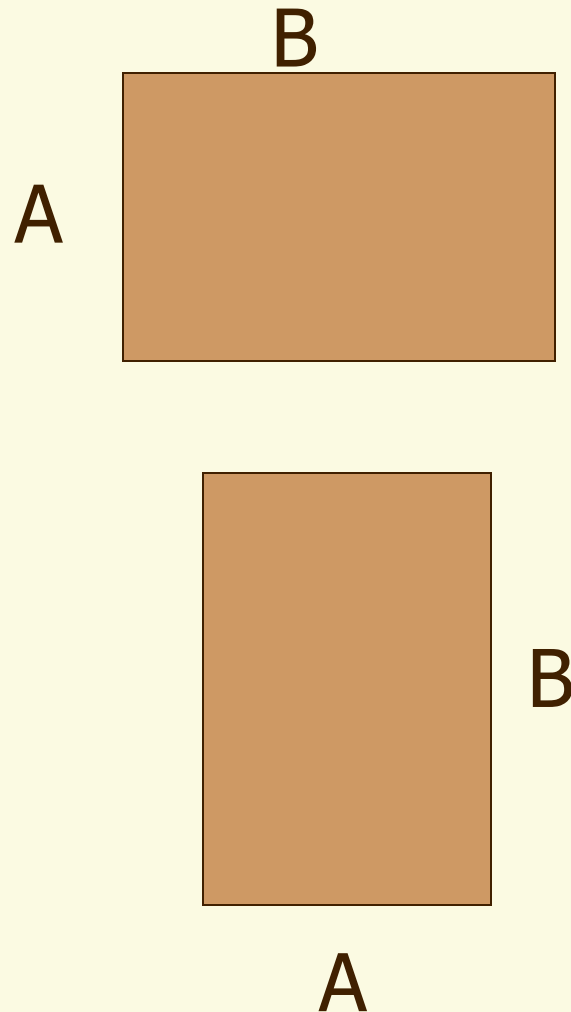
Properties of line segments?

Geometric reasoning?


- $A \cdot B = B \cdot A$
- Equivalent areas?

Arithmetic reasoning?

- Divisibility



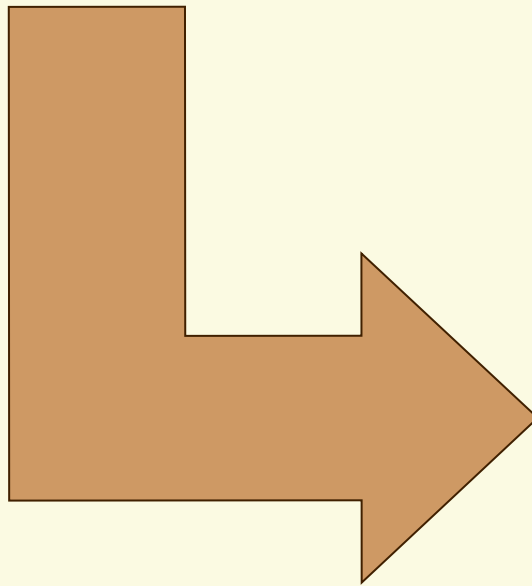
Unique Factorization

 “If a number be the least that is measured by prime numbers, it will not be measured by any other prime number except those originally measuring it.”

» The Elements, book IX,
proposition 14

Heath, 1906

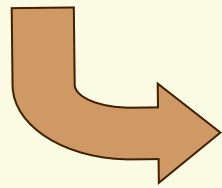
☞ "...a number can be resolved into prime factors in only one way"



☞ Claim: proposition 14 of book IX is equivalent to the FTA

Reasoning

☞ "...the least that is measured by prime numbers..."




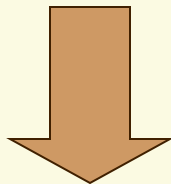
» the least common multiple of a list of primes

☞ If $\text{lcm}(a,b,c) = A$ and we find a',b',c' such that $A = \text{lcm}(a',b',c')$


☞ Then by IX;14 every element in a,b,c must equal exactly one element in a',b',c' .

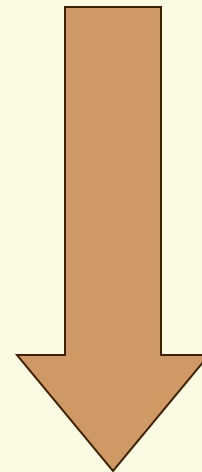
Criticism:

 Provides only for the unique prime factorization of integers with a square free factorization



TRUE

 The full proof is beyond Euclid's reach.




False


Fundamental?


 Gauss

 unique factorization


 properties of
relatively prime
numbers

 Euclid

 division algorithm

 working definition
of relatively prime

 results on primes


 unique prime
factorization

— a corollary


Fundamental?


 verifies no previous result

 late in third book of number theory


 used to prove no later propositions


The Essence of FTA


 VII;30: If two numbers by multiplying one another make some number, and any prime number measure the product, it will also measure one of the original numbers.

 XI;14: If a number be the least that is measured by prime numbers, it will not be measured by any other prime number except those originally measuring it.


A gateway theorem


 Let $N = \text{lcm}(A, B, C, \dots)$ where A, B, C, \dots are powers of distinct primes;

 let p be a prime such that $p|N$, $p^n|N$, but p^{n+1} does not divide N ;

 then p^n is exactly one element of A, B, C, \dots

The proof:


 Let $N = \text{lcm}(A, B, C, \dots)$ where A, B, C, \dots are powers of distinct primes;

 let p be a prime such that $p|N$, $p^n|N$, but p^{n+1} does not divide N


Moving along:

- Since A, B, C, \dots are powers of distinct primes, they all relatively prime to one another by (iv).
- This meets the conditions for (v) and (vi).
- By (vi), since p divides N , p divides exactly one term of the set $\{A, B, C, \dots\}$, say A .

Furthermore:

 By (ii), A is a power of p

 We must show that $A = p^n$

 If A does not equal p^n , then by (i) one must divide the other.

1) Suppose p^n divides A .

By (i), $A = p^n q$ for some $q \in \{1, p, p^2, \dots, p^{n-1}\}$.

By (iii), $p \mid q$.

Recall $A \mid N$ since $N = \text{lcm}(A, B, C, \dots)$ which implies that $p^n q \mid N$

Thus a power of p greater than or equal to $(n+1)$ divides N . This is a contradiction.

2) Suppose A divides p^n



Thus $p^n = A \cdot q$

By (iii) $p \mid q$ as before..

Now set $N = p^n M$

☞ B measures N and by (iv) is relatively prime to p^n

☞ Therefore, $B \mid M$.

☞ The same follows for C and all other elements that originally divided N (other than A).

Hence $A \cdot N$ is a common multiple of A, B, C, \dots

But if A divides p^n , then $(A \cdot M)$ divides $(p^n \cdot M)$ and $(p^n \cdot M) = N$.

This contradicts the construction of N as the least common multiple of A, B, C, \dots

Thus $p^n = A$.

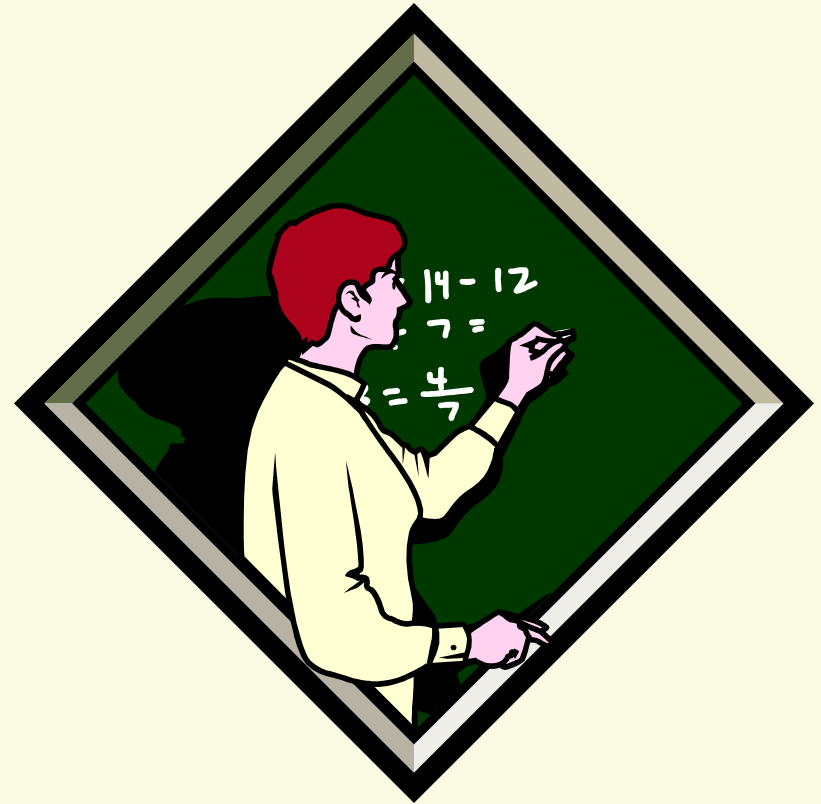
Q.E.D

The FTA follows as a corollary

- let $N = \text{lcm}(A, B, C, \dots)$ where A, B, C are powers of distinct primes
- Suppose $N = \text{lcm}(A', B', C', \dots)$ where A', B', C', \dots are powers of distinct primes.
- By the previous result, every element of A', B', C', \dots equals exactly one element of A, B, C, \dots and vice versa.
- So the two sets are identical


Can we criticize Euclid?


- ❏ Lack of generality?
- ❏ Geometric reasoning?
- ❏ A strong theory?
 - FTA



A Brief Comparison


 **Euler**

 *Elements of
Algebra*

 assumed unique
prime
factorization of
the integers.

 **Legendre**

 *Théorie des
Nombres*

 assumed unique
prime
factorization of
the integers.

A modern master

 **Gauss**

 *Disquisitiones Arithmeticae*

 adequate notation

 credited for first statement of FTA

 proves uniqueness

 assumes existence

Kudos to Euclid



- Overcame limited notation
- May not have included all possible cases
- But his proof was rigorous and complete