Did Euclid Need the Euclidean Algorithm to Prove Unique Factorization?

David Pengelley and Fred Richman

1. INTRODUCTION. The fundamental theorem of arithmetic says that every natural number is uniquely a product of primes. The heart of this uniqueness is found in Book VII of Euclid's *Elements* [**3**]:

Proposition 30 (Euclid's Lemma). *If a prime divides a product, then it divides one of the factors.*

Euclid begins Book VII by introducing the Euclidean algorithm. From his proof that the Euclidean algorithm works, he deduces an algebraic result:

Porism (Algebraic Gcd Property). *If a number divides two numbers, then it divides their greatest common divisor.*

Euclid's lemma can be derived from the algebraic gcd property, but it is not at all apparent that Euclid himself does this. We would be quite surprised if he didn't use this property because he points it out early on and because we expect him to make use of the Euclidean algorithm in some significant way. In this paper, we explore the question of just how the algebraic gcd property enters into Euclid's proof, if indeed it does.

Central to Euclid's development is the idea of four numbers being proportional: a is to b as c is to d. Euclid gives two different definitions of proportionality, one in Book VII for numbers ("Pythagorean proportionality") and one in Book V for general magnitudes ("Eudoxean proportionality"). We will discover that it is essential to keep in mind the difference between these two definitions and that many authorities, possibly including Euclid himself, have fallen into the trap of believing that Eudoxean proportionality for numbers is easily seen to be the same as Pythagorean proportionality.

Finally, we will suggest a way to make Euclid's proof good after 2300 years.

2. THE EUCLIDEAN ALGORITHM. Euclid's number theory is contained in Books VII through IX of the *Elements*. At the beginning of Book VII, he presents the Euclidean algorithm. The input to the algorithm is a pair of (positive whole) numbers a and b with $a < b$, and the algorithm consists of indefinite repetition of three steps:

$$\text{Repeat}\begin{cases} 1.\quad \text{if } a \text{ divides } b, \text{ return } a; \\ 2.\quad \text{while } a < b,\ \text{let } b = b - a; \\ 3.\quad \text{let } (a, b) = (b, a). \end{cases}$$

Step 2 is the *division algorithm*: we keep subtracting a from b until b is less than a. Alternatively, we write $b = qa + r$, where $r < a$, and then replace b with r. In step 3 we interchange the roles of a and b, because b is now the smaller of the two.

The Euclidean algorithm is supposed to return the greatest common divisor of a and b. To ensure that it does requires a proof, which Euclid supplies. His proof is essentially the first part of the following theorem, which we leave to the reader to verify.

Loop Invariants. *If $b = qa + r$, then the following statements are true:*

1. *the common divisors of a and b are exactly the common divisors of a and r;*
2. *the subgroup of the integers generated by a and b is equal to the subgroup generated by a and r.*

Applying the theorem each time we go through the loop in the algorithm, we see that the set of common divisors of a and b is a *loop invariant*: it is the same after completing the three steps as it was before. Thus, when we exit the algorithm, which happens when a divides b, we are guaranteed that the greatest common divisor is returned because, if a divides b, then a is the greatest common divisor of a and b. Euclid first proves that the output of the algorithm is a common divisor of a and b, and then, in order to prove that it is the *greatest* common divisor, he shows that any other common divisor has to divide it, so has to be smaller. This is the algebraic gcd property that Euclid notes in the porism.

The algebraic gcd property is the theoretical fact that is revealed by an analysis of the Euclidean algorithm. An efficient algorithm to compute the greatest common divisor cuts no theoretical ice. You can't prove anything interesting from it because any two numbers have a greatest common divisor simply because the set of common divisors is finite. However, the fact that any other common divisor divides the greatest common divisor is surprising and fraught with consequences. It is only through the porism that the Euclidean algorithm can play a real role in Euclid's number theory.

In light of the porism, we can replace the notion of the *greatest* common divisor by a purely algebraic one: an *algebraic gcd* of two numbers is a common divisor that is divisible by any other common divisor. There is no reason to believe a priori that any two numbers have an algebraic gcd, but this is exactly what the porism tells us.

Part 2 of the theorem tells us that the subgroup generated by a and b is a loop invariant. At the end, when a is equal to the greatest common divisor of the original a and b, it says that $\gcd(a, b)$ is in the subgroup generated by a and b, that is, we can write

$$\gcd(a, b) = sa + tb$$

for some integers s and t. This is known as *Bezout's equation*. From Bezout's equation it is easy to prove Euclid's porism that any common divisor of a and b must divide $\gcd(a, b)$.

We often prove Euclid's lemma today using Bezout's equation. Suppose p is a prime that divides ab. If p doesn't divide a, then p and a have no nontrivial common divisor, so Bezout's equation says that there exist integers s and t such that

$$sp + ta = 1.$$

Multiplying this equation by b we get

$$spb + tab = b,$$

which shows that p divides b, since it divides ab.

Alternatively, the algebraic gcd property can be used to prove that if p does not divide a, then $\gcd(pb, ab) = b$, so p divides b. As we explore how Euclid himself proves Euclid's lemma, we will watch carefully to see if he appeals to this property.

3. LOOKING FOR A PROOF.

We now present a slightly mythologized story of a quest for a proof of Euclid's lemma. More specifically, our story starts with the question: Does Euclid have anything interesting to tell us about how to prove Euclid's lemma?

As indicated earlier, Euclid starts Book VII with a description of the Euclidean algorithm, together with a porism stating that the greatest common divisor of two numbers is divisible by any other common divisor. His proof of Euclid's lemma refers to Propositions 20 and 19.

Proposition 20. *If u and v are the smallest numbers so that $u : v = c : d$, then u divides c and v divides d.*

We shall derive Euclid's lemma from Proposition 20 in more or less the same way that Euclid did. Suppose that a prime p divides ab, say $ab = pc$. Consider the fraction

$$\frac{a}{p} = \frac{c}{b}.$$

If u and v are the smallest numbers such that $u/v = a/p$, then Proposition 20 informs us that v divides both p and b. Therefore, $v = 1$ or $v = p$ because p is prime. In the first case p divides a, in the second p divides b. Thus Proposition 20 is obviously the key proposition. How does Euclid prove it?

We follow Heath's paraphrase [**3**] of Euclid's proof of Proposition 20. Euclid shows that u divides c (and so v divides d), or as he phrases it, that u is *part* of c. This means that

$$u = \frac{c}{n}$$

for some positive integer n. He does this by ruling out the alternative, that u is not part of c, in which case we could write

$$u = m \cdot \frac{c}{n},$$

where n divides c and $m > 1$. That is, c/n is an nth part of c, and u is equal to m of those nth parts. In Proposition 4, Euclid showed how to compute such numbers m and n from u and c using the Euclidean algorithm, and Heath refers to Proposition 4 in his paraphrase.

Euclid now claims that $u : c = v : d$. This is justified by another proposition:

Proposition 13 (*Alternando*). *If $a : b = c : d$, then $a : c = b : d$.*

That's okay, for if $a/b = c/d$, then $a/c = b/d$.

Continuing the proof of Proposition 20, Euclid notes that

$$v = m \cdot \frac{d}{n}.$$

His phrase for this is "v is the same parts of d that u is of c," that is, v is m nth parts of d just as u is m nth parts of c. Because $m > 1$, the numbers c/n and d/n are smaller than u and v. But as $c/n : c = d/n : d$, it follows that $c/n : d/n = c : d$, which contradicts the fact that u and v were the smallest numbers with that property. So u must divide c.

There is a serious problem with this reasoning. We know that n divides c, because that's how we chose n, but why does n divide d, that is, why is d/n a (whole) number? It's true that the Euclidean algorithm produces relatively prime numbers m and n (although Euclid does not mention this fact), and we know that $nv = md$. But to conclude from these two facts that n divides d requires more than Euclid's lemma itself, and that's what we are ultimately trying to prove! This provoked Zeuthen [**12**, pp. 155–157] to say that Euclid's proof of his lemma is worthless, because Euclid had to assume something essentially stronger than the lemma itself in order to prove Proposition 20. Thus instead of finding an alternative proof of the fundamental theorem of arithmetic, we've found a mistake in Euclid!

Wait a minute. This is *Euclid* we're talking about, the author of the most famous mathematics text of all time, not some undergraduate taking an introduction to number theory. While he is surely not immune to making mistakes, this one seems rather outlandish. Maybe if we dig a little deeper we'll find out that he sees things more clearly than we do. Let's go back and check on what he's doing, starting with the definition of $a : b = c : d$.

In our analysis thus far, we took $a : b = c : d$ to mean $a/b = c/d$, the usual *equality of fractions*: $ad = bc$. That was pretty naive. Everybody else, including Zeuthen, realizes that Euclid had two very different notions of proportion, one in Book V that dealt with arbitrary magnitudes and one in Book VII that dealt with numbers. The one in Book V is the celebrated Greek theory of proportions that was developed to handle incommensurable magnitudes. This theory, which has similarities with the modern theory of real numbers, is usually associated with Eudoxus. The one in Book VII deals with numbers, which are commensurable magnitudes—in fact, they are all multiples of a fixed unit magnitude. It has often been suggested that the theory in Book VII is an earlier one, perhaps due to the Pythagoreans.

Euclid certainly doesn't mean $ad = bc$ when he writes "a is to b as c is to d" in Book VII. He defined what we shall call *Pythagorean proportionality*, to distinguish it from the *Eudoxean proportionality* of Book V. We use the adjective "Pythagorean" to indicate that this proportionality deals with whole numbers only. Here is Euclid's definition in modern form.

Definition 20 (Pythagorean Proportionality). *We say that $a : b = c : d$ if there exist x, y, m, and n such that*

$$\begin{aligned} a &= mx, & b &= nx, \\ c &= my, & d &= ny. \end{aligned}$$

Notice that this can be thought of as saying that the fractions a/b and c/d have a common cancellation, namely, m/n. Clearly this implies that $ad = bc$ (equality of fractions). The converse, although it is true for natural numbers, is much deeper and fails in other multiplicative settings where unique factorization into primes does not obtain (see Examples 1 and 2). Observe also that Pythagorean proportionality simply says that a is m nth parts of b and that c is the same parts of d. This is pretty much how Euclid actually phrased it.

The equivalence of Pythagorean proportionality and equality of fractions is needed in Euclid's proof of his lemma. Recall how he derived the lemma from Proposition 20. He supposed that p was a prime and that $ab = pc$, so $a/p = c/b$ (equality of fractions). He then appealed to Proposition 20. But Proposition 20 is about Pythagorean proportionality, not about equality of fractions. The proposition in the *Elements* that assures that Pythagorean proportionality is the same as equality of fractions is the following:

Proposition 19. *$a : b = c : d$ if and only if $ad = bc$.*

We will return to Proposition 19 shortly, but first let's see why the proof of Proposition 20 is correct, *pace* Zeuthen. For the crucial step, we know that $u : c = v : d$, so there exist x, y, m, and n such that

$$\begin{aligned} u &= mx, & c &= nx, \\ v &= my, & d &= ny. \end{aligned}$$

This means that n divides both c and d by definition! We don't have to prove it. Moreover, $m > 1$ because we are assuming, by way of contradiction, that u does not divide c. Of course, we now have to worry whether Proposition 13 (*alternando*) is true, because it does not simply say that if $a/b = c/d$, then $a/c = b/d$. However, *alternando* is easily seen to be true by interchanging the roles of m, n and x, y in the equations of Definition 20.

Euclid didn't prove *alternando* in this way because he viewed the numbers a, b, c, d, x, and y as magnitudes, albeit all multiples of the same unit, while m and n were things that answered the question: How many? Thus the number x is a part of the number a, and m tells us how many xs it takes to make a. Objects like m and n have been referred to in the modern literature as "repetition numbers" by Fowler [**4**] and "scalars" by Bashmakova [**1**]. Fowler calls the ordinary numbers "cardinal numbers." Indeed, for a modern student it might help in understanding this distinction to think of numbers as represented by finite *sets*. When we multiply a set a by a scalar m we take the union of m disjoint copies of a. When Euclid wanted to multiply two numbers a and b, he let m be the number of units in a and set $ab = mb$.

How, then, does Euclid prove Proposition 19, that Pythagorean proportionality is equivalent to equality of fractions? Since this proposition is all we need to complete the proof of Euclid's lemma, surely we will see an appeal to the porism here, either directly or indirectly. The interesting half of the proposition is the implication from $ad = bc$ to $a : b = c : d$. Euclid's proof goes as follows. If $ad = bc$, then certainly $ac : ad = ac : bc$. On the other hand, it is immediate from the definition of Pythagorean proportionality that $ac : ad = c : d$ (take $x = ay$) and $ac : bc = a : b$. Consequently, $a : b = c : d$.

Amazing! No appeal whatsoever to the porism. Euclid has provided us with a proof of his lemma that, ironically, does not depend in an essential way on the algorithm that bears his name, even though he began Book VII with that algorithm and its algebraic consequences for the greatest common divisor. Can we believe that? It seems like magic. Where did the work get done?

Well, the symbolism we've adopted—using the equality sign in the notation for a proportion—is deceptive and may make it difficult for you to spot the flaw in Euclid's argument. Euclid himself said, "Things which equal the same thing also equal one another." Because we have internalized this axiom, it is dangerous to use an equality sign in a situation where transitivity does not obviously hold. Please accept our apologies. In fact, it is a nontrivial task to prove that Pythagorean proportionality is transitive. Try it for yourself. It's true for the positive integers, but like Euclid's lemma, it fails in more general multiplicative settings, as in the following two examples. Moreover, because equality of fractions *is* transitive, Proposition 19 also fails.

Perhaps the simplest setting where the fundamental theorem of arithmetic fails is that of our first example:

Example 1. Consider the multiplicative monoid of positive integers $1, 4, 7, 10, \ldots$ that are congruent to 1 modulo 3. In this monoid, the numbers 4, 10, and 25 are primes, and $4 \cdot 25 = 10 \cdot 10$. Pythagorean proportionality is not transitive: the reader can check that

$$4 : 10 = 4 \cdot 25 : 10 \cdot 25 = 10 \cdot 10 : 10 \cdot 25 = 10 : 25,$$

whereas $4 : 10 \neq 10 : 25$ because 4, 10, and 25 are primes. Moreover, the numbers 40 and 100 do not have an algebraic gcd. Indeed, the common divisors of 40 and 100 are exactly 4 and 10, neither of which divides the other.

Our second example is more complicated, but possibly more satisfactory because it is a system in which you can also add:

Example 2. Consider the semiring S of real numbers $a + b\sqrt{2}$ such that a and b are nonnegative integers, not both 0. Here we have

$$7(5 + 2\sqrt{2}) = (3 + 8\sqrt{2})(1 + 2\sqrt{2}),$$

and all four factors are primes. Note that S is not the ring $\mathbf{Z}[\sqrt{2}]$ of algebraic integers, where a and b are allowed to be negative and the fundamental theorem of arithmetic holds. The only invertible element in S is 1, while $1 + \sqrt{2}$ and all of its powers are invertible in $\mathbf{Z}[\sqrt{2}]$. Pythagorean proportionality fails in S for the same reason that it did in Example 1. Moreover, $7(5 + 2\sqrt{2})$ and $7(1 + 2\sqrt{2})$ do not have an algebraic gcd.

4. HOW TO FIX EUCLID'S ARGUMENT.

It's interesting that Euclid explicitly proves, in Proposition 11 of Book V, that *Eudoxean* proportionality is transitive but fails to provide a proof that *Pythagorean* proportionality is transitive, even though the proof of Proposition 19 makes essential use of this fact. Is there a simple argument we could incorporate into Book VII to show that Pythagorean proportionality is transitive as well?

Bashmakova [**1**] thought there was. She identified the unjustified use of transitivity in the proof of Proposition 19 as the problem, as opposed to Zeuthen's claim that the proof of Proposition 20 suffered from *petitio principii*. Then she suggested using the transitivity of Eudoxean proportionality to fix it. To that end she gave a straightforward proof, which does not invoke the porism, that Pythagorean proportionality implies Eudoxean proportionality. But if this approach worked, then we would still have a proof of Euclid's lemma that does not appeal to the porism. The problem is that Bashmakova did not prove the converse, namely, that Eudoxean proportionality for numbers implies Pythagorean proportionality. That's the part she really needed to address. Indeed, it's easy to prove, without using the porism, that Eudoxean proportionality for numbers is equivalent to equality of fractions, so Proposition 19 can be viewed as saying that Eudoxean and Pythagorean proportionality are equivalent. From this perspective, Euclid's error in the proof of Proposition 19 occurs when he is proving that Eudoxean proportionality implies Pythagorean proportionality—the other half of the proof is fine. In short, Bashmakova's fix is no fix at all. (We discovered Bashmakova's paper from a reference in Narkiewicz [**8**].)

Heath did not comment on Euclid's unsupported use of transitivity. However, in his notes on Eudoxean proportionality [**3**, vol. 2, pp. 126–9], he gave a proof, attributed to R. Simson, that Pythagorean proportionality is the same as Eudoxean proportionality applied to whole numbers. But this proof is fatally flawed at the end, where the different definitions of *part* in Books V and VII are confused: in Book V a *part* of a magnitude is any submultiple of another magnitude, whereas in Book VII a *part* of a number must also be another number.

The two notions of proportionality are not so easily related, although many authors have been tempted to imagine that they are. Pythagorean proportionality is about divisibility of numbers and is tailored to studying factorization. Eudoxean proportionality, which for numbers is equivalent to equality of fractions, says nothing about factorization. That they are equivalent for numbers is essentially the content of Proposition 19.

What is the best way to fix Euclid's argument? We suggest a way that uses Euclid's porism that the greatest common divisor is an algebraic greatest common divisor, as discussed in section 2. The idea, which may also be found in [**10**, Theorem 205], is to show that if any choice of x and y establishes a Pythagorean proportion $a : b = c : d$, then the canonical choices $x = \gcd(a, b)$ and $y = \gcd(c, d)$ do. Thus transitivity holds, so the proof of Proposition 19 is fixed. Indeed, transitivity could fail only if we were forced to use a common divisor of c and d in the proportion $a : b = c : d$ that was different from the one used in the proportion $c : d = e : f$. If we can always use the greatest common divisor, then transitivity clearly holds.

The Fix. *Suppose that $a : b = c : d$. If $a = p \gcd(a, b)$ and $b = q \gcd(a, b)$, then $c = p \gcd(c, d)$ and $d = q \gcd(c, d)$.*

Proof. By definition there exist m, n, x, and y such that

$$\begin{aligned} a &= mx, \quad & b &= nx, \\ c &= my, \quad & d &= ny. \end{aligned}$$

Because x is a common divisor of a and b, and y is a common divisor of c and d, the porism says that we can find i and j such that $\gcd(a, b) = ix$ and $\gcd(c, d) = jy$. The first thing we want to do is to show that $i = j$. By symmetry it suffices to show that i divides j. Now ix divides mx, so iy divides my. Similarly, ix divides nx, so iy divides ny. Thus iy divides both $my = c$ and $ny = d$. From the porism we conclude that iy divides $\gcd(c, d) = jy$, so i divides j. Finally, $c = p(iy) = p(jy) = p \gcd(c, d)$ and $d = q(iy) = q(jy) = q \gcd(c, d)$. ■

What kind of proof of Euclid's lemma do we end up with? Let's review what we've done. Pythagorean proportionality is essentially a relation between fractions (not rational numbers), a priori stronger than the usual equivalence. It says that a/b is related to c/d if a/b and c/d have a common cancellation, namely, m/n with m and n as in Definition 20. (Of course, Euclid would never phrase it that way, because for him m and n are entities of a type different from a and b, as discussed after Proposition 19.) The porism to the Euclidean algorithm can be used to show that this relation is transitive via our fix, and transitivity is used to show that it is equivalent to equality of fractions $ad = bc$ (Proposition 19). Then, because Pythagorean proportionality is equivalent to equality of fractions, we see that if we cancel a/b as much as possible, we get the smallest fraction equivalent to a/b under equality of fractions (lowest terms). That's not clear without Proposition 19: it could have been that a and b were relatively prime, yet a/b was not in lowest terms in the sense that there were smaller numbers c and d

so that $a/b = c/d$. (In Example 1, the numbers 10 and 25 are relatively prime, but the formal fraction $10/25$ is not in lowest terms because $10/25 = 4/10$.) The equivalence of the two conditions (i) that a and b are relatively prime and (ii) that a/b is in lowest terms lies at the heart of Euclid's proof.

To establish Euclid's lemma, we assume that p is a prime that divides ab, say $ab = pc$. Then $a/p = c/b$, from which it follows that a/p and c/b have a common cancellation because equality of fractions implies Pythagorean proportionality (Proposition 19). Now either p divides a and we're done, or p does not divide a, so we can't cancel a/p because p is prime. In the latter case c/b must cancel down to a/p (Proposition 20), implying that p divides b.

5. CANONICAL PARTS. Focusing on the greatest common divisor suggests that perhaps Euclid always had canonical parts in mind when he dealt with Pythagorean proportion. (This more or less corresponds to our normally thinking of fractions as being in lowest terms.) If one required canonical parts throughout, then the transitivity needed in the proof of Proposition 19 would be trivial, scarcely worth mentioning. In fact, Zeuthen (in a later paper [**13**, pp. 395–435]) and Itard [**5**] proposed this interpretation. They believed that when Euclid showed how to construct the greatest common divisor using the Euclidean algorithm and gave its algebraic properties in the porism, he was at the same time showing how to interpret the proportion $a : b = c : d$. Indeed, in the proof of Proposition 4 near the beginning of Book VII, Euclid wrote a as m nth parts of b by using the Euclidean algorithm to construct $b/n = \gcd(a, b)$.

Why doesn't the canonical-parts interpretation of Pythagorean proportionality solve the whole problem? Bashmakova entertained such an idea but rejected it, partly because of another of Euclid's propositions in Book VII:

Proposition 6. *If $a : b = c : d$, then $a : b = (a + c) : (b + d)$.*

This proposition, which follows easily for Pythagorean proportionality using Euclid's proof, requires substantial additional argument to prove under the canonical parts interpretation. Itard [**5**] points out this problem. Although it is not apparent from our presentation, Proposition 6 is essential for Euclid's development of the proof of his lemma. The proof we gave for Proposition 13 (*alternando*) is not Euclid's, and while it works for Pythagorean proportionality, it is inadequate under the canonical parts interpretation. Euclid's quite different proof of *alternando*, which is valid under both interpretations (as are most of his propositions), relies on Proposition 6.

Moreover, *alternando* is required at a key step in the proof of Proposition 19 under the canonical parts interpretation: the step where one observes that $ac : ad = c : d$. That's clear for Pythagorean proportionality but not for canonical parts. However, $ac : c = ad : d$ is clear for canonical parts (the greatest common divisors are c and d), and *alternando* converts this statement to $ac : ad = c : d$. Euclid actually goes through *alternando* to prove Proposition 19. Thus if his proof of Proposition 6 is flawed, so ultimately is his proof of Euclid's lemma.

What is wrong with the proof of Proposition 6 under the canonical parts interpretation? Suppose that

$$\begin{aligned} a &= mx, & b &= nx, \\ c &= my, & d &= ny, \end{aligned}$$

where $x = \gcd(a, b)$ and $y = \gcd(c, d)$. Then clearly

$$\begin{aligned} a &= mx, & b &= nx, \\ a + c &= m(x + y), & b + d &= n(x + y), \end{aligned}$$

but we still have to verify that $x + y = \gcd(a + c, b + d)$. This follows from our fix, so that theorem also serves to repair Euclid's proof of his lemma under the canonical parts interpretation.

Thus the overall picture of Euclid's arguments leading to the proof of his lemma is as follows. The proof of Proposition 19 is not valid for Pythagorean proportionality, while the proof of Proposition 6 is not valid under the canonical parts interpretation. Our fix, which relies on the porism, establishes that the two interpretations are equivalent, thereby salvaging Euclid's line of reasoning under either interpretation. These two interpretations, and our fix, were spelled out by Taisbak in [**10**].

6. CONCLUSION. In an attempt to discover how Euclid proved the key lemma for the fundamental theorem of arithmetic, we ran into the question of whether Euclid used, or needed to use, the Euclidean algorithm in an essential way. As written, his proof makes no essential appeal to the algorithm. On the other hand, in his proof of Proposition 19, which asserts that Pythagorean proportionality is equivalent to equality of fractions (and thus to Eudoxean proportionality), Euclid unjustifiably assumes that Pythagorean proportionality is transitive. This gap can be filled with an argument that uses the porism to the Euclidean algorithm, and it seems reasonable that Euclid could and should have supplied such an argument. The fact that Pythagorean proportionality follows from equality of fractions has been called the *Vierzahlensatz*. This theorem is proved and elaborated upon by Surányi [**9**], who claims that it had been noted by Euler.

Transitivity of Pythagorean proportionality has been spotlighted by our investigation. Its significance is put into perspective by its connection with two other multiplicative properties: the existence of algebraic gcds and the uniqueness of prime factorization. In a cancellative commutative monoid with the divisor chain condition, these three properties are equivalent. For the natural numbers other completely different approaches to Euclid's lemma and unique factorization are available. One can use induction, or the geometric approach of Surányi [**9**].

Several modern commentators have overlooked the transitivity gap in Euclid's proof of Proposition 19, or the gap in Proposition 6 under the canonical parts alternative [**2**], [**3**], [**6**], [**7**], [**11**], [**13**]. Some have been deceived into thinking that Pythagorean proportionality is easily proved to be a special case of Eudoxean proportionality [**1**], [**3**], [**6**] without appealing to the porism to the Euclidean algorithm. In fact, Pythagorean proportionality is a priori more stringent than Eudoxean proportionality applied to numbers, as our two examples in other multiplicative settings show. For the natural numbers, Pythagorean and Eudoxean proportionality are equivalent, but establishing this fact is nontrivial.

How could Euclid have left such a large gap? When he defined Eudoxean proportionality for magnitudes, he proved that it was transitive (Proposition 11 of Book V). In Book VII he defined Pythagorean proportionality in a completely different way, but assumed without proof that it, too, was transitive. While the transitivity is not obvious, he could have obtained it from the porism with which he began Book VII. It remains extraordinarily perplexing that Euclid stated the porism, but failed to use it where he most needed it.

Finally, the common view today is that Eudoxean proportionality is a sophisticated idea that subsumed the simpler Pythagorean proportionality and made it obsolete. Our analysis indicates that, on the contrary, Pythagorean proportionality is not an immediate special case of Eudoxean proportionality. It is a priori a strictly stronger relation, especially suited for studying divisibility.

ACKNOWLEDGMENTS. We thank Guram Bezhanishivili for assistance with Russian translation, Corné Kreemer for assistance with Dutch, and the interlibrary loan staffs of our universities for much assistance with resources. We also thank Andrzej Ehrenfeucht for helpful comments.

REFERENCES

1. I. G. Bashmakova, Arithmetical books of Euclid's *Elements*, *Istor.-Mat. Issled.* **1** (1948) 296–328.
2. E. J. Dijksterhuis, *De Elementen van Euclides, Part II,* P. Noordhoff, Groningen, 1930.
3. Euclid, *The Thirteen Books of Euclid's Elements* (trans. T. L. Heath), Dover, New York, 1956.
4. D. H. Fowler, *The Mathematics of Plato's Academy*, Oxford University Press, Oxford, 1999.
5. J. Itard, *Les livres arithmétiques d'Euclide*, Hermann, Paris, 1961.
6. W. R. Knorr, *The Evolution of the Euclidean Elements*, D. Reidel, Dordrecht, Holland, 1975.
7. I. Mueller, *Philosophy of Mathematics and Deductive Structure in Euclid's Elements*, MIT Press, Cambridge, 1981.
8. W. Narkiewicz, *The Development of Prime Number Theory, from Euclid to Hardy and Littlewood*, Springer-Verlag, New York, 2000.
9. J. Surányi, Schon die alten Griechen haben das gewusst, in *Grosse Augenblicke aus der Geschichte der Mathematik,* R. Freud, ed., Akadémiai Kiadó, Budapest, and B. I. Wissenschaftsverlag, Mannheim, 1990, pp. 9–50.
10. C. M. Taisbak, *Division and Logos. A Theory of Equivalent Couples and Sets of Integers*, Odense University Press, Odense, 1971.
11. B. L. van der Waerden, Die Arithmetik der Pythagoreer. I., *Math. Annalen* **120** (1948) 127–153.
12. H. G. Zeuthen, *Geschichte der Mathematik im Altertum und Mittelalter*, A.F. Höst, Copenhagen, 1896.
13. ———, *Sur la constitution des livres arithmétiques des éléments d'Euclide et leur rapport à la question de l'irrationalité*, Oversigt over det Kongelige Danske Videnskabernes Selskabs Forhandlinger 1910, no. 5, Copenhagen; also found as Part 8 of *Notes sur l'histoire des mathématiques*, B. Lunos Kgl. hof-bogtr. (F. Dreyer), Copenhagen, 1893–1911.

DAVID PENGELLEY is a professor at New Mexico State University. In addition to ongoing research in algebraic topology, he initiated a program utilizing student projects in teaching calculus, yielding the MAA book *Student Research Projects in Calculus*. He also collaborates on adapting primary historical sources for teaching mathematics, leading to two books of annotated sources and a graduate course on the role of history in teaching mathematics. This has also led to research projects in history. He received the Award for Distinguished Teaching from the MAA Southwestern Section, loves backpacking, is active on environmental issues, and has become a fanatical badminton player.
Department of Mathematical Sciences, New Mexico State University, Las Cruces, NM 88003, USA
davidp@nmsu.edu

FRED RICHMAN received an A.B. from Princeton University and a Ph.D. from the University of Chicago under the direction of Irving Kaplansky. He taught for many years at New Mexico State University, during which time his research interests were Abelian group theory and constructive mathematics. He has worked at the Center for Communications Research in Princeton and for TCI Software in Las Cruces. He has coauthored books on constructive algebra, mathematics for liberal arts, and modern algebra. He is currently at Florida Atlantic University in Boca Raton.
Department of Mathematics, Florida Atlantic University, Boca Raton, FL 33431, USA
richman@fau.edu