How did Theaetetus prove his theorem?

Barry Mazur

November 20, 2005

Rough rough draft for the volume for Eva

Eva Brann has taught me many things, among which is the importance of cherishing something that can be called "the long conversation." This "long conversation" has a time-splicing seamlessness: it can be picked up any time, even after long absences, and its themes are as perfectly fresh, perfectly vital, perfectly young as ever, but at the same time ever more resonant, more important. I have also come to think of some of the great communal intellectual projects, mathematics for example, as a long conversation that humanity has had, is having, and will continue to have.

I feel blessed for having—for still having—some long specific conversations with Eva, supremely important to me. One of these has to do with the idea of "appreciation," that important word which characterizes many of Eva's writings, e.g. about Jane Austen, or Homer, for these are *appreciations* in the profoundest sense of that word.

Surely the art of *appreciation* is a great gift of the spirit. The ex-wife of a great contemporary mathematician once said to me, with equal measures of exasperation and dearly paid-for admiration, that her ex-spouse was somehow overcome with appreciative joy every time he proved the pythagorean theorem. This, to me, is high praise.

Others would have a different view. André Weil, in discussing the passage from "intuition to certitude" in mathematics, writes

> as the Gita teaches us, knowledge and indifference are attained at the same moment. Metaphysics has become mathematics, ready to form the material for a treatise whose icy beauty no longer has the power to move us.

Oh, but *appreciation* in its fullest sense, means continuing to get pleasure, and acknowledging that pleasure, from the things we *think* we already understand, and getting yet more pleasure facing the things we don't yet understand.

How thankful we should be—about numbers—that the first few of them, $1, 2, 3$, are so immediate to our understanding, or at least seem that way, and are so ubiquitously useful to us. Beyond these numerical companions, lies more and yet more, trailing into the bittersweet landscape of the Kantian *mathematical sublime* with its infinities and profundities. Happily, the "sweet" comes after the "bitter," in that, first, we bitterly face this infinite prospect: we try to grasp that ungraspable infinite with our finite minds. Only by so trying are we prepared for the sweet afterthought, that we, with our merely finite minds can miraculously manage to comprehend the impossibility of this infinite enterprise. Each of us emerges from this experience with our personal consolation prize: a "starry sky within," as Kant calls it.

What isn't acknowledged in the picture painted in the previous paragraph is the abundance of insights, and sheer joy, to be had en route. Why is there so much to understand about $1, 2, 3 \ldots$? Why are so many stepping stones in the path of this understanding so often joyous to the soul?

Why isn't learning about numbers, for example, like learning to use a stapler? You figure out how to work it, and then you just use it for its various purposes, paying no further attention to it than occasionally adding a supply of staples.

1 Three ancient theorems about numbers

I want to discuss three mathematical gems of number theory—sources of joy, in my opinion—all three of them magnificently formulated in ancient Greek texts that have come down to us, and each of them pointing the way to far greater depths. I said *magnificently formulated* rather than *magnificently proved* but, in fact, two out of the three are both formulated *and* proved in Euclid's *Elements.* As for the third, alluded to in the title of this article, there isn't a shred of a formulation of it, *or a proof*, in Euclid. Nor is there a trace of a proof of it anywhere in the ancient literature, but we will get to that.

The three gems are:

- Euclid's proof of the infinitude of prime numbers, as in Proposition 22 of Book IX.
- The "Euclidean algorithm," as in Propositions 1, 2, and 34 of Book VII of the *Elements.*
- Theaetetus' theorem that—when put in modern terms—says that the square root of a whole number A is rational (i.e., is a fraction or a whole number) if and only if A is a perfect square. [So, $\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{7}, \sqrt{8}, \sqrt{10}, \sqrt{11}, \sqrt{12}, \sqrt{13}, \sqrt{14}, \sqrt{15}, \sqrt{17}, \sqrt{18}, \ldots$ are irrational.]

2 Theorems that prove themselves

All three of the theorems I want to discuss are wonderfully stated in the ancient literature. But I want to make a mild reformulation of the first two, to advertise a principle that I feel sometimes helps a lot to clarify things, whenever it is applicable. I'll call it the **self-proving theorem** principle. In effect, if you can restate a theorem, without complicating it, so that its proof, or the essence of its proof, is *already contained in the statement of the theorem*, then you invariably have

- a more comprehensible theorem,
- a stronger theorem, and
- a shorter and more comprehensible proof!

The first two theorems have "self-proving" formulations. Here they are:

3 Euclid's proof of the infinitude of primes

"Infinite" is a word with a built-in *negative polarity.* It is *not* something, i.e., not finite. There is a vast ancient conversation about this, centering on the shades of intention behind the word *apeiron* meaning—variously—unbounded, unlimited, indefinite, ... all of these translations having a telltale negative prefix. All the more remarkable, then, is Dedekind's positive-sounding definition of **infinite**

set as a Hilbert hotel, so to speak; that is, as set S for which there is a one-one correspondence of S with a proper subset of itself.

Whenever we say we have proven a negative *something*, we have usually actually proven a positive *something else* that we then interpret, somehow. The see-saw aspect of Kant's antinomies in the *Critique of Pure Reason* has that quality, where you shift polarity (negative-to-positive, positive-to-negative) as you change viewpoint. But proofs, demonstrations, generally, by their very nature, "accentuate the positive."

Often, perhaps always, when we translate a positive statement to a negative one, there is information—sometimes subtle, sometimes gross—that is lost in this translation. One sees this most poignantly in some important theorems that are actually packaged as "negative results," and "limits of reason," and yet, what they are directly providing—before being recast as negative—is some extraordinary affirmation of reason. One example of this is Matjasevic's famous proof that that there is no algorithm to determine whether a polynomial equation in many variables with whole number coefficients has or doesn't have a solution in whole numbers. I've just stated it in negative terms, but what is actually proven is the richness of diophantine expression: roughly speaking, that *any* collection of whole numbers that can be algorithmically listed by a computer can also be described by diophantine means.

All this is preamble to my stating Euclid's theorem in a positive way, essentially as it is given in the *Elements*, i.e., as a self-proving theorem. It is helpful to put the theorem in an "exchange of gifts" mode; that is, a "You give me an X and I'll give you a Y" format.

> *If you give me any finite (non-empty, of course!) collection of prime numbers, I will form the number N that is 1 more than the product of all the primes in the collection, so that every prime in your collection has the property that when N is divided by it, there is a remainder of 1. There exists at least one prime number dividing this number N and any prime number dividing N is new in the sense that it is not in your initial collection.*

The proof of this is essentially contained in its statement. My number N is contrived to have the property that all the primes of your collection cannot be prime divisors of N for they each leave a remainder of 1 when one tries to divide my N by them. But, N being bigger than 1 has some prime dividing it.

For example, if you gave my the "collection" consisting only of the prime 2, the N I would form would be $2 + 1$ or $N = 3$, which is itself a "new" prime not on your list. If then, you gave me, as list 2 and 3, the N I would form is $2 \cdot 3 + 1$, or $N = 7$, again itself a "new" prime not on your list. If you gave me, as list, $2, 3$ and 7, my N would be $2 \cdot 3 \cdot 7 + 1 = 43$, and yet again it would be itself a "new" prime not on your list. If you enriched your list with this newly found prime, and give me $2, 3, 7, 43$, I would form as "my" N, the number $N = 2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1807$. Now my N is not prime—as it had been in the previous cases—for it factors $1807 = 13 \times 139$. Both factors, 13 and 139, are primes. At this point we have a bonanza, in that both of these primes, 13 and 139—as we would have known, from Euclid's proof even without looking back at our list—are "new,' i.e., not on our list.

The general consequence, then, is that *no* finite list that you could give me will exhaust the totality of all prime numbers: I have shown you a way of finding new prime numbers that are not on *any* finite list. What a mixture we have here of simplicity and depth!

4 The Euclidean Algorithm

When I talk of "number" I will mean positive whole number. A **divisor** of a number N is a number d that, as people say, *divides N evenly*, meaning that it divides N with *no remainder*; in other words, the number d is a divisor of N if, and only if, the fraction N/d is a whole number.

So, for example, 4 is a *divisor* of 12, for 12 divided by 4 is 3. But 5, for example, is not a divisor of 12: if you try to divide 12 by 5 you get a *remainder* of 2. In fact the only *divisors* of 12 are

$$1, 2, 3, 4, 6, \text{ and } 12 \text{ itself.}$$

We need only two other pieces of official vocabulary, *common divisors* and *greatest common divisor*, and they each have the meanings that you might expect: If you have a pair of numbers, a **common divisor** of them is just a number that is a divisor of each of them. For example, the common divisors of the pair 12 and 18 are $1, 2, 3,$ and 6. The **greatest common divisor** of a pair of numbers is the largest of their common divisors. So, the *greatest common divisor* of the pair 12 and 18 is 6.

This notion of *greatest common divisor* is pivotal in any dealings one has with numbers, and a major insight in Euclid's number theory—that is, his Book VII—is the recognition of the key role played by greatest common divisor, which is, nowadays, lovingly given the acronym GCD.

In our example, above, we easily worked out that the greatest common divisor of 12 and 18 is 6. But when the pair of numbers gets large, it is not immediately apparent how to compute their greatest common divisor. This is where the Euclidean Algorithm comes in. I'll state it in its splendid simplicity:

> *Suppose you are given a pair of numbers A and B with A greater than B. Any common divisor of A and B is a common divisor of B and $A - B$; and conversely, any common divisor of B and $A - B$ is a common divisor of A and B.*

That's it! In the above modest sentence you have the working innards of the single most used algorithm in the history of algorithms. Not only is it, when spiffed up the tiniest bit, a fast-working process, but it is the very model of a fast-working process; its *rate of operation* sets the standard by which the speed of other algorithms are judged. And the proof of the Euclidean Algorithm? It depends on nothing more than knowing that if a number divides divides A and B then it divides $A - B$ and B; and conversely. In a sense, the Euclidean algorithm is simply stating its own proof.

Now its *proof* may be immediate, but its *use* is astounding. The beauty is that you can run this little machine first forwards, and then backwards, and in each of these runs you will get (different) important information.

Here is a brief "Manual for Use" of this Euclidean algorithm (cast in a slightly more modern idiom than you will find in Euclid).

To get the *greatest* common divisor of any two numbers, A and B you run the algorithm forwards. I mentioned above that to get it to be speedy you should to spiff it up a bit. Here's how. If A is greater than B, instead of subtracting B only *once* from A, to arrive at two numbers, B and $A - B$, with the same GCD, well, if $A - B$ is still greater than B, you could have subtracted twice B from A, all at once, to have gotten that B and $A - 2B$ have the same GCD as A and B; in fact, you may as well subtract B as many times from A as you can, all at once, to arrive at a number, $A - nB$ that is less than or equal to B, to get that the pair of smaller numbers, B and $A - nB$, have the same GCD as your original pair. Repeated application of this "Euclidean Algorithm" will successively reduce the size of the pair of numbers whose greatest common divisor you are seeking.

This reduction of size of the numbers we are dealing with is a crucial point. *Any* process that has to do with (positive whole) numbers and such that application of the process either reduces the size of the numbers being dealt with, or else terminates, *must terminate.*

This is the case with our Euclidean algorithm, and moreover, the chain of iterated application of this algorithm *can only* no longer be repeated—indeed will terminate—when the pair of numbers (whose greatest common divisor you are reduced to finding) are *equal numbers*, for then no further

subtraction of a "B" from an "A" is permitted. At this point, however, the answer stares us in the face, for the greatest common divisor of a pair of *equal* positive whole numbers is indeed that common number.

Try it on any pair of numbers you want; say $A = 2975$ and $B = 221$.

- (*First application of the Euclidean algorithm*) We can subtract $B = 221$ thirteen times from $A = 2975$ to get that the GCD of 2975 and 221 is the same as the GCD of 221 and $2975 - 13 \times 221 = 102$. So think of 221 as our *new* "A" and 102 as our *new* "B," and to find their GCD, repeat:
- (*Second application of the Euclidean algorithm*) We can subtract $B = 102$ twice from $A = 221$ to get that the GCD of 221 and 102 is the same as the GCD of 102 and $221 - 2 \times 102 = 17$. So think of 102 as our *new* "A" and 17 as our *new* "B," and repeat again:
- (*Third application of the Euclidean algorithm*) We can subtract 17 five times from 102 to get that the GCD of 102 and 17 is the same as the GCD of 17 and $102 - 5 \times 17 = 17$. And now, we're done, for the GCD of 17 and 17 is, of course, 17.

Conclusion: The GCD of the pair $A = 2975$ and $B = 221$ is 17.

But let us not turn this little machine off yet, for the even deeper application is to be had when we run it backwards: Looking at the "second application" above, we see that our GCD, namely 17, is $221 - 2 \times 102$, which I want to think of as $1 \times 221 - 2 \times 102$; the *second application* above is telling us that 17 is a multiple of 221 minus a multiple of 102. Now looking at the "first application,' we see that 102 is $2975 - 13 \times 221$, which I want to think of as $1 \times 2975 - 13 \times 221$; similarly, the *first application* above is telling us that 102 a multiple of 2975 minus a multiple of 221. Putting these together, we get that 17, our GCD of our initial pair of numbers 2975 and 221, is expressible as a difference of multiples of these two numbers; specifically:

$$17 = 1 \times 221 - 2 \times 102 = 1 \times 221 - 2 \times (2975 - 13 \times 221) = 27 \times 221 - 2 \times 2975.$$

This, then, is what the Euclidean algorithm does for us: it computes the greatest common divisor of a pair of numbers elegantly for us, and then—when run backwards—it expresses that GCD as a difference of multiples of those two numbers. This is precious information.

To celebrate the compactness of this Euclidean algorithm, I can't restrain myself from simply reciting it again, in its entirety:

> *Suppose you are given a pair of numbers A and B with A greater than B. Any common divisor of A and B is a common divisor of B and $A - B$; and conversely, any common divisor of B and $A - B$ is a common divisor of A and B.*

5 The Euclidean algorithm, in Euclid

The account just given of Euclid's algorithm was reasonably faithful, I feel, to the spirit of Euclid's Book VII. But I did take liberties to make some shifts and changes. To appreciate the nature of Euclid's text, it pays to discuss these changes. You might wonder why when I gave a reference in Euclid to *the Euclidean algorithm,* I listed not one proposition, but rather three of them (Propositions 1,2, and 34). Why did it take Euclid three propositions, two of them coming at the beginning of Book VII and one coming at the end of the book, to express his algorithm?

First, since Euclid makes a sharp distinction between "the unit" (i.e., what we would call the *number* 1) and numbers that actually denote a plurality (i.e., numbers ≥ 2) he is drawn to provide separate but similar accounts of his algorithm depending upon whether the result it gives, as greatest

common divisor, is a unit (this is discussed in Proposition 1) or is what Euclid would consider to be a bona fide number—i.e., is 2 or greater (this is discussed in Proposition 2).

Second, in the discussion I gave in the previous section, the "Manual for Use" that was offered came immediately after the basic statement of the algorithm. This is not what happens in Euclid's Book VII. In rough terms, it is Proposition 34—only coming towards the end of the book—that tells us how to effectively use Euclid's algorithm.

That the explanation of how to make use of this marvelous algorithm ambles in so late in this little volume implies something quite curious about what occurs in the middle of Book VII, as we will see later.

Related to this, and altogether astonishing, is the strange fact that *not even a single specific numeral* makes its appearance in all of Book VII, the earliest profound treatise on numbers that we have. Much scholarly debate concerns itself with whether *diagrams* did or did not occur in early manuscripts of Euclid's volumes on geometry, and what role they played in the constructions and demonstrations in geometry. It might also be worthwhile to ponder the clear lack of numerical examples—or any specific numbers at all—in Euclid's foundational text on number theory, and to ask what this implies about the way in which the text was studied, or was meant to be studied.

6 Theaetetus

A friend, Bob Kaplan, once pointed out to me that the platonic dialogue, *The Theaetetus*, is framed in such a way that one might take its central text to be something of a legal deposition—fastidiously preserved and presented only thirty years or so after the trial of Socrates—giving evidence that Socrates had indeed *not* perverted Athenian youth. For we are given two intensely vivid portraits in the dialogue: of young Theaetetus, in focussed conversation with Socrates about the nature of knowledge; and of older Theaetetus, now an Athenian general, mortally wounded in carrying out his duties for Athens. The general refuses to take time to rest in Megara, for he was in a hurry to get home to Athens, desiring to die in his native city. The dialogue, then, is itself a testimonial to the commitment of philosophy to *long conversation* unrestricted by the time exigencies of the water-clock in Athenian law courts.

Here is the statement of young Theaetetus's theorem, as described in the dialogue (147, 148; Loeb transl.):

> THEAET. We divided all numbers into two classes. The one, the numbers which can be formed by multiplying equal factors, we represented by the shape of the square and called **square** or **equilateral** numbers.
>
> SOC. Well done!
>
> THEAET. The numbers between these, such as 3 and 5 and all numbers which cannot be formed by multiplying equal factors, but only by multiplying a greater by a less or a less by a greater, and are therefore always contained in unequal sides, we represented by the shape of the oblong rectangle and called **oblong** numbers.
>
> SOC. Very good; and what next?
>
> THEAET. All the lines which form the four sides of the equilateral or square numbers we called **lengths**, and those which form the oblong numbers we called **surds**, because *they are not commensurable with the others in length,* but only in the areas of the planes which they have the power to form. And similarly in the case of solids.

In modern language:

The Theorem of Theaetetus. The square root of any (positive whole) number that is not a perfect square (of whole numbers) is irrational. The cube root of any (whole) number that is not a perfect cube (of whole numbers) is irrational.

As I have already mentioned, there is no proof of this theorem to be found, it seems, in the extant ancient literature. What is strange, though, is that a popular delusion seems to be lurking in the *secondary literature* on this topic. Specifically, you will find—in various places— the claim that Theaetetus' theorem is proven in Proposition 9 of Book X of Euclid's *Elements*. It doesn't serve any purpose here to list the places where you find this incorrect assertion, except to say that it is incorrect, and it remains a thriving delusion since at least one important article published as late as 2005 repeats it. It is an especially strange delusion since nothing subtle is going on here. Even a cursory glance at Proposition 9 Book X will convince you that what is being demonstrated there—if you take it in a modern perspective—is an utter triviality. Proposition 9 of Book X stands, though, for an important issue in ancient thought if taken on its own terms, but it won't prove irrationality of anything for us, let alone irrationality of all the numbers that Theaetetus proves. One might imagine that Heath's commentary on this—which is perfectly clear, and says exactly what is indeed proved in Proposition 9—would dispel the misconception that Theaetetus's theorem about the irrationality of surds is contained in this proposition, but it seems that this has held on with some tenacity. I would guess that the source of this error is quite early; as early as the commentaries of Pappus, but I offer this guess timidly because that would seem to imply that poor Proposition 9 of Book X has often been cited, but far less often read with attention since the fourth century AD.

7 Pappus

Here, then, are some curious statements of Pappus[1] on the subject, that I hope some historian of mathematics will elucidate for us.

> [Theaetetus] divided all numbers into two classes, such as are the product of equal sides (i.e., factors) on the one hand, and on the other, such as are contained by a greater side (factor) and a less; and he represented the first [class] by a square figure and the second by an oblong...
>
> Euclid, on the other hand, after he examined this treatise (or theorem) carefully for some time and had determined the lines which are commensurable in length and square; those, namely, whose squares have to one-another the ratio of a square number to a square number, proved that all lines of this kind are always commensurable in length...
>
> [T]he difference between Euclid's proposition and that of Theaetetus which precedes it, has not escaped us...

Is Pappus referring to some proposition of Euclid not available to us? Is Pappus, in contrasting Euclid with Theaetetus, suggesting that Theaetetus has proven the deeper theorem, or that Euclid has? Or is the statement that "the difference between Euclid's proposition and that of Theaetetus which precedes it, has not escaped us" making no comment on the relative merits of the two results, but only that Pappus sees them as different? I know of no modern commentary on this sentence in Pappus beyond the remarks in the volume cited, which indeed refer to Proposition 9 of Book X; it is an especially confusing matter, because there are hints in loc. cit. section 11 (page 74) that Pappus believes that it is Euclid's result that is the deeper: Pappus notices there that the r and

[1] Section 10, page 73 in "The Commentary of Pappus on Book X of Euclid's Elements," Arabic text and translation by William Thomson, Harvard University Press, Cambridge Mass, 1930.

s of Euclid, being lengths can themselves be irrational (relative to some unnamed, but stipulated unit measure, of course) and Euclid's proposition covers this, whereas Theaetetus's language, which is in effect about ratios of "numbers to numbers" precludes thinking about such a situation. To a modern, however, the introduction of an irrelevant extra unit—as in what Pappus claims Euclid to do—is a red herring and not a whit more general. Pappus seems insensitive to this, but is focussed, rather, on the (important to him, of course) issue of transference, or translatability, of the notion of ratio from the context of *lengths* to that of *numbers*.

However one interprets this text, one has to admire the intensity of Pappus's convictions about the subject matter. Pappus writes that he holds ignorance of the fact that incommensurables exist to be

> a brutish and not a human state, and I am verily ashamed, not for myself only, but for all Greeks, of the opinion of those men who prefer to believe what this whole generation believes, [namely], that commensurability is necessarily a quality of all magnitudes.

8 Incommensurability of $\sqrt{2} : 1$ and the "even and the odd"

There are two well-known proofs of the irrationality of $\sqrt{2}$ that turn on the distinction of *even* and *odd*. So if the pythagoreans were—as they are reputed to have been—involved in these matters, it is fair enough that Aristotle at one place refers to the pythagoreans as (my rough paraphrase) "the folks of the even and the odd."

I will rapidly review both of these proofs; what may be worth bearing in mind is that the even/odd distinction in the first of these proofs has to do with the actual numbers involved, while in the second proof it has to do with the exponents of the factors involved.

> **(1). To prove: that the equation $\sqrt{2} = n/m$ is impossible with n and m (positive) whole numbers.**

First assume that the fraction n/m is in "lowest terms," so that either the numerator or the denominator (n or m) is odd.

Next, by squaring (both sides of) that putative equation $\sqrt{2} = n/m$, you get the equation

$$2m^2 = n^2$$

which tells us that n^2 is even; since the square of an odd number can be seen to be odd, we get that n itself is even; so m must be odd.

Now use the even-ness of n, to know that you may write n as twice a whole number; say, $n = 2k$. Then substitute $2k$ for n in the displayed equation, to get:

$$2m^2 = (2k)^2 = 4k^2.$$

The coup de grace comes when you simplify this displayed equation by dividing by 2, and get $m^2 = 2k^2$ telling you that m^2, and hence m itself, must be even.

This is an absurdity because we know that both m and n are even, which contradicts the initial reduction of the fraction n/m to "lowest terms." The only conclusion one can make is that the initial supposition that there *is* an equation of the form $\sqrt{2} = n/m$ is wrong.

The second proof will give us the same kind of conclusion.

> **(2). To prove: that the equation $\sqrt{2} = n/m$ is impossible with n and m (positive) whole numbers.**

As in the first proof, we come to the same equation, $2m^2 = n^2$. But now we argue

- that the "number of prime factors" of the number on the right-hand side of this equation is even, for it is a perfect square, and the number of prime factors of a perfect square is even, while
- the number on the left-hand side of the equation is odd for it is the product of the prime number 2 by a perfect square.

This would be a contradiction *if* we knew also that any number can be written as a product of prime numbers *uniquely* where the only possible variation is in the order of the prime factors. We would even get our contradiction if we only knew that you cannot write a given number as a product of an even number of prime factors, and also as a product of an odd number of prime factors. But, we have to know *something* along those lines.

That initial *if* is a big *if*. It is in fact true that any number can be uniquely written as a product of prime numbers: this theorem is variously called the *unique factorization theorem*, or the *fundamental theorem of arithmetic*. Indeed, it is very decidedly fundamental, for much theoretical work about numbers depends critically on its truth. This *fundamental theorem of arithmetic* has a peculiar history. It is not trivial, and any of its proofs take work, and, indeed, are interesting in themselves. But it is nowhere stated in the ancient literature. It was used, implicitly, by the early modern mathematicians, Euler included, without anyone noticing that it actually required some verification, until Gauss finally realized the need for stating it explicitly, and proving it.

The relevance of proof **(2)** to our story is twofold. First, although there is no explicit proof of irrationality of $\sqrt{2}$ in Euclid proper, there is a proof of it (Proposition 117) in Book X that is close in spirit to proof **(2)**. This Proposition 117, a probable late addition, is not included in Heath's translation. Second, any of the known proofs of Theaetetus' theorem follow the general lines of proof **(2)**. Here is a modern proof.

(3). To prove (Theaetetus's Theorem): that the equation $\sqrt{d} = n/m$ is impossible with n and m (positive) whole numbers if d is a whole number not a perfect square.

As in the previous two proofs, we contemplate the putative equation

$$dm^2 = n^2,$$

and wish to show that it leads to a contradiction.

Find a prime number p dividing d with the property that the exponent e of the maximal power of the prime p that divides d is odd. This means that we are looking for a prime p such that p^e is a divisor of d but p^{e+1} is not, and e is an odd number. So, if d were, say, 250, we could take p to be 5, because 5^3 divides 250 but 5^4 does not; so the (odd number) 3 is the exponent of the maximal power of the prime 5 that divides 250. It is important to us that we can, in fact, find such a prime number (i.e., whose maximal power dividing d is odd) *exactly* when d is *not* a perfect square.

We are now going to try to compute the exponent of the maximal power of p that divides the right-hand-side of the displayed equation, and the exponent of the maximal power of p that divides the left-hand-side of the equation. As you might guess, the first of these is even, and the second is odd.

We will be able to perform our computation (of the exponent of the maximal power of p that divides each side of the displayed equation) if we knew, for example, how these "exponents of maximal powers of p dividing numbers" behave when you multiply two numbers. It seems reasonable to hope, for example, that the following rule applies:

The additive rule: *If p is a prime number, and A and B are numbers, the exponent of the maximal power of p that divides the product $A \cdot B$ is the sum of the exponent of the maximal power of p that divides A, and the exponent of the maximal power of p that divides B.*

If we use this additive rule, we can compute handily:

- If ν is the exponent of the largest power of p that divides n, then (by the additive rule) 2ν is the exponent of the maximal power of p that divides n^2, so the exponent of the maximal power of p dividing the right-hand-side of our putative equation is

  $$2\nu,$$

  which, of course, is even.

- If μ is the exponent of the largest power of p that divides m, then (by the additive rule) 2μ is the exponent of the maximal power of p that divides m^2, so the exponent of the maximal power of p dividing the left-hand-side of our putative equation, i.e., dm^2, is (by the additive rule, again)

  $$2\mu + e,$$

  which is odd, because e is odd.

To conclude our argument, we note the contradiction that we have one and the same number—the left-hand-side and the right-hand-side of an equation—such that the exponent of the maximal power of p dividing it is both *even* and *odd*. The culprit here is our initial assumption that we can find m and n (positive, whole) numbers forming an equation

$$\sqrt{d} = n/m$$

when d is a number that is not a perfect square. Such an equation is therefore impossible.

The same format will give us the addendum that Theaetetus, in the dialogue of the same name, muttered under his breath, at the end of his description of his theorem; namely, the cube root of a number is irrational if the number in question is not a perfect cube. Theaetetus could continue and prove a similar theorem for fourth roots, fifth roots, etc. if he wished to do so, and if he developed the vocabulary to discuss higher roots.

9 The engines of proofs

I wrote earlier about theorems that prove themselves; but, strictly speaking no theorem proves itself. Any demonstration that is interesting tends to have some *engine* or *engines* in it, so it can proceed. I like the mechanical analogy here: an automobile must have lots of "stuff" to render it usable, but at its heart, there is its engine, a prime moving part, that gets it actually rolling.

I grant that it may be something of a subjective judgment, but I think of it often as an exercise helpful in appreciating the flavor of a specific theorem to decide what you think its engine is.

Sometimes the engine is pretty close to the theorem itself, as with the Euclidean algorithm, where there are two engines, to my way of reckoning. The first is a basic *distributive law* telling us that if a number, d, is a divisor of two numbers, it is also a divisor of their sum and difference. The second is that we are reducing a problem about two numbers to a problem about two "smaller" numbers, and such a process must terminate after only finitely many iterations, and we bank on this general fact.

With Euclid's theorem on the infinitude of primes, there are also at least two little engines at work: the concept of "remainder after division" and the fact that any number greater than one is divisible by some prime number.

I view the *additive rule* as the crucial *engine* in the proof **(3)** that we have just sketched. The additive rule, in turn, can be reconstructed from a crucial piece of information that I will refer to by the phrase *when a prime divides a product*.

> **When a prime divides a product:** *If a prime p divides a product of two numbers, $A \cdot B$, then p divides A or it divides B.*

This then is the basic "moving part" in the demonstration of proof **(3)**. Its statement is (essentially[2] Euclid's Proposition 24 of Book VII. What is its proof?

10 When a prime divides a product of two numbers

We teach this, in some form or other, in any beginning course in number theory or algebra:

If a prime p divides $A \cdot B$ then p divides A or it divides B.

and we have our choice of various strategies for its proof. The *engine* behind its most standard proof is nothing more than the Euclidean algorithm—a tool perfectly at Euclid's disposal. Here is a sketch of this standard strategy.

If the prime p divides A we can go home, so suppose it does not. Since p is a prime number not dividing A, we can conclude that the greatest common divisor, i.e., the GCD, of the numbers p and A is 1. Now recall that by running the Euclidean algorithm backwards you can always express the GCD of two numbers as a difference between a multiple of one of the numbers and a multiple of the other. In this case, then we would be able to express 1—the GCD of p and A— as the difference between multiples of one and multiples of the other. Allow me, then, to do this by writing

$$1 = s \cdot p + r \cdot A$$

where s, r are whole numbers (but they might be negative as well as positive).

Multiply this equation by B to get

$$B = spB + rAB.$$

Now our prime number p divides the first summand on the right, spB because p itself occurs as a factor in that number. The prime p also divides the second summand rAB because, by our hypothesis, it divides AB. Therefore it divides the sum; that is, p divides B.

For proofs **(1)** and **(2)** all you would need is this displayed theorem for the prime number $p = 2$, which is of a lesser order of difficulty: it is simply saying that the product of two numbers is even only if one of those two numbers is even. This fact, which is just telling us that the product of two odd numbers is odd, can be demonstrated by express the two odd numbers as $2a - 1$ and $2b - 1$ where a and b are numbers, performing the multiplication, and noting that the product is again odd, being of the form $2(2ab - a - b) + 1$.

[2]Euclid phrases this slightly differently, but the essence, of the statement hasn't been significantly modified by our recasting of it. He formulates the property as saying that if a number is *relatively prime* to A and divides $A \cdot B$ then it divides B.

11 When a prime divides a product of two numbers, in Euclid

As I have mentioned, the statement that if a prime divides a product of two numbers it divides (at least) one of them, is essentially Euclid's Proposition 24 of Book VII.

The engine driving Euclid's demonstration of Proposition 24, however, is Proposition 20 of Book VII. Our agenda then is

- first to review the statement of Proposition 20,
- then to show how it establishes Proposition 24,
- and then to focus our attention on how to establish Proposition 20.

Proposition 20 of Book VII says (my mild paraphrase):

> *If a/b is a fraction, i.e., a ratio of two whole numbers a and b, and if c/d is a fraction such that*
>
> $$a/b = c/d,$$
>
> *and such that among all fractions equal to a/b the fraction c/d has the smallest numerator c, then c divides a (and d divides b).*

Accept this Proposition, and the essence of the proof in Euclid's Proposition 24 is easy enough to sketch:

If the prime number p divides the product AB, we write AB as a multiple of p, getting an equation of the form

$$AB = mp$$

where m is a number. Now form the ratios:

$$B/m = p/A$$

and let r be the rational number that is their common value. By Proposition 20, if c/d is the fraction equal to r where c, d are whole numbers and c is the *smallest* numerator of any fraction equal to r, then c divides all numerators of fractions equal to r. Therefore c divides p. But since p is a prime number we have only two possibilities. Either $c = 1$, which would mean that $p/A = 1/c$ giving us that p divides A, which would make us happy. Or else, $c = p$, but since, as the displayed equation shows, B is also a numerator of a fraction equal to r we would then have that $c = p$ divides B, which would also make us happy. That is, depending upon the two possibilities, $c = 1$ or $c = p$, we would have that p divides A, or B, as was to be proved.

The final item on our little agenda, then, is Proposition 20.

12 Proposition 20 of Book VII

Here, again, is the statement of that proposition.

> **Proposition 20:** *Let r be a (positive) rational number. The smallest numerator of all fractions equal to r divides the numerator of any fraction equal to r.*

Now I don't quite follow Euclid's proof of this pivotal proposition, and I worry that there may be a tinge of circularity in the brief argument given in the text. Yet, we have been amply prepared, by the previous propositions (specifically, Propositions 5 and 6) of Book VII, for a perfectly clear demonstration of the statement that is in Proposition 20, and so—with Euclid's permission— I

would like to present "a" clear argument. I hope that what I will recount does not vastly violate the tradition of Euclid's mathematical thinking. It is peculiar, though, that Euclid's commentarists, very often quite loquacious about other issues, seem to be strangely silent about Proposition 20 and its opaque proof, for it is an important piece of Euclid's number theory; even Heath, who is usually magnificently generous in his comments at problematic moments in the Euclidean text, seems not to flinch as he restates, in modern language, the step in Euclid's demonstration of Proposition 20 that is difficult for me to understand.

To prove Proposition 20, then, let a/b be the initial fraction and c/d be the fraction such that $a/b = c/d$ and such that the numerator c is the smallest numerator of any fraction equal to a/b.

Of course, if $a = c$ we are done, so c is strictly less than a. Find the largest multiple of c, $m \cdot c$, that is strictly less than a. Then we have that $a - m \cdot c$ is less than or equal to c, for if it were strictly greater than c, then next multiple in line, namely $(m+1) \cdot c$ would be strictly less than a.

For example, if a were 7 and c were 3, then twice 3, which is 6, is the largest multiple of 3 strictly less than 7; and $a - m \cdot c = 7 - 6 = 1$ is indeed strictly less than $c = 3$.

At this point we shall make use of the information in Propositions 5 and 6 of Book VII—put in modern terms they are some of the standard algebraic rules for manipulation of fractions. To paraphrase their statements:

> *If we have an equality of two fractions*
>
> $$\frac{S}{T} = \frac{U}{V}$$
>
> *with S larger that U then the fraction whose numerator is the difference of the numerators of $\frac{S}{T}$ and $\frac{U}{V}$; and whose denominator is the difference of the denominators of $\frac{S}{T}$ and $\frac{U}{V}$, is also equal to the common value of $\frac{S}{T} = \frac{U}{V}$. In symbols:*
>
> $$\frac{S}{T} = \frac{S-U}{T-V}.$$

Since

$$\frac{a}{b} = \frac{m \cdot c}{m \cdot d}$$

and a is larger than $m \cdot c$ we can conclude that the fraction whose numerator is the difference of the numerators of $\frac{a}{b}$ and $\frac{m \cdot c}{m \cdot d}$, and whose denominator is the difference of the denominators of $\frac{a}{b}$ and $\frac{m \cdot c}{m \cdot d}$, is also equal to $\frac{a}{b}$. In symbols:

$$\frac{a}{b} = \frac{a - mc}{b - md}.$$

But $a - mc$ which is now exhibited as a *numerator* of a fraction equal to $\frac{a}{b}$ is also, by construction, less than or equal to c. Since c is the smallest such numerator, we better have $a - mc = c$, or, in other words, $a = (m+1) \cdot c$, i.e., a is a multiple of c, as was to be demonstrated.

13 Making two proofs talk to each other

It is time to take stock of what we have done so far:

- We contemplated the statement of Proposition 24 of Book VII *if a prime divides a product it divides one of the factors* as an important engine.
- We gave one of the standard modern proofs of this statement. This proof makes essential use of the Euclidean algorithm, so I'll refer to it as the *Euclidean algorithm proof.*

- We reviewed the route that Euclid offers us, as a strategy for the proof of his Proposition 24; namely via his Proposition 20.
- We gave a sketch of a correct proof of Proposition 20, culling material from earlier in Book VII (specifically, Propositions 5 and 6), in hopes that we have remained within the compass of Euclid's vision of number. I'll refer to this proof as the *"smallest numerator" proof.*

Although the Euclidean algorithm is surely one of the strategies palpably available to Euclid, the very structure of his Book VII would keep Euclid from employing the *Euclidean algorithm proof.* For, Proposition 24 is comfortably in the middle of his text, and although the text begins straightaway with a *formulation* of the Euclidean algorithm (Props. 1, 2), information critical for the use of this algorithm is kept to the very end (Proposition 34).

As a result, we now have two quite different demonstrations of the statement *if a prime divides a product it divides one of the factors;* namely, via the Euclidean algorithm, and via the proposition regarding the smallest numerator, as we described above.

Whenever we have two proofs of the same thing, we have three questions in front of us:

- Are they "really" different proofs?
- Do they "really" prove the same thing?
- Is there a way of synthesizing them, forming something larger, more clarifying than either of them?

A preliminary chore sometimes needs to be done, to be able to compare the two proofs at all. Sometimes we must rephrase one, or both of them, in slightly different language, so that they are capable of "speaking to each other." This is necessary here, so let me refashion, and sharpen, the statement of the *smallest numerator proof* ever so slightly, to prepare it for its encounter with the *Euclidean algorithm proof.*

> **The Smallest Numerator Proposition, recast.** *If a positive rational number r is expressed as a fraction in two ways $r = \frac{A}{B} = \frac{C}{D}$ then it can also be expressed as a fraction $r = \frac{E}{F}$ where the numerator E is the greatest common divisor of the numerators A and C.*

The reason why the recast proposition implies the fact that the smallest numerator divides all numerators of fractions equal to a given rational number, is that (using the notation we have at our disposal) the greatest common divisor E divides A and C; now if C *were* the smallest numerator, it would be necessarily the case that $C = E$, and therefore C divides A, and A could have been taken to be *any* numerator of a fraction equal to r. This latter statement is just our old version of the "smallest numerator proposition."

The recast version of the smallest numerator proposition has a more concrete aspect than the original formulation, and no wonder: it has engaged as a resource, the mighty Euclidean algorithm, thereby moving a step closer to the *Euclidean algorithm proof.* If we were to follow this further, we would find our two proofs merging into one unified understanding of *when a prime divides a product.* But, of course, we would not, even then, be done.

14 Turning things around

Sometimes, when we have defined a concept P and then have proven, by a proposition, that P is equivalent to Q—that Q *characterizes* P—we find that we have a remarkable option open to us. We can turn the tables on the *definition* and the *proposition* by "starting over again," so to speak, and

redefining that same concept as Q, and then regarding the proposition as affirming that Q is indeed equivalent to P.

We see shades of this turn-around-strategy in other disciplines: we wish to define the almost ungraspable notion of *intelligence*, for example, and we have a sense that, whatever it is, it is—if not equivalent to, at least–somehow related to performance on a certain curious *test*. We then, it seems, formulate a definition in terms of performance on that test, refashioning the name of what we're after as *Intelligence Quotient*. We don't do this capriciously, of course: we are not, after all, hellbent on confusing ourselves. We would not, I imagine, do such a strange thing—put the responsibility of earmarking such an extraordinary concept as *intelligence* onto the shoulders of a single number—if we had a more straightforward definition—or measure—of intelligence. Perhaps we shouldn't do this, with any confidence, in any case.

The "turn-around tactic" in mathematics has quite a different flavor. There, we assume that we have a perfectly clear definition of the concept P to begin with. We only turn around and redefine the same concept as Q if doing so sheds light—a new light—on the concept that is already grasped.

One of the most striking "turn-arounds" in modern mathematics is in the very definition of prime number. The property satisfied by primes, for which we have give two proofs, namely *when a prime divides a product it divides one of the factors* is a characterization of prime numbers: A prime number *p has* this property, as we have seen. A composite number N *does not have* this property (factor N as $N = A \cdot B$ with A and B both less than N, and here we have a case where N divides, and in fact is equal to, a product, but doesn't divide either factor).

Not only is this property a characterization of prime number, but it reflects a fundamental feature of prime numbers; in fact, such an important characterizing feature of primality that there is much to be gained in our understanding if we simply turn the tables on the the way we introduce primes into our discussion, and make the following new

> **Turn-Around Definition:** *A* **prime number** *is a number that has the property that whenever it divides a product of two numbers, it divides one (or both) of the numbers*

What we have done in the preceding sections, from this vantage, is, effectively, to have shown two proofs of the fact that this table-turned definition of prime number coincides with our usual definition.

This new definition, expressed in the language of the modern notion of ideals is the gateway to the modern conception of algebra, and the profound link between geometry and algebra. But that is another story, and will only deepen our appreciation of *when a prime divides a product* as the somewhat laconically addressed glorious center of Euclid's Book VII, and as a possible engine to Theaetetus's demonstration of his theorem.

15 Reading Euclid

In a prior section we forced one aspect of Euclid—his algorithm that frames Book VII like a pair of book-ends—to talk with another aspect of Euclid—the somewhat terse middle of Book VII. It seemed to me that this glorious text deserves to have such a face-to-face internal encounter. Of course, all reading is a more external encounter between at least two subjects, reader and writer, as aided by a speechless and speechful messenger, namely the material book. Most of the time, when we refer to our reading we may quote the author at length, discuss chapters, sections, and page numbers but we rarely refer to the physical presence of the book itself, ever in front of us as we contemplate its contents.

In my case, I have a copy of Sir Thomas Heath's three volume paperback series that translates and comments on the thirteen books of *Euclid's Elements*, published by Dover in 1956, but now lacking some of their front covers. This set was originally used as school texts by my young sister-in-law Ali, Alexandra Dane Dor-Ner, when she studied Euclid at St. John's College in Santa Fe in

the mid-sixties, and the books were passed to me when she died some fifteen years ago. My copy of Book VII, is especially invigorated by Ali's marginal notes, recording her extraordinarily vivid encounter with Euclid. I'm intrigued to see that it is around Propositions 5 and 6 that Ali's pencil notes have reached a crescendo. So, when I read, the three of us are in "the room" together: Euclid, Ali, me. Her questioning of Euclid has its intense moments, and when this happens, I find that I can sit back and imagine Euclid—distracted from gazing upon beauty bare—responding.

"Unproved"– Ali writes at one point, and on reading this I'm taken, at the same time, with a sense of pride for my (then teen-age) relative, and a sense of admiration for the accomplishment of Euclid, who had instilled such a high level of scrutinizing question-asking and question-answering, that halfway through his thirteen books, a reader will have learned this so intimately so as to demand it, vigorously, of Euclid himself.

Eva Brann, in her essay "The Second Power of Questions" talks of the different kinds of *questions, problems, dilemmas* and *mysteries.* The lesser categories of problems, dilemmas and mysteries, Eva says, "belong to a type of question that calls for the answer to do away with the question." Eva pinpoints the distinction between *mysteries* and *problems*, by quoting a fourth-grader who, in *Thinking: The journal of Philosophy for Children*, says: " If I were to find myself on the moon, it'd be a mystery how I got there but it'd be a problem how to get back."

The title question of this article, for example, lives somewhere in these lesser categories. But there exist also the "true" questions, about which Eva writes:

> These are never resolved nor do they lapse, but they collect about themselves an ever-live complex of reflective results.

Eva is celebrating the type of questions that provide nourishment for long conversations, inviting anyone to enter, to think afresh, to converse. It is astounding how deftly Euclid's inquiry about numbers points us to some of these "true" questions, among the most abiding questions in mathematics.