in Pitici, Mircea (ed), The Best Writing on Mathematics 2014. Princeton: Princeton University Press, 2015.

Extreme Proofs I: The Irrationality of $\sqrt{2}$

John H. Conway and Joseph Shipman

Mathematicians often ask, "What is the best proof" of something, and indeed Erdős used to speak of "Proofs from the Book," meaning, of course, God's book. Aigner and Ziegler (1998) have attempted to reconstruct some of this Book.

Here we take a different and more tolerant approach. We shouldn't speak of "the best" proof because different people value proofs in different ways. Indeed one person's value might oppose another's. For example, a proof that quotes well-known results from Galois theory is valued negatively by someone who knows nothing of that theory but positively by the instructor in a course on Galois theory. Other "values" that have been proposed include brevity, generality, constructiveness, visuality, nonvisuality, "surprise," elementarity, and so on. A single mathematician may hold more than one of the values dear. Clearly the ordering of proofs cannot be a total order.

It is enjoyable and instructive to find proofs that are optimal with respect to one or more such value functions not only because they tend to be beautiful but also because they are more likely to point to possible generalizations and applications.

In this respect, we can discard a proof C that uses all the ideas of shorter proofs A and B because nobody should value it more highly than both A and B. We model this by putting C on the line segment AB, and it suggests that we think of proofs of a given result as lying in a convex region in some kind of space, which in our pictures will be the Euclidean plane.

Indeed, because at any given time there are only finitely many known proofs, we may think of them as lying in a polyhedron (in our pictures, a polygon), and the value functions as linear functionals, as in optimization theory, so that any value function must be maximized at

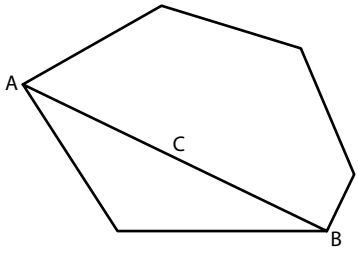

FIGURE 1. A visualization of "proof space."

some vertex. We shall call the proofs at the vertices of this polygon the *extreme proofs*.

It can be difficult to decide whether two proofs are "really the same." Usually a proof has a natural domain of applicability, which we shall call its "scope," and this domain provides us with the "scope test," a necessary condition for essential difference: proofs are "really different" if they have different scopes.

The Irrationality of $\sqrt{2}$

This article explores the proof space of one of the oldest and most familiar theorems of all: that there is no rational number a/b whose square is 2. This theorem was traditionally credited to Pythagoras, but it is perhaps more correct to ascribe it to the Pythagorean school, for Iamblichus tells us of the rule that all discoveries of this school were attributed to its founder.

According to Plato's *Theaetetus*, Theodorus demonstrated how to prove the irrationality of square roots of nonsquare numbers up to 17, an assertion that has given rise to much speculation about the reason he stopped there. It has been suggested that the reason might be that the proofs were geometrical and differed from case to case. Our first proof is one that Theodorus might have used for $\sqrt{2}$.

Tennenbaum's "Covering" Proof

The assertion that $\sqrt{2}$ is the quotient p/q of two integers is equivalent to $p^2 = 2q^2$, which is equivalent to the assertion that a $p \times p$ square has the same area as two $q \times q$ ones.

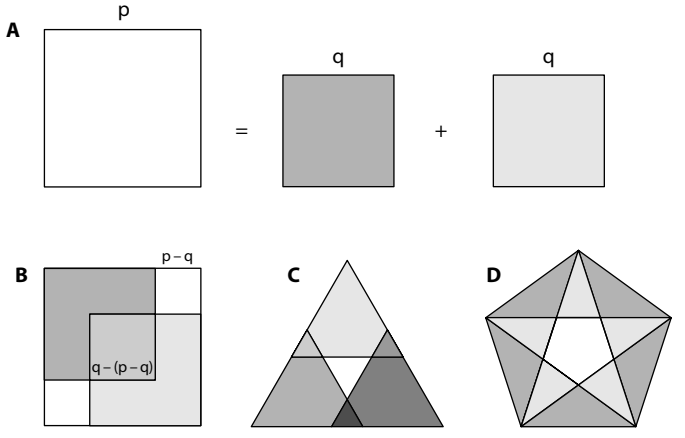

FIGURE 2. "Covering" proofs.

Stanley Tennenbaum therefore supposes that the large square at left in Figure 2A is the smallest one of integral side (p) that has the same area as two smaller ones of equal integer side (q) at right. Then, fitting the two smaller squares into opposite corners, we obtain Figure 2B, in which the central doubly covered square has the same total area as the two uncovered ones, a smaller example than we started with—a contradiction.

DISCUSSION

Traditionally, this type of argument is called a "proof by descent," and it relies on the principle (usually tacitly assumed by the ancients) that any nonempty set of positive integers has a least element.

This type of proof is difficult to generalize, but a glance at Figure 2C suggests a similar proof for $\sqrt{3}$, and you might find one for $\sqrt{5}$ after studying Figure 2D.

"Folding" Proofs

A traditional Greek statement of our theorem is that the diagonal and side of a square are incommensurable; that is, they cannot both be

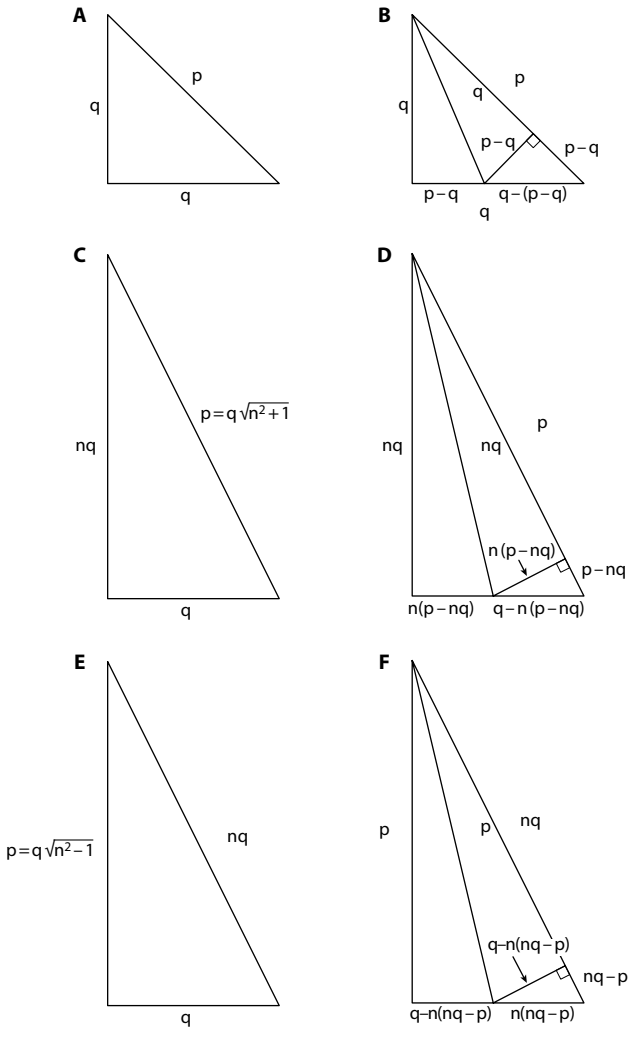

FIGURE 3. "Folding" proofs.

integer multiples of a common ("unit") length. Suppose that they are, and let the smallest such pair of integers be p and q, as in Figure 3A (in modern terms, $\sqrt{2} = p/q$). Folding the half-square triangle as in Figure 3B, we see that there is a smaller half-square triangle with integer sides—contradiction.

Discussion

In some sense, this proof is mechanically the same as Tennenbaum's; both suppose that the fraction in least terms that represents $\sqrt{2}$ is p/q and deduce the same contradiction, that $(q-(p-q))/(p-q)$ is a smaller one. It also assumes basic facts about Euclidean geometry, including the Pythagorean theorem. In effect, both proofs carry out geometrically the first step in the division algorithm that is at the heart of the Unique Factorization Theorem (also known as the Fundamental Theorem of Arithmetic).

However, our "scope test" shows that this proof is more general than the covering proof because essentially the same proof works for showing the irrationality of square roots of numbers of the form n^2+1.

As before, all labeled sides have integer lengths, and the fold shows a smaller triangle with integer-length sides that is similar to the original one. Apostol (2000) provided a similar proof.

Just as we needed a geometric equivalent to the division algorithm, to perform this proof in the style of Euclid requires the geometrical equivalent of the fact that any set of positive integers has a smallest element, namely, the Archimedean axiom that given any two segments, some multiple of each segment exceeds the other in length.

An analogous proof handles the case of $\sqrt{(n^2-1)}$ (as was also noted by Apostol): use a right triangle with base q, hypotenuse qn, and height $p=q\sqrt{(n^2-1)}$, and make the "same fold."

We thus obtain proofs for the irrationality of the square roots of 2, 3, 5, 8, 10, 15, 17, 24, 26, 35, 37, 48, 50, 63, 65, 80, 82, 99, . . . (of course, 8 already follows from 2).

We can also handle 6 because $\sqrt{6}=(1/2)\sqrt{24}$, and 7 because $\sqrt{7}=(1/3)\sqrt{63}$, and $\sqrt{11}$ because $\sqrt{11}=(1/3)\sqrt{99}$.

We observe that this trick works for all nonsquares D because the Pell equation $x^2-1=Dy^2$ is always solvable in integers (Stark 1978). This is not true for the form x^2+1 in some cases, for example, when $D=7$, so it was necessary to generalize the proof to handle $\sqrt{(n^2-1)}$.

No surviving manuscripts indicate that the ancient Greeks knew this fact (although we would not put it past Diophantus or Archimedes). They were certainly capable of finding the "geometric proof" that we now know always exists, in any particular case. Thus, Theodorus could have had a geometric proof in the style of Euclid for all D.

For $D=13$, the smallest solution is $(649^2-1=(13)(180)^2)$, so the original "n^2+1" proof works best $(18^2+1=(13)5^2)$. For $D=14$, we

can use ($15^2 - 1 = (14)4^2$). This answer provides a possible explanation for why Theodorus stopped at 17; to do 19 requires finding ($170^2 - 1 = (19)(39)^2$). It would have been even more difficult to demonstrate proofs for $D = 31$ ($1520^2 - 1 = (31)(273)^2$), and for $D = 61$, where the smallest solution is ($29{,}718^2 + 1 = (61)(3805)^2$).

"Traditional" Even/Odd Proof

The traditional arithmetical proof is to suppose that $\sqrt{2} = p/q$ in least terms, so that $p^2 = 2q^2$. But the square of an odd number is odd, so p must be even; say that it equals $2r$. Now $4r^2 = 2q^2$, and we deduce $q^2 = 2r^2$, showing that 2 equals the "simpler" fraction q/r.

Discussion

This proof is "extreme" in seeming to depend on the most elementary concepts. We did need the fact that fractions have canonical "least" forms, implying that any set of positive integers has a smallest element. Also, we are relying on the division of integers into two classes, "even" and "odd," with the property that a product is odd iff both factors are odd:

*	even	odd
even	even	even
odd	even	odd

How much does this proof generalize? Note that the same argument works for higher-order roots because the table implies that any power of an odd number is odd, not just its square.

We can replace 2 by any prime, and the proof is the same. Call a number "3even" (pronounced "threeven") if it is divisible by 3, otherwise it is "3odd" ("throdd"), for instance; then

*	3even	3odd
3even	3even	3even
3odd	3even	3odd

Of course, in using the fact that a prime divides a product only if it divides one of the factors, we are assuming the key lemma necessary to

prove the Unique Factorization Theorem; this lemma is obvious for the prime 2, but we didn't totally avoid "unique factorization."

This proof doesn't work for nonprimes (2 and 3 are 6odd, but their product isn't). To generalize to roots of nonprimes, we need to make a bigger table with more residue classes, but that's not really the "same proof" any longer.

Bashmakova's Proof

We don't know whether Theodorus stopped before or after proving the theorem for 17, and he apparently could not handle the general case (in the dialogue, Theaetetus claims to have improved on Theodorus by proving the general case). But here is a proof that works "up to 17," according to the Russian historian of mathematics, Isabella Bashmakova (Bashmakova and Lapin 1986):

Suppose that $p^2 = Nq^2$, with p/q in least terms. If N is divisible by 4, we may replace N by $N/4$ until it isn't. Suppose that N is even but not divisible by 4: then p^2 is even, so p is, so $p^2/2$ is, so $(N/2)q^2$ is, so (since $N/2$ is odd) q^2 is, so q is, so p/q is not in least terms—contradiction. So assume that N is odd. Since at least one of p and q must be odd, both are, so p^2 and q^2 are both 1 mod 8, so N is also. Thus we obtain a contradiction for any N except 1, 9, 17, 25, 33, . . . of which 17 is the first nonsquare and so the first failure of the proof.

Discussion

In one sense, this is not an "extreme" proof because it treats the cases of even and odd N with different ideas, and in fact for $N = 2$ it is really the same as the "traditional" proof. We include it for historical interest and because the "remainder" argument is a distinctly new idea, even though it only applies for N equal to 3, 5, or 7 mod 8.

Reciprocation Proof

This proof (from Conway and Guy 1996) overcomes the Unique Factorization difficulty. Suppose again that $\sqrt{2} = P/Q$. Then it also equals $2/\sqrt{2} = 2Q/P$. These two numbers P/Q and $2Q/P$ have "fractional parts" expressible as q/Q and p/P, which must be equal. But then P/Q and p/q

must be equal, so that p/q is the desired simpler fraction because $p < P$ and $q < Q$.

Discussion

This solution handles $\sqrt{N}$ for any nonsquare N without invoking Unique Factorization; however, it does use "division with remainder" once; this much is unavoidable if the notion of "fractional part" is to make sense. Euclid (*Elements*) also provides a proof (Book X, Proposition 9) with this "scope."

Unique Factorization Proof

Let a and b be positive integers. There is a prime factorization of a^2 (obtained by doubling the exponents in a prime factorization of a) in which the exponent of 2 is even, and similarly for b^2; but then $2b^2$ has a factorization in which the exponent of 2 is odd, and, by the Fundamental Theorem of Arithmetic, different factorizations must be of different numbers, so a^2 cannot equal $2b^2$, and a/b is not a square root of 2.

Discussion

This proof uses a hammer to crack a nut. It is not self-contained because we have not proven the Fundamental Theorem of Arithmetic. It clearly generalizes to show that no rational number can be the nth root of an integer that is not a perfect nth power: for the exponents of the primes in the factorizations of a^n and b^n are divisible by n, and if a^n is to equal kb^n, then all the exponents in the prime factorization of k must also be divisible by n, and when you divide them all by n you obtain an integer whose nth power is k. How is this proof "extreme"? Well, it's the shortest proof and the most transparent proof if the Fundamental Theorem of Arithmetic "comes for free," and it generalizes to arbitrary integers in both the base and the exponent.

After explaining how he had shown the irrationality of square roots, Theaetetus remarked "and the same for solids," suggesting that he also had a way to handle cube roots. Wayne Aitken has noted (FOM [Foundations of Mathematics] e-mail discussion list archived at http://www.cs.nyu.edu/pipermail/fom/2007-November/012259.html) that, even

though Euclid never stated the Fundamental Theorem of Arithmetic, one may use his proposition VIII.8 to derive the irrationality of nth roots by an argument similar to Euclid X.9, which treats square roots.

Analytic Proof

This proof, presented in Laczkovich (2001), is a quickie for those who know some algebra. For positive integers n, $(\sqrt{2}-1)^n$ has the form $a\sqrt{2}+b$ where a and b are integers, not necessarily positive. But if $\sqrt{2}$ were rational with denominator D, then for integral a,b, $a\sqrt{2}+b$ would be rational with denominator dividing D and so could not approach a limit of 0 as $(\sqrt{2}-1)^n$ must, since $0 < (\sqrt{2}-1) < 1$.

Discussion

From this type of argument, one may learn not only that $\sqrt{2}$ is irrational but also some quantitative information on how closely it can be approximated by rational numbers. The proof obviously generalizes to other

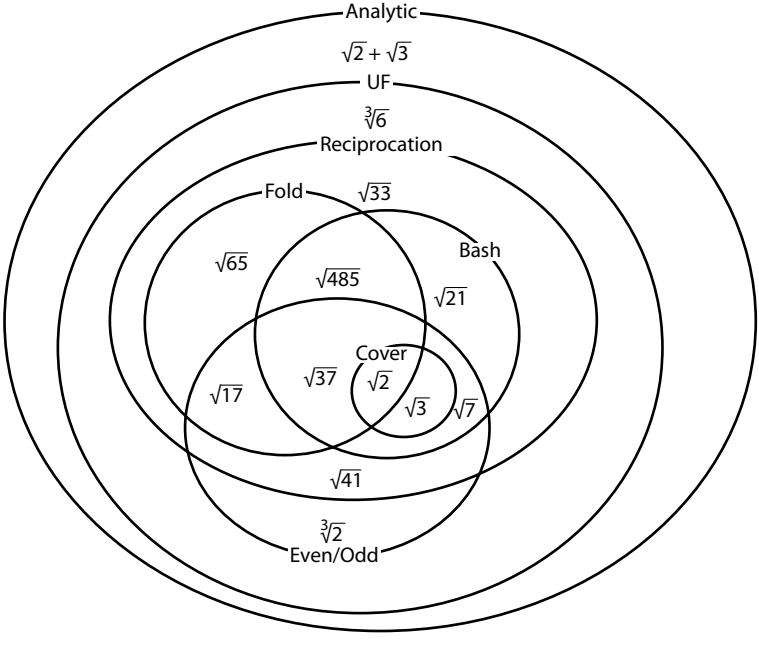

Figure 4. Relationships between proofs, with examples of all possibilities.

square roots; only slightly less obviously, it generalizes to "kth roots," using expressions of the form $aN^{(k-1)/k} + bN^{(k-2)/k} + \ldots + yN^{1/k} + z$, which will have denominators no larger than D^{k-1} if $N^{1/k}$ is rational with denominator D.

In fact, the proof generalizes further still and shows that all real algebraic integers (roots of polynomials with integer coefficients and a highest-degree coefficient of 1) are either integers or irrational numbers. All you have to note is that higher powers of the root can be replaced recursively by sums and differences of lower powers because the root satisfies a monic polynomial.

Because we took advantage of a new principle, that every real number is "close to an integer" (a distance of at most 1/2), this generalization is even more "extreme" than the one from the Unique Factorization proof.

Conclusion

All these proofs show the irrationality of various numbers; in the order we have presented them, each one handled some new cases to which the previous proofs did not apply. We summarize the seven proofs in the table that follows and provide a diagram illustrating their "scopes."

Table 1. Synopsis of Proof Types

Name of Proof	Domain of Applicability	Key Idea	Remarks	Why Proof Is "Extreme"
Covering	$\sqrt{2}$, $\sqrt{3}$, $\sqrt{?}$	Doubly covered = uncovered	$n = 2$ case from Stanley Tennenbaum; $n = 3$ from Conway	Visually obvious
Folding	Square roots of $(n^2 + 1)$	Folding a triangle	Apostol (2000): Similar proof for $(n^2 - 1)$. Conway and Shipman: handles all integers by Pell equation theory	Purely geometrical

Table 1. (*Continued*)

Name of Proof	Domain of Applicability	Key Idea	Remarks	Why Proof Is "Extreme"
Traditional even/odd	All roots of primes	Even–odd argument	Who first noted that this works for any prime?	Depends on simplest concepts
Bashmakova's	Square roots of integers $\neq 1 \bmod 8$	Remainder argument	Isabella Bashmakova and A. I. Lapin (1986) noted connection to *Theaetetus*' Theodorus (Plato)	Historical interest?
Reciprocation	Square roots of all integers	1 Step of division algorithm	Conway and Guy (1996)	Purely arithmetical; "slickest"
Unique factorization	All roots of all integers	Compare exponents in factorizations	Who first stated that all roots of nonpowers are irrational?	Most useful, shortest if Unique Factorization Theorem assumed
Analytic	Algebraic integers	Analytic estimate	Laczkovich [**L**] gives proof for $\sqrt{2}$, generalizes to roots of integers	Most general, quantitative, "surprising"

References

Apostol, T., "Irrationality of the Square Root of Two—A Geometric Proof," *American Mathematical Monthly* 107: 841–42, 2000.

Aigner, Martin, and Günter M. Ziegler, *Proofs from THE BOOK*, Springer, Berlin, 1998.

Bashmakova, I. G., and A. I. Lapin, *Pifagor*, Kvant, No. 1, 1986, p. 10 (in Russian).

Hardy, G. H., and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th ed., Clarendon Press, Oxford, U.K., 1959.

Conway, John H., and Richard K. Guy, *The Book of Numbers*, Copernicus, New York, 1996.

Euclid, *Elements: All Thirteen Books in One Volume*, T. L. Heath (trans.), Green Lion Press, Santa Fe, NM, 2002, http://www.greenlion.com/euclid.html.

Laczkovich, Miklós, *Conjecture and Proof*, Mathematical Association of America, Washington, DC, 2001.

Plato, *Theaetetus*. Benjamin Jowett (trans.), 3rd ed., Vol. 4 of 5, Oxford University Press, 1892, Oxford, U.K., http://oll.libertyfund.org/title/768/93834.

Stark, Harold M., *An Introduction to Number Theory*, MIT Press, Cambridge, MA, 1978.