# Irrationality via well-ordering

Gerry Myerson*

**Abstract**

Some irrationality facts that are usually proved using divisibility arguments can instead be proved using well-ordering. How far can we go, and who got there first?

There are many proofs of the irrationality of the square root of two. Here, we are concerned with proofs that are algebraic and rely on well-ordering, and not on divisibility by 2. Our purposes are to see how far such proofs can go, and to say a few words about their history.

**Theorem 1.** *The square root of 2 is irrational.*

*Proof.* Assuming $\sqrt{2}$ is rational, let $n$ be the smallest positive integer whose product with $\sqrt{2}$ is an integer; then $n(\sqrt{2}-1)$ is a smaller positive integer whose product with $\sqrt{2}$ is an integer, contradiction.

Here is a first step in extending the method of proof to a more general result.

**Theorem 2.** *If $m$ is an integer, and $\sqrt{m}$ is not an integer, then $\sqrt{m}$ is irrational.*

*Proof.* Assuming $\sqrt{m}$ is rational but not an integer, let $k$ be the integer such that $k<\sqrt{m}<k+1$, and let $n$ be the smallest positive integer whose product with $\sqrt{m}$ is an integer; then $n(\sqrt{m}-k)$ is a smaller positive integer whose product with $\sqrt{m}$ is an integer, contradiction.

Can the approach be souped up to prove the irrationality of $\sqrt[3]{2}$?

**Theorem 3.** *The cube root of two is irrational.*

*Proof.* Assuming $\sqrt[3]{2}$ is rational, let $n$ be the smallest positive integer whose products with $\sqrt[3]{2}$ and with $(\sqrt[3]{2})^2$ are both integers; then $n(\sqrt[3]{2}-1)$ is a smaller positive integer with the same property, contradiction.

Now it is clear how to prove the irrationality of $\sqrt[3]{m}$, or indeed of $\sqrt[k]{m}$ for any positive integers $k$ and $m$ for which $\sqrt[k]{m}$ is not an integer.

**Theorem 4.** *If $k>0$ and $m$ are integers, and $\sqrt[k]{m}$ is not an integer, then $\sqrt[k]{m}$ is irrational.*

Received 21 June 2007; accepted for publication 7 November 2007.
*Mathematics, Macquarie University, NSW 2109. E-mail: gerry@maths.mq.edu.au

*Proof.* Assuming $\sqrt[k]{m}$ is rational but not an integer, let $n$ be the smallest positive integer whose products with $(\sqrt[k]{m})^j$ are integers for $1 \le j \le k-1$; then $n\{\sqrt[k]{m}\}$ is a smaller positive integer with the same property, contradiction.

Here $\{z\}$ is the fractional part of $z$, which differs from $z$ by an integer, and satisfies $0 < \{z\} < 1$ when $z$ is not an integer.

We can push the idea one step further.

**Theorem 5.** *Let $f$ be a monic polynomial with integer coefficients. Let $\alpha$ be a solution of $f(\alpha) = 0$. Then if $\alpha$ is not an integer, it is irrational.*

*Proof.* Assume the hypotheses, assume $\alpha$ is rational, and let $n$ be the smallest positive integer whose product with $\alpha^j$ is an integer for all $j$ less than the degree of $f$. Then $n\{\alpha\}$ is a smaller positive integer with the same property, contradiction.

Perhaps this proof could use some elaboration.

First of all, if $\alpha$ is rational, say, $\alpha = a/b$ with $a$ and $b$ integers, $b > 0$, then $b^{d-1}$, where $d$ is the degree of $f$, has the property that multiplication by $\alpha^j$ gives an integer for all $j$ less than the degree of $f$. Thus, the set of all such positive integers is not empty. By well-ordering, there is a least such positive integer, which we call $n$.

As $\alpha$ is not an integer, we have $0 < \{\alpha\} < 1$, so $0 < n\{\alpha\} < n$, so $n\{\alpha\}$ is positive and smaller than $n$. We write $\{\alpha\} = \alpha - k$ for some integer $k$.

Now $n\{\alpha\}\alpha^j = n\alpha^{j+1} - kn\alpha^j$ is clearly an integer for $0 \le j < d-1$. But the equation $f(\alpha) = 0$ with $f$ a monic polynomial with integer coefficients implies that $\alpha^d$ is a sum of integer multiples of smaller powers of $\alpha$, so also in the case $j = d-1$ we get that $n\{\alpha\}\alpha^j$ is an integer.

This completes the justification of the proof.

Now let $K$ be a number field (that is, a field containing the rationals and of finite dimension as a vector space over the rationals). Let $\mathcal{O}$ be the ring of integers of $K$ (that is, the set of those elements of $K$ which are roots of a monic polynomial with integer coefficients).

**Theorem 6.** *$\mathcal{O}$ is integrally closed in $K$.*

This means that if $\alpha$ is in $K$ and $f(\alpha) = 0$ for some monic polynomial $f$ with coefficients in $\mathcal{O}$ then $\alpha$ is in $\mathcal{O}$. This is a standard fact from algebraic number theory (see, e.g. [6]). Theorem 5 says $\boldsymbol{Z}$ is integrally closed in $\boldsymbol{Q}$, so Theorem 6 can be seen as the next step in the progression that took us from Theorem 1 to Theorem 5. I don't know whether there is a proof in the spirit of the other proofs in this paper. I note that the unique factorisation theorem, which can be used to prove Theorems 1 through 5, can't be used to prove Theorem 6, since $\mathcal{O}$ may not be a unique factorisation domain. The closest I have come to a well-ordering proof

of Theorem 6 is the following. We remind the reader that a Euclidean domain is an integral domain admitting a Euclidean algorithm.

**Theorem $5\frac{1}{3}$.** A Euclidean domain is integrally closed in its field of fractions.

*Proof.* Let $D$ be a Euclidean domain. Let $K$ be the field of fractions of $D$. Let $\alpha$ in $K$ be integral of degree $n$ over $D$ (that is, let $\alpha$ be a zero of an irreducible monic polynomial of degree $n$ with coefficients in $D$).

Let $N$ be the norm on $D$. Let $b$ be a non-zero element of $D$ of smallest norm whose product with each of $\alpha, \alpha^2, \ldots, \alpha^{n-1}$ is in $D$. Let $b\alpha = a$, and let $a = bq + r$, where $q$ and $r$ are in $D$ and $r = 0$ or $N(r) < N(b)$. Then by the usual calculations $r\alpha^j$ is in $D$ for $j = 1, 2, \ldots, n-1$, so $r = 0$, so $\alpha = q$ is in $D$.

Of course, unique factorisation can also be used to prove Theorem $5\frac{1}{3}$.

Now here's what I know about the history of these proofs. I need to bring in a variation on the theme.

*Proof of Theorem 1 (variant).* Assume $\sqrt{2} = a/b$, with $a$ and $b$ integers. Then $\sqrt{2} = a/b = (2b - a)/(a - b)$, contradiction.

Equality between $a/b$ and $(2b - a)/(a - b)$ is easily established by multiplying out and noting that $a^2 = 2b^2$. The contradiction comes from noting that $a - b < b$ (or that $2b - a < a$, or that $(2b - a) + (a - b) < a + b$), and appealing to well-ordering.

This proof of Theorem 1 has in common with the previous proof that it relies on well-ordering and not on divisibility by 2. The resemblance is closer than that, for under the hypothesis $\sqrt{2} = a/b$ we see that $a - b = b(\sqrt{2} - 1)$ which is exactly the crucial quantity in the earlier proof. I think it's really one proof in two forms, which I'll call the A-form and the B-form. The distinction between them is that in A-form proofs we hypothesise a positive integer $n$ whose products with some other quantity or quantities are integral, and produce a smaller positive integer with the same property; in B-form proofs, we assume the quantity of interest is a fraction, and deduce that it is also a 'smaller' fraction (in some appropriate well-ordering of fractions).

Something like the B-form appears in Steinhaus [13]. It's on pages 38–39 of the 1969 edition (but note the reference, below, to the first, 1938, edition). The precise equation $a/b = (2b - a)/(a - b)$ does not appear, and the equations that do appear are motivated as much by geometric arguments of similarity as by algebraic calculations, but Steinhaus does use well-ordering and not divisibility to reach the desired conclusion.

It's quite possible that someone took that path long before Steinhaus. I haven't seen any earlier reference. Dickson's History [3] is silent on proofs of irrationality.

Some sources attribute the well-ordering proof to Niven. It does not appear in either of his books on irrational numbers ([8], [9]). It does not appear in the 1960 edition of the textbook he wrote with Zuckerman, but the B-form of Theorem 2 appears as an exercise on pages 182–183 of the 1980 edition [10].

The paper of Maier and Niven [7] gives the B-form of Theorem 2. Then it gives A-form proofs of Theorems 4 and 5. These A-form proofs also rely on the division

theorem, and seem to me to be a bit less straightforward than the proofs we give here.

The Maier–Niven paper also gives a reference to page 132 of the 1938 edition of the Steinhaus book, an edition which is not available to me.

Subbarao [14] gives a B-form proof of Theorem 2. He asks whether the line of reasoning can be extended to establish the irrationality of $\sqrt[k]{m}$ more generally.

Lange [5] notes both [7] and [14], and gives a B-form proof of the irrationality of $\sqrt[k]{m}$. Lange's proof proceeds in two stages, using the type B argument in each stage. Lange doesn't use the division theorem.

Estermann [4] gives A-form proofs of Theorems 1 and 2. To the best of my knowledge, this marks the first appearance of these proofs in their most elegant formulation.

Bloom [1] gives a B-form proof of Theorem 1, writing that it was presented by Niven in a lecture in 1985.

I'm going to skip over the many recent textbooks I've seen that give well-ordering proofs of irrationality, as they don't give references and don't go beyond Theorem 2.

Brown [2] proves Theorems 1, 2, 4 and 5 by an A-form argument. Brown arranges the proofs of Theorems 4 and 5 in such a way as to need two inductions. Brown gives no references.

The proof of Theorem 5 given in this paper appears electronically but not, to the best of my knowledge, in print. It was posted to the Usenet newsgroup sci.math by Severian [12]. Severian gave no references. It is also posted at the Platonic Realms website [11]; it was sent to that site by Richard Palais. Professor Palais has told me that he does not recall where he first saw the proof, and that he suspects it goes back a long way.

The proof of Theorem $5\frac{1}{3}$ given here may be new.

**Summary**

Proofs of irrationality that depend on well-ordering and not on divisibility arguments can be very elegant. They have a long and confusing history. The arrangements given in this paper appear, to me, to be tidier than those already in the printed literature. It would be nice to have a proof in the same spirit that the ring of integers in a number field is integrally closed.

## References

[1] Bloom, D.M. (1995). A one-sentence proof that $\sqrt{2}$ is irrational. *Math. Mag.* **68,** 286.
[2] Brown, K.S. Gauss' lemma without explicit divisibility arguments. http://www.mathpages.com/home/kmath118.htm (accessed 9 December 2007).
[3] Dickson, L.E. (1919, 1920, 1923). *History of the Theory of Numbers*, 3 volumes. Carnegie Institution of Washington.
[4] Estermann, T. (1975). The irrationality of $\sqrt{2}$. *Math. Gaz.* **59,** 110.
[5] Lange, L.J. (1969). A simple irrationality proof for $m$th roots of positive integers. *Math. Mag.* **42,** 242–244. MR 41 #140.

[6] Marcus, D.A. (1977). *Number Fields*. Springer. MR 56 #15601.
[7] Maier, E.A. and Niven, I. (1964). A method of establishing certain irrationalities. *Math. Mag.* **37,** 208–210.
[8] Niven, I. (1956). *Irrational Numbers* Mathematical Association of America. MR 18, 195c.
[9] Niven, I. (1961). *Numbers: Rational and Irrational*. Random House. MR 24, #A66.
[10] Niven, I. and Zuckerman, H.S. (1980). *An Introduction to the Theory of Numbers*, 4th edn. Wiley. MR 81g:10001.
[11] Platonic Realms, The irrationality of the square root of 2. http://www.mathacademy.com/pr/prime/articles/irr2/index.asp (accessed 9 December 2007).
[12] Severian. Re: A simple proof for the irrationality of the square root of 3, post to Usenet newsgroup sci.math, 12 July 2000.
[13] Steinhaus, H. (1969). *Mathematical Snapshots*, 3rd edn. Oxford University Press, North Carolina, USA. MR 2000h:00002.
[14] Subbarao, M.V. (1968). A simple irrationality proof for quadratic surds. *Amer. Math. Monthly* **75,** 772–773.