

IRRATIONAL SQUARE ROOTS

$\sqrt{n}$ is rational only when n is a perfect square

Drew M. Schaffner

1 STATEMENT

THEOREM 1.1 (*Square roots*). Let n be a positive integer. Then $\sqrt{n}$ is rational if and only if $n = k^2$ for some integer k . In particular, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$ and $\sqrt{6}$ are irrational.

2 SETTING

We use only the integers and the well-ordering principle: every non-empty set of positive integers has a least element. A real number x is *rational* if $x = p/q$ for integers p and $q \geq 1$.

3 IDEA OF THE PROOF

If $\sqrt{n} = p/q$, then $\sqrt{n}$ times a suitable integer combination of p and q produces a representation with a strictly smaller denominator. Choosing the smallest denominator first gives a contradiction. This needs no primes and no unique factorisation.

4 PROOF

LEMMA 4.1 (*Integer part*). If n is not a perfect square, there is an integer k with $k < \sqrt{n} < k + 1$.

PROOF. Let k be the largest integer with $k^2 \leq n$; it exists because $0^2 \leq n$ and $j^2 > n$ for $j > n$. Then $k^2 \leq n < (k + 1)^2$, and $k^2 \neq n$ by assumption, so $k < \sqrt{n} < k + 1$. ■

Proof of Theorem 1.1. If $n = k^2$, then $\sqrt{n} = k/1$ is rational. Conversely, suppose n is not a perfect square but $\sqrt{n}$ is rational. Take k from Lemma 4.1. The set

$$S = \{q \geq 1 : q\sqrt{n} \in \mathbb{Z}\}$$

is non-empty, so by well-ordering it has a least element q . Write $p = q\sqrt{n}$, and put

$$q' = p - kq = q(\sqrt{n} - k), \quad p' = q'\sqrt{n} = nq - kp.$$

Both q' and p' are integers, because $p' = q\sqrt{n} \cdot \sqrt{n} - kq\sqrt{n} = nq - kp$. Since $0 < \sqrt{n} - k < 1$, we have $0 < q' < q$. So $q' \in S$ and $q' < q$, contradicting the minimality of q . ■

5 A SECOND PROOF, BY PRIME FACTORISATION

LEMMA 5.1 (Euclid). *If a prime ℓ divides ab , then $\ell \mid a$ or $\ell \mid b$.*

This is standard; it follows from Bézout's identity. If $\ell \nmid a$, then $\gcd(a, \ell) = 1$, so $1 = ax + \ell y$ for some integers x, y , and $b = abx + \ell by$ is divisible by ℓ .

Second proof of Theorem 1.1. Suppose $\sqrt{n} = p/q$ in lowest terms, so that $\gcd(p, q) = 1$ and $p^2 = nq^2$. If $q > 1$, let ℓ be a prime dividing q . Then $\ell \mid p^2$, so $\ell \mid p$ by Lemma 5.1, contradicting $\gcd(p, q) = 1$. Hence $q = 1$ and $n = p^2$. ■

6 REMARKS

Remark 6.1. The second proof generalises at once. If a rational number p/q in lowest terms is a root of a monic polynomial $x^d + c_{d-1}x^{d-1} + \cdots + c_0$ with integer coefficients, then multiplying by q^d shows $q \mid p^d$, so $q = 1$. A rational root of such a polynomial must therefore be an integer. Taking $x^d - n$, the number $\sqrt[d]{n}$ is rational only when n is a perfect d th power.

Remark 6.2. The first proof is a version of the descent in the Foundations notes, where it is carried out for $\sqrt{2}$ with $k = 1$. There the new representation is $\sqrt{2} = (2q - p)/(p - q)$.