

A proof of the irrationality of $\sqrt{2}$

Leslie Lamport

December 1, 1993

Abstract

Printable version of a sample proof that uses Lamport's proof style [1], illustrating how structured proofs can be converted to HTML pages via L^AT_EX₂H_TM_L enriched with extensions for Lamport's proof style.

Theorem There does not exist r in \mathbf{Q} such that $r^2 = 2$.

PROOF SKETCH: We assume $r^2 = 2$ for $r \in \mathbf{Q}$ and obtain a contradiction. Writing $r = m/n$, where m and n have no common divisors (step ⟨1⟩1), we deduce from $(m/n)^2 = 2$ and the lemma that both m and n must be divisible by 2 (⟨1⟩2 and ⟨1⟩3).

ASSUME: 1. $r \in \mathbf{Q}$
2. $r^2 = 2$

PROVE: False

⟨1⟩1. Choose m, n in \mathbf{Z} such that

1. $\gcd(m, n) = 1$
2. $r = (m/n)$

⟨2⟩1. Choose p, q in \mathbf{Z} such that $q \neq 0$ and $r = p/q$.

PROOF: By assumption ⟨0⟩:1.

LET: $m \triangleq p / \gcd(p, q)$

$n \triangleq q / \gcd(p, q)$

⟨2⟩2. $m, n \in \mathbf{Z}$

PROOF: ⟨2⟩1 and definition of m and n .

⟨2⟩3. $r = m/n$

PROOF: $m/n = \frac{p / \gcd(p, q)}{q / \gcd(p, q)}$ [Definition of m and n]
 $= p/q$ [Simple algebra]
 $= r$ [By ⟨2⟩1]

⟨2⟩4. $\gcd(m, n) = 1$

PROOF: By the definition of the gcd, it suffices to:

ASSUME: 1. s divides m

2. s divides n

PROVE: $s = \pm 1$

⟨3⟩1. $s \cdot \gcd(p, q)$ divides p .

PROOF: $\langle 2 \rangle$:1 and the definition of m .
 $\langle 3 \rangle$ 2. $s \cdot \gcd(p, q)$ divides q .
 PROOF: $\langle 2 \rangle$:2 and definition of n .
 $\langle 3 \rangle$ 3. Q.E.D.
 PROOF: $\langle 3 \rangle$ 1, $\langle 3 \rangle$ 2, and the definition of \gcd .
 $\langle 2 \rangle$ 5. Q.E.D.
 $\langle 1 \rangle$ 2. 2 divides m .
 $\langle 2 \rangle$ 1. $m^2 = 2n^2$
 PROOF: $\langle 1 \rangle$ 1.1 implies $(m/n)^2 = 2$.
 $\langle 2 \rangle$ 2. Q.E.D.
 PROOF: By $\langle 2 \rangle$ 1 and the lemma.
 $\langle 1 \rangle$ 3. 2 divides n .
 $\langle 2 \rangle$ 1. Choose p in \mathbf{Z} such that $m = 2p$.
 PROOF: By $\langle 1 \rangle$ 2.
 $\langle 2 \rangle$ 2. $n^2 = 2p^2$
 PROOF: $2 = (m/n)^2$ [$\langle 1 \rangle$ 1.2 and $\langle 0 \rangle$:2]
 $= (2p/n)^2$ [$\langle 2 \rangle$ 1]
 $= 4p^2/n^2$ [Algebra]
 from which the result follows easily by algebra.
 $\langle 2 \rangle$ 3. Q.E.D.
 PROOF: By $\langle 2 \rangle$ 2 and the lemma.
 $\langle 1 \rangle$ 4. Q.E.D.
 PROOF: $\langle 1 \rangle$ 1.1, $\langle 1 \rangle$ 2, $\langle 1 \rangle$ 3, and definition of \gcd .

References

- [1] Leslie Lamport, 1993, How to write a proof. In *Global Analysis of Modern Mathematics*, pp. 311–321. Publish or Perish, Houston, Texas, February 1993. A symposium in honor of Richard Palais’ sixtieth birthday (also published as SRC Research Report 94). <http://research.microsoft.com/users/lamport/proofs/src94.ps.Z>