

## Irrationality and roots

In everything that we do here, the numbers will be integers, except for rational numbers which are ratios of integers  $p/q$ , and square roots of integers, which will be shown to be either integers, or irrational (with no  $p$  and  $q$  such that  $p/q = \sqrt{N}$ ).

The product of two integers is an integer.

*Proof.*

This follows since multiplication of two integers  $m \cdot n$  is equivalent to repeated addition of  $n$  to itself. We start by  $n$  to 0 and repeat a total of  $m$  times.

That integers add and subtract to give integers is an inherent property of  $\mathbb{N}$ , since the addition  $s + n$  is the addition of 1 to  $s$  a total of  $n$  times. Forming successive integers by adding 1 defines  $\mathbb{N}$ .

□

If  $n \cdot n = N$ , then  $n$  is the square root of  $N$ . With both  $n$  and  $N$  integer,  $N$  is a *perfect square*.

We will show that if  $N$  is not a perfect square, then its square root is irrational.

**Euclid's proof that  $\sqrt{2}$  is irrational**

There do not exist integer  $a$  and  $b$  such that  $(a/b)^2 = 2$ .

In all these proofs, we require that  $a/b$  be in "lowest terms." If there exist integer  $c$ ,  $x$  and  $y$  such that  $cx/cy = a/b$ , then  $a$  and  $b$  must be replaced with  $x$  and  $y$ .

Euclid's algorithm for the greatest common divisor gives an easy method for determining whether a common factor  $c$  exists.

[https://en.wikipedia.org/wiki/Euclidean\\_algorithm](https://en.wikipedia.org/wiki/Euclidean_algorithm)

We need the following preliminary result.

*Lemma*

The square of an even integer is even, while the square of an odd integer is odd.

*Proof of the lemma*

Any even number can be written as  $2k$  and its square as  $4k^2$  which is even.

Any odd number can be written as  $2k+1$  (for integer  $k$ ), which squares to give  $4k^2 + 4k + 1$ . The first two terms are clearly even and add to give another even number, one more than that is an odd number.

Therefore, if  $a^2$  is even, then so is  $a$ , for it were odd, its square would be odd too.

*Proof (1).*

Suppose there do exist such  $a$  and  $b$ . Then  $a^2 = 2b^2$ , which means that  $a$  is even. Then we can write  $a = 2k$  so

$$(2k)^2 = 4k^2 = 2b^2$$

$$2k^2 = b^2$$

which means that  $b$  must be even.

But then  $a/b$  is not in lowest terms. This is a contradiction. Therefore, there do not exist such  $a$  and  $b$ .

□

If both  $a$  and  $b$  were even it would be obvious, since all even numbers end in one of five digits: 0, 2, 4, 6, 8 (in base 10).

### Apostol's geometric proof

There are many other proofs of the irrationality of the square root of 2.

[https://www.cut-the-knot.org/proofs/sq\\_root.shtml](https://www.cut-the-knot.org/proofs/sq_root.shtml)

Here we will look at a geometric proof from Tom Apostol (see the link). A more elaborate exposition is:

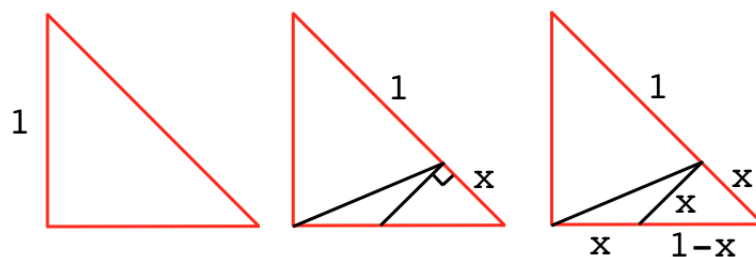
<https://jeremykun.com/2011/08/14/the-square-root-of-2-is-irrational-ge>

Theorem: if there is an isosceles triangle with integer sides, then there is a smaller one with the same property.

*Proof* (2).

Draw an isosceles triangle with side length 1, then Pythagoras tells us that the hypotenuse is equal in length to  $\sqrt{2}$  (left panel).

Our hypothesis is that this length is a rational number, and its ratio to the side is in "lowest terms".



Mark off the length of the side (length 1) on the hypotenuse, and erect a perpendicular (middle panel). Also draw the line segment to the opposite vertex of the original triangle.

The new small triangle that is formed containing the right angle and with side length  $x$  in the middle panel is isosceles, because it is a right triangle, and it contains one of the complementary angles of the original right triangle.

By hypothesis, its side length  $x$  is the difference of two rational numbers, so  $x$  is a rational number.

Furthermore, the *other* small triangle is also isosceles. Its base angles, when added to the equal angles of an isosceles triangle, form right angles. This allows us to mark the side along the base as having length  $x$  as well.

Therefore, the hypotenuse of the new, small right triangle is a rational number, since it is equal to  $1 - x$ .

We are back where we started, with an isosceles right triangle that has all rational sides.

It is clear that this process can continue forever. The sides will never be in "lowest terms" because we can always form a new similar but smaller right triangle, which amounts to evenly dividing both the sides and the hypotenuse by a rational number.

□

### **rational root theorem**

#### *Euclid's Lemma*

When we write  $p|ab$  ( $p$  "divides" the product  $ab$ ), we mean that there exists  $c$  such that  $c \cdot p = ab$ .

If  $p|ab$ , then either  $p|a$  or  $p|b$  (or both).

An easy proof of Euclid's lemma relies on the prime factorization theorem. I've gone through Hardy's wonderful proof of this theorem elsewhere.

The prime factorization theorem says that every integer can be written as a unique product of prime factors (some may be repeated). So, for example  $a = p_1 \cdot p_2 \dots$  and so on.

*Proof of the lemma*

Suppose to the contrary,  $p|ab$  but  $p$  does not divide either  $a$  or  $b$ .

Both  $a$  and  $b$  have a unique prime factorization and those factors multiplied together are the prime factors of  $n$ . These factors do not include  $p$ , and yet the factorization is unique.

This is a contradiction.

$p$  must divide at least one of  $a$  or  $b$ .

□

*Proof (3).*

Consider

$$x^2 - N = 0$$

The solution is  $x = \sqrt{N}$ .

We develop the rational root theorem for this special case. The theorem says that for

$$a_n x^n + \dots + a_1 x + a_0$$

if the rational number  $p/q$  is a solution, then it must be that  $p|a_0$  and  $q|a_n$ .

Suppose  $p/q = x$  is a rational solution in lowest terms. Then

$$\left(\frac{p}{q}\right)^2 - N = 0$$

$$p^2 = Nq^2$$

Since  $p$  divides the left-hand side, it must divide either  $N$  or  $q$  on the right. But  $p$  is co-prime to  $q$ . Therefore it must be that  $p|N$ . If  $N$  is prime then  $p$  is equal to  $N$ .

An analogous argument shows that  $q|1$ , so  $q = 1$ .

Therefore, the possible values for  $p/q$  are  $\pm N/1$ , but none of these solves the equation.

Thus, there is no solution in the rational numbers.

#### **all prime numbers**

Here is another proof that works for all prime numbers.

*Proof* (4).

Suppose that  $\sqrt{N} = a/b$  where  $a$  and  $b$  are integers and their ratio is a rational number. Then,

$$a^2 = Nb^2$$

By the prime factorization theorem,  $a = p_1 \cdot p_2 \dots$ , so  $a^2 = p_1^2 \cdot p_2^2 \dots$ . Thus  $a^2$  has an even number of factors and so does  $b^2$ .

But  $N$  is a prime number, its only prime factor is itself. Therefore in the above expression there is an odd number of prime factors on the left and an even number on the right.

But every number, including  $a^2$ , has a unique prime factorization. This is a contradiction.

Therefore, every square root of a prime number is irrational.

We can also adapt the very first proof to prime numbers.

*Proof (5).*

We have  $a$  and  $b$  such that

$$a^2 = Nb^2$$

and also  $a$  and  $b$  are co-prime, and  $N$  is prime. Then,  $N$  divides  $a^2$ . Therefore, by Euclid's lemma  $N|a$ .

This means we can find  $c$  such that  $cN = a$  and thus

$$(cN)^2 = c^2 N^2 = b^2$$

$$cN = b$$

which means that  $N|b$ . But we claimed that  $a$  and  $b$  are co-prime. This is a contradiction.

Therefore there do not exist such  $a$  and  $b$ .

**all except perfect squares**

*Lemma*

An irrational number times a rational number is always irrational.

*Proof of the lemma.*

Given  $r$  is rational and  $x$  is irrational. Suppose that  $rx$  is rational. Thus  $rx/r$  must be rational. But  $rx/r = x$ . This is a contradiction. Therefore  $rx$  is irrational.

*Proof (6).*

For arbitrary  $N$ , write

$$N = p_1^{e_1} \cdot p_2^{e_2} \dots$$

where the  $p_i$  are prime and the exponents  $e_i$  are integers.

If all the  $e_i$  are even, then  $N$  is a perfect square. So at least one of  $e_i$  is odd. Let  $e_1$  be odd.

If  $e_1 = 1$ , then use Proof (5), and show that both  $a$  and  $b$  are multiples of  $p_1$ .

Otherwise,  $e_1 > 1$  and odd, and we can write

$$\left(\frac{a}{b}\right)^2 = N = M \cdot p_1 \cdot [p_1^{(e_1-1)/2}]^2$$

Since  $(e_1 - 1)/2$  is even, the squared term on the right-hand side is a perfect square and thus rational.

We thus have  $Mp_1$  times a rational number is equal to a rational number. So  $Mp_1$  must also be rational.

Now use Proof (5) to show that  $p_1$  divides both  $a$  and  $b$ , which is a contradiction.

#### **example**

For the last proof, let  $N = 216 = 2^3 \cdot 3^3$ . Then  $N = 2 \cdot (4 \cdot 27)$ . Therefore  $a$  is even ... and so  $b$  is even ... contradiction.

<http://mathforum.org/library/drmath/view/57117.html>