Rationale of Irrationality

The mathematics[$] one is taught at schools is really rather utilitarian, and little if any attention is paid to the deeper implications of arithmetic[$] in particular. But, fortunately, the ancient Greeks had devoted a great deal of their awesome collective – and individual – brainpower to investigations of this sort, and I've always been rather intrigued by their discoveries (or at least, those that I could understand).

Three of the best-known names were Pythagoras (born ca 570 BC), Euclid (born ca 325 BC) and Archimedes (born ca 287 BC), and I'd like to dwell on a fascinating connection between the two first-mentioned of these.

Pythagoras didn't originate his eponymous theorem about the square on the hypotenuse[$] of a right-angled triangle, which had been discovered empirically centuries or even millennia previously, but he gave it a rationale, quite possibly the proof that Euclid reproduced in his *Elements* (a compendium of the geometry[$] and number theory as known by that time).

But the particular case of a right-angled isosceles[$] triangle caused a crisis which has reverberated down the centuries to this day. If the legs of the triangle were each (say) a metre in length, the theorem reported that the length in metres of the hypotenuse was the square root of $(1^2 + 1^2)$, ie $\sqrt{2}$.

The result was taken calmly, until one Hippasus, tasked with evaluation of this quantity, found to his horror that it couldn't be expressed rationally, ie as a ratio, one whole number divided by another whole number. The senior ranks of the Brotherhood decided that this awkward inconsistency with their beliefs had to be suppressed; Hippasus was taken out to sea, tied to an anvil and dropped overboard.

But the news couldn't be kept secret, and in conjunction with Zeno's paradoxes concerning the infinitesimal and the infinite had a profound consequence for the development of early Greek mathematics, steering it towards geometry rather than arithmetic and algebra

In what follows, 'number' means positive integer, and 'divides' means 'divides exactly, without remainder'.

[$] All these terms were originated by the ancient Greeks. The word 'hypotenuse' is particularly interesting, as its literal meaning is "stretching under". This goes back to the even-more ancient Egyptian use of a 3-4-5 knotted rope to define the required right-angles at the base corners of Important buildings such as square pyramids. The scalene triangle with commensurate sides was of course infinitely preferable to the incommensurate 1-1-$\sqrt{2}$ sides of an isosceles triangle.

A] To prove that $\sqrt{2}$ is irrational using Pythagorean proof

01.00] Suppose that $\sqrt{2}$ is rational.

$\therefore$ $\sqrt{2} = a/b$ where a and b are coprime

$\therefore$ $2 = a^2/b^2$

$\therefore a^2 = 2b^2$

01.01] $2b^2$ is evidently divisible by 2 and is therefore even

01.02] $\therefore a^2$ is even, and a is therefore even (odd times odd is odd)

01.03] $\therefore a = 2c$, where c is some number, odd or even

02.00] $\therefore a^2 = 4c^2 = 2b^2$ so $b^2 = 2c^2$

02.01] $\therefore b^2$ is even, and b is therefore even (odd times odd is odd)

02.02] $\therefore b = 2d$, where d is some number, odd or even

03.00] So **a and b are both divisible by 2, and cannot be coprime**

03.01] ie √2 cannot be rational, and is therefore irrational. QED.

I came across this proof when I was about 13 and have wondered, ever since, whether there was some way of proving a similar result for √3, and √5, and so on. Well of course there is, using Euclid's Lemma, and let's just trial it for √2.

B] To prove that √p is irrational using Euclid's Lemma

01.00] Suppose that √p is rational, where p is any prime

$\therefore \sqrt{p} = a/b$ where a and b are coprime

$\therefore p = a^2/b^2$

$\therefore p.b^2 = a^2$

01.01] $p.\ b^2$ is evidently divisible by p

01.02] But a^2 is divisible by p only if a is divisible by p (Euclid's Lemma)

01.03] $\therefore p.b^2 = a^2$ is only possible if **a is divisible by p**

02.00] If a is divisible by p then a^2 is divisible by p^2

02.01] $\therefore p.b^2$ is divisible by p^2

02.02] $\therefore b^2$ is divisible by p

02.03] But b^2 is divisible by p only if **b is divisible by p** (Euclid's Lemma)

03.00] So **a and b must both be divisible by p, and cannot be coprime**

03.01] So √p cannot be rational, and is therefore irrational. QED.

But what about cube roots, fourth roots, fifth roots and so on ?

C] To prove that $\sqrt[n]{p}$ $(n>2)$ is irrational using Euclid's Lemma

01.00] Suppose that $\sqrt[n]{p}$ is rational, where n is integer and p is any prime

$\therefore$ $\sqrt[n]{p} = a/b$ where a and b are coprime

$\therefore$ $p = a^n/b^n$

$\therefore$ $p.b^n = a^n$

01.01] $p.b^n$ is evidently divisible by p

01.02] But a^n is divisible by p only if a is divisible by p (Euclid's Lemma)

01.03] $\therefore$ $p.b^n = a^n$ is only possible if **a is divisible by p**

02.00] If a is divisible by p then a^n is divisible by p^n

02.01] $\therefore$ $p.b^n$ is divisible by p^n

02.02] $\therefore$ b^n is divisible by p

02.03] But b^n is divisible by p only if **b is divisible by p** (Euclid's Lemma)

03.00] So **a and b must both be divisible by p, and cannot be coprime**

03.01] So $\sqrt[n]{p}$ cannot be rational, and is therefore irrational. QED

D] Excelsior

We're making good progress, but there are other subsets of numbers that haven't yet been addressed. Let's stick to square roots to start with.

- Perfect square numbers (4, 9, 16, 25, etc)
- Even numbers greater than 2 (6, 8, 10, 12, etc)
- Odd non-prime numbers (15, 21, 27, 33, 35, 39, etc)

D1] To prove that $\sqrt{n}$ $(n = m^2)$ is rational

01.00] $\sqrt{m^2} = m$, a whole number (2, 3, 4, 5, etc) and is therefore rational.

D2] To prove that $\sqrt{2n}$ is irrational using Pythagorean proof

01.00] Suppose that $\sqrt{2n}$ is rational.

$\therefore$ $\sqrt{2n} = a/b$ where a and b are coprime

$\therefore 2n = a^2/b^2$

$\therefore a^2 = 2nb^2$

01.01] $2nb^2$ is evidently divisible by 2 and is therefore even

01.02] $\therefore a^2$ is even, and a is therefore even (odd times odd is odd)

01.03] $\therefore a = 2c$, where c is some number (incorporating n), odd or even

02.00] $\therefore a^2 = 4c^2 = 2b^2$ so $b^2 = 2c^2$

02.01] $\therefore b^2$ is even, and b is therefore even (odd times odd is odd)

02.02] $\therefore b = 2d$, where d is some number, odd or even

03.00] So **a and b are both divisible by 2, and cannot be coprime**

03.01] ie $\sqrt{2n}$ cannot be rational, and is therefore irrational. QED.

D3] To investigate $\sqrt{2n+1}$ composites that aren't perfect squares

I have a nasty feeling that these may turn out to be sui generis, but hang on.

The proof below, that √15 is irrational, uses the unique prime factorisation theorem that every positive integer has a unique factorisation as a product of positive prime numbers.

The vital point is that the factors 3x5 in a squared entity must reflect the same factors in the entity itself (they can't have come from nowhere), and indeed the squared entity therefore actually gets a double dose of them !

https://socratic.org/users/george-c
https://socratic.org/questions/how-do-you-prove-that-square-root-15-is-irrational

Suppose $\sqrt{15} = p/q$ and that p and q are the smallest such positive integers. [ie √15 is expressed in lowest possible terms, $p > q$].

Then $p^2 = 15q^2$

The right hand side has factors of 3 and 5, so p^2 must be divisible by both 3 and 5. By the unique prime factorisation theorem, p too must be divisible by 3 and 5 [this takes thinking about, but it's correct – nihil ex nihilo].

So $p = 3x5k = 15k$ for some k
$\therefore 15^2k^2 = 15q^2$
$\therefore 15k = \sqrt{15}q$
$\therefore \sqrt{15} = q/k$ [ie √15 is expressed in lowest possible terms, $q > k$]. /contd

Thus k<q<p, contradicting our assertion that p,q is the smallest pair of values such that √15 = p/q.

So our initial assertion was false; there is no such pair of integers and √15 is therefore irrational.

The proof below, that √21 is irrational, follows the same strategy.

https://socratic.org/users/george-c
https://socratic.org/questions/59cbee0f11ef6b6a4bd9f74d

Suppose √21 = p/q and that p and q are the smallest such positive integers [ie √21 is expressed in lowest possible terms, p > q].

Then $p^2 = 21q^2$

Note that the right hand side is divisible by the prime numbers 3 and 7.

So p^2 is divisible by both 3 and 7.

By the unique prime factorisation theorem, p too is divisible by both 3 and 7 and hence by 3x7 = 21.

So p = 3x7k = 21k for some k

∴ $21^2k^2 = 21q^2$

∴ 21k = √21q

∴ √21 = q/k [ie √21 is expressed in lowest possible terms, q > k].

Note that p>q>k.

Thus q>k is a smaller pair of positive integers with quotient √21, contradicting our assertion that p>q was the smallest such pair.

So our initial assertion was false; there is no such pair of integers and √21 is therefore irrational.

George C is a clearly a philodidact in the best possible sense, infused with the Asimovian urge to communicate his enthusiasm for the wonderful world of human reasoning and understanding.

And it does seem that this procedure can be assumed to apply to all numbers in this category.

E1] To prove Euclid's Lemma (base case)

Firstly, what exactly is a lemma ? It seems to mean a relatively minor preliminary to more substantial results that are classified as theorems. Euclid, on whom I am certainly not an authority, probably established quite a number of lemmas in his monumental opus, but this particular one, leading as it does to what is known nowadays as the Fundamental Theorem of Arithmetic, has come to be called the Lemma in particular.

In its most general form (used above in [C]) it states that

- If a prime p divides a product $a_1a_2a_3a_4$ ….. a_n, then it must divide at least one of the factors a_i

In a more basic form (used above in [B]), Euclid originally stated that

- If a prime p divides a product ab, then it must divide at least one of the factors a or b

In modern times, Euclid’s proof has been regarded as obscure at best and even inadequate. I’m no mathematician, but I feel that his reputation can be salvaged in this regard, if only to make the Lemma at least plausible.

01.00] Given that ab = c
And that a prime p divides c (ie c = mp)
And that the prime p does not divide a (ie p and a are in fact coprime)
Then RTP that the prime p divides b (ie that b = np)

02.00] So ab = mp

∴ b = (m/a) p

03.00] All these quantities are of course individually integer and must yield an integer result. But there can be no cancellation between p and a, as they are coprime.

The cancellation must therefore occur between m and a, to provide an integer n :

b = np

Thus p divides b. QED.

To get a flavour of what the numbers are doing, suppose that a = 8, b = 6, and p = 3. Then [02.00] becomes 6 = (16/8).3 and n is therefore 2.

E2] To prove Euclid’s Lemma (general case)

01.00] Given that $a_1a_2a_3…a_N$ = c
And that a prime p divides c (ie c = mp)
Then RTP that p divides at least one of {a_1 , a_2 , a_3 , … , a_N }

02.00] By repeated application of the base case Lemma,

If p divides c then either p divides $a_1a_2a_3…a_{N-1}$ or p divides a_N
If p d.n. divide a_N then either p divides $a_1a_2a_3…a_{N-2}$ or p divides a_{N-1}
If p d.n. divide a_{N-1} then either p divides $a_1a_2a_3…a_{N-3}$ or p divides a_{N-2}
If p d.n. divide a_{N-2} then either p divides $a_1a_2a_3…a_{N-4}$ or p divides a_{N-3}
…
If p d.n divide a_5 then either p divides $a_1a_2a_3$ or p divides a_4

If p d.n divide a_4 then either p divides a_1a_2 or p divides a_3
If p d.n divide a_3 then either p divides a_1 or p divides a_2
If p d.n divide a_2 then p divides a_1

At least one of these exhaustive possibilities must apply. QED.

F] To prove the Unique Prime Factorisation theorem

Also known by the more grandiose name of the Fundamental Theorem of Arithmetic, it's a pons asinorum to most of us who had never been told about Euclid's Lemma, which makes the proof of the UPF very much easier indeed.

Rather forbiddingly stated that "Every positive integer *n* > 1 can be represented in exactly one way as a product of prime powers",

$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} = \prod_{i=1}^{k} p_i^{n_i}$$

it may be paraphrased by saying that every number can be represented as a multiplication of prime factors, some of which may occur repeatedly, and that no two numbers have exactly the same pattern of factors.

It could be said that the particular pattern of primes embodied by any given number is its fingerprint, its mugshot, its DNA.

The simplest proof by far runs as follows, and you wouldn't be surprised that it operates by reductio ad absurdum, otherwise known as proof by contradiction, a type of argument beloved by the Greeks.

Suppose that there is in fact at least one integer that has two distinct prime factorizations.

Let n be the least such integer and write $n = p_1 p_2 \ldots p_j = q_1 q_2 \ldots q_k$, where each p and q is prime.

As both representations have the same overall value, we can be assured that p_1 divides $q_1 q_2 \ldots q_k$, so p_1 divides some q by Euclid's lemma.

Without loss of generality, say p_1 divides q_1. Since p_1 and q_1 are both prime, it follows that $p_1 = q_1$. Returning to our factorizations of n, we may cancel these two terms to conclude $p_2 \ldots p_j = q_2 \ldots q_k$.

We now have two distinct prime factorizations of some integer strictly smaller than n, which contradicts the minimality of n.

So there can be no such integer with two distinct prime factorizations. QED.

Crikey, that was easy ! But what was that bit about Euclid's Lemma ?

- If a prime p divides a product $a_1a_2a_3a_4$ ….. a_n, then it must divide at least one of the factors a_i

Pomme de terre, Rodney – apart from the letters of the alphabet employed, precisely tailored to the task in hand.