SOME IRRATIONAL NUMBERS

PETE L. CLARK

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

Proof. Suppose not: then there exist integers a and $b \neq 0$ such that $\sqrt{2} = \frac{a}{b}$, meaning that $2 = \frac{a^2}{b^2}$. We may assume that a and b have no common divisor – if they do, divide it out – and in particular that a and b are not both even.

Now clear denominators:

$$a^2 = 2b^2.$$

So $2 \mid a^2$. It follows that $2 \mid a$. Notice that this is a direct consequence of Euclid's Lemma – if $p \mid a^2$, $p \mid a$ or $p \mid a$. On the other hand, we can simply prove the contrapositive: if a is odd, then a^2 is odd. By the Division Theorem, a number is odd iff we can represent it as $a = 2k + 1$, and then we just check: $(2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ is indeed again odd. So $a = 2A$, say. Plugging this into the equation we get

$$(2A)^2 = 4A^2 = 2b^2, \; b^2 = 2A^2,$$

so $2 \mid b^2$ and, as above, $2 \mid b$. Thus 2 divides both a and b: contradiction. □

Comment: This is a truly "classical" proof. In G.H. Hardy's *A Mathematician's Apology*, an extended rumination on the nature and beauty of pure mathematics, he gives just two examples of theorems: this theorem, and Euclid's proof of the infinitude of primes. As he says, this is inevitably a proof by contradiction (unlike Euclid's proof, which constructs new primes in a perfectly explicit way). The original statement is logically more complicated than what we actually prove in that it takes for granted that there is some *real* number $\sqrt{2}$ – characterized by being positive and having square equal to 2 – and then shows a "property" of this real number, namely it not being a fraction. But the essence of the matter is that a certain mathematical object *does not* exist – namely a rational number $\frac{a}{b}$ such that $(\frac{a}{b})^2 = 2$. This was the first "impossibility proof" in mathematics.

This is also one of the most historically important theorems in mathematics. History tells us that the result was discovered by Pythagoras, or at least someone in his school, and it was quite a shocking development (some sources say that the unnamed discoverer was fêted, others that he was cast into the sea). It caused Greek mathematicians to believe that geometric reasoning was more reliable than numerical, or quantitative reasoning, so that geometry became extremely well-developed in Greek mathematics at the expense of algebra.

Can we prove that $\sqrt{3}$ is irrational in the same way(s)? The Euclid's Lemma argument gives the irrationality of $\sqrt{p}$ for any prime p: write $\sqrt{p} = \frac{a}{b}$ in lowest terms, square and simplify to get $pb^2 = a^2$; then $p|a^2$ so $p|a$, so $a = pA$, and then

Thanks to Laura Nunley for pointing out a typo.

substituting we get $pb^2 = p^2A^2$, $b^2 = pA^2$, so $p \mid b^2$ and finally $p \mid b$: contradiction.

It is interesting to notice that even without Euclid's Lemma we can prove the result "by hand" for any fixed prime p. For instance, with $p = 3$ we would like to prove: $3 \mid a^2 \implies 3 \mid a$. The contrapositive is that if a is not divisible by 3, neither is a^2. Since any number which is not divisible by 3 is of the form $3k + 1$ or $3k + 2$, we need only calculate:

$$(3k+1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1,$$
$$(3k+2)^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1,$$

so in neither case did we get, upon squaring, a multiple of three. For any prime p, then, we can show $p|a^2 \implies p|a$ "by hand" by squaring each of the expressions $pk + i$, $0 < i < p$ and checking that we never get a multiple of p.

One can also look at this key step as a property of the ring Z_p of integers modulo p: if $0 \neq a \in Z_p$ then $0 \neq a^2 \in Z_p$. But – aha! – this is just saying that we don't want any nonzero elements in our ring Z_p which square to 0, so it will be true when Z_p is *reduced* (remember, this means that there are no nilpotent elements). When p is prime Z_p is an integral domain (even a field) so there are not even any zero divisors, but referring back to the algebra handout we proved more than this: for any n, Z_n is reduced iff n is squarefree. Thus, although the full strength of $p \mid ab \implies p \mid a$ or $p \mid b$ holds *only* for primes, the special case $p \mid a^2 \implies p \mid a$ is true not just for primes but for any squarefree integer p. (Stop and think about this for a moment; you can see it directly.) Thus the same argument in fact gives:

Proposition 2. *For any squarefree integer $n > 1$, $\sqrt{n}$ is irrational.*

What about the case of general n? Well, of course $\sqrt{n^2}$ is not only rational but is an integer, namely n. Moreover, an arbitrary positive integer n can be factored to get one of these two limiting cases: namely, any n can be uniquely decomposed as

$$n = sN^2,$$

where s is squarefree. (Prove it!) Since $\sqrt{sN^2} = N\sqrt{s}$, we have that $\sqrt{n}$ is rational iff $\sqrt{s}$ is rational; by the above result, this only occurs if $s = 1$. Thus:

Theorem 3. *For $n \in \mathbb{Z}^+$, $\sqrt{n}$ is rational iff $n = N^2$ is a perfect square.*

Another way of stating this result is that $\sqrt{n}$ is either an integer or is irrational.

What about cube roots and so forth? We can prove that $\sqrt[3]{2}$ is irrational using a similar argument: suppose $\sqrt[3]{2} = \frac{a}{b}$, with $\gcd(a, b) = 1$. Then we get

$$2b^3 = a^3,$$

so $2 \mid a^3$, thus $2 \mid a$. Put $a = 2A$, so $b^3 = 2^2A^3$ and $2 \mid b^3$. Thus $2 \mid b$: contradiction.

Any integer can be written as the product of a cube-free integer[1] and a perfect cube; with this one can prove that the $\sqrt[3]{n}$ is irrational unless $n = N^3$. For the sake of variety, we prove the general result in a different way.

Theorem 4. *Let $k > 2$ be a positive integer. Then $\sqrt[k]{n}$ is irrational unless $n = N^k$ is a perfect kth power.*

[1] I.e., an integer n with $\operatorname{ord}_p(n) \leq 2$ for all primes p.

Proof. Suppose n is not a perfect kth power. Then there exists some prime $p \mid n$ such that $\text{ord}_p(n)$ is not divisible by k. Let us use this prime to get a contradiction:

$$\frac{a^k}{b^k} = n,\ a^k = nb^k.$$

Take ord_p of both sides:

$$k\,\text{ord}_p(a) = \text{ord}_p(a^k) = \text{ord}_p(nb^k) = k\,\text{ord}_p(b) + \text{ord}_p(n),$$

so $\text{ord}_p(n) = k(\text{ord}_p(a) - \text{ord}_p(b))$ and $k \mid \text{ord}_p(n)$: contradiction. □

From a more algebraic perspective, there is yet a further generalization to be made. A complex number α is an **algebraic number** if there exists a polynomial

$$P(t) = a_n t^n + \ldots + a_1 t + a_0$$

with $a_i \in \mathbb{Z}$, $a_n \neq 0$, such that $P(\alpha) = 0$. Similarly, α is an **algebraic integer** if there exists such a polynomial P with $a_n = 1$ (a **monic polynomial**). We write $\overline{\mathbb{Q}}$ for the set of algebraic numbers and $\overline{\mathbb{Z}}$ for the set of algebraic integers.

Example: $\alpha = \frac{1}{2} \in \overline{\mathbb{Q}}$ because α satisfies the polynomial $2t - 1$; $\beta = \sqrt[5]{2} \in \overline{\mathbb{Z}}$ because β satisfies the polynomial $t^5 - 2$.

Theorem 5. *If $\alpha \in \mathbb{Q} \cap \overline{\mathbb{Z}}$, then $\alpha \in \mathbb{Z}$.*

Proof. Write $\alpha = \frac{a}{b}$ with $\gcd(a, b) = 1$ and assume α satisfies a monic polynomial:

$$(\frac{a}{b})^n + c_{n-1}(\frac{a}{b})^{n-1} + \ldots + c_1(\frac{a}{b}) + c_0 = 0.$$

We can clear denominators by multiplying through by b^n to get

$$a^n + bc_{n-1} \cdot a^{n-1} + \ldots + b^{n-1}c_1 \cdot a + b^n c_0 = 0,$$

or

$$a^n = b\left(-c_{n-1} \cdot a^{n-1} - \ldots - b^{n-2}c_1 \cdot a - b^{n-1}c_0\right). \tag{1}$$

If $b > 1$, then some prime p divides b and then, since p divides the right hand side of (1), it must divide the left hand side: $p \mid a^n$, so $p \mid a$. But, as usual, this contradicts the fact that a and b were chosen to be relatively prime. □

Example: It's not clear from the definition whether $\frac{1}{2} \in \overline{\mathbb{Z}}$: the polynomial $2t-1$ is not monic, but maybe $\frac{1}{2}$ satisfies some *other* monic polynomial? Theorem 4 implies that the answer is negative: otherwise would have $\frac{1}{2} \in \mathbb{Z}$.

We can deduce Theorem 4 from Theorem 5 by noticing that for any k and n, $\sqrt[k]{n}$ is a root of the polynomial $t^k - n$ so lies in $\overline{\mathbb{Z}}$. On the other hand, evidently $\sqrt[k]{n}$ is an integer iff n is a perfect kth power, so when n is not a perfect kth power, $\sqrt[k]{n} \in \overline{\mathbb{Z}} \setminus \mathbb{Z}$, so by Theorem 5, $\sqrt[k]{n} \notin \mathbb{Q}$.

In fact Theorem 5 is a special case of a familiar result from high school algebra.

Theorem 6. *(Rational Roots Theorem) If*

$$P(x) = a_n X + \ldots + a_1 x + a_0$$

is a polynomial with integral coefficients, then the only possible rational roots are those of the form $\pm\frac{c}{d}$, where $c \mid a_0$, $d \mid a_n$.